A Systematic Study

of

Gröbner Basis Methods

Vom Fachbereich Informatik
der Technischen Universität Kaiserslautern
genehmigte Habilitationsschrift
von

Dr. Birgit Reinert

Datum der Einreichung: 6. Januar 2003
Datum des wissenschaftlichen Vortrags: 9. Februar 2004

Dekan:	Prof. Dr. Hans Hagen
Habilitationskommission:	
Vorsitzender:	Prof. Dr. Otto Mayer
Berichterstatter:	Prof. Dr. Klaus E. Madlener
	Prof. Dr. Teo Mora
	Prof. Dr. Volker Weispfenning

Vorwort

Die vorliegende Arbeit ist die Quintessenz meiner Ideen und Erfahrungen, die ich in den letzten Jahren bei meiner Forschung auf dem Gebiet der Gröbnerbasen gemacht habe. Meine geistige Heimat war dabei die Arbeitsgruppe von Professor Klaus Madlener an der Technischen Universität Kaiserslautern. Hier habe ich bereits im Studium Bekanntschaft mit der Theorie der Gröbnerbasen gemacht und mich während meiner Promotion mit dem Spezialfall dieser Theorie für Monoid- und Gruppenringe beschäftigt. Nach der Promotion konnte ich im Rahmen eines DFG-Forschungsstipendiums zusätzlich Problemstellungen und Denkweisen anderer Arbeitsgruppen kennenlernen - die Arbeitsgruppe von Professor Joachim Neubüser in Aachen und die Arbeitsgruppe von Professor Theo Mora in Genua. Meine Aufenthalte in diesen Arbeitsgruppen haben meinen Blickwinkel für weitergehende Fragestellungen erweitert. An dieser Stelle möchte ich mich bei allen jenen bedanken, die mich in dieser Zeit begleitet haben und so zum Entstehen und Gelingen dieser Arbeit beigetragen haben.

Mein besonderer Dank gilt meinem akademischen Lehrer Professor Klaus Madlener, der meine akademische Ausbildung schon seit dem Grundstudium begleitet und meine Denk- und Arbeitsweise wesentlich geprägt hat. Durch ihn habe ich gelernt, mich intensiv mit diesem Thema zu beschäftigen und mich dabei nie auf nur einen Blickwinkel zu beschränken. Insbesondere sein weitreichenden Literaturkenntnisse und die dadurch immer neu ausgelösten Fragen aus verschiedenen Themengebieten bewahrten meine Untersuchungen vor einer gewissen Einseitigkeit. Er hat mich gelehrt, selbständig zu arbeiten, Ideen und Papiere zu hinterfragen, mir meine eigene Meinung zu bilden, diese zu verifizieren und auch zu vertreten.

Professor Teo Mora und Professor Volker Weispfenning danke ich für die Übernahme der weiteren Begutachtungen dieser Arbeit. Professor Teo Mora danke ich insbesondere auch für die fruchtbare Zeit in seiner Arbeitsgruppe in Genua. Seine Arbeiten und seine Fragen haben meine Untersuchungen zum Zusammenhang zwischen Gröbnerbasen in Gruppenringen und dem Todd-Coxeter Ansatz für Gruppen und die Fragestellungen dieser Arbeit wesentlich geprägt.

Meinen Kollegen aus unserer Arbeitsgruppe danke ich für ihre Diskussionsbereitschaft und ihre geduldige Anteilnahme an meinen Gedanken. Insbesondere

Andrea Sattler-Klein, Thomas Deiß, Claus-Peter Wirth und Bernd Löchner haben immer an mich geglaubt und mich ermutigt, meinen Weg weiter zu gehen. Mit ihnen durfte ich nicht nur Fachliches sondern das Leben teilen.

Um eine solche Arbeit fertigzustellen braucht man jedoch nicht nur eine fachliche Heimat. Mein Mann Joachim hat nie an mir gezweifelt und mich immer unterstützt. Auch nach unserem Umzug nach Rechberghausen hat er mein Pendeln nach Kaiserslautern und das Brachliegen unseres Haushalts mitgetragen. Ohne meine Eltern Irma und Helmut Weber und meine Patentante Anita Schäfer wäre insbesondere nach der Geburt unserer Tochter Hannah diese Arbeit nie fertiggestellt worden. Sie haben Hannah liebevoll behütet, so dass ich lesen, schreiben und arbeiten konnte, ohne ein schlechtes Gewissen zu haben. Hannah hat von Anfang an gelernt, dass Forschung ein Leben bereichern kann und die Zeit mit ihrer erweiterten Familie und die vielen Reisen nach Kaiserslautern genossen.

Gewidmet ist diese Arbeit meiner Mutter, die leider die Fertigstellung nicht mehr erleben durfte, und Hannah, die auch heute noch Geduld aufbringt, wenn ihre Mutter am Computer für ihre "Schule" arbeitet.

Rechberghausen, im August 2004 Birgit Reinert

Für meine Mutter
und Hannah

Contents

Chapter 1

Introduction

One of the amazing features of computers is the ability to do extensive computations impossible to be done by hand. This enables to overcome the boundaries of constructive algebra as proposed by mathematicians as Kronecker. He demanded that definitions of mathematical objects should be given in such a way that it is possible to decide in a finite number of steps whether a definition applies to an object. While in the beginning computers were used to do incredible numerical calculations, a new dimension was added when they were used to do symbolical mathematical manipulations substantial to many fields in mathematics and physics. These new possibilities led to open up whole new areas of mathematics and computer science. In the wake of these developments has come a new access to abstract algebra in a computational fashion – computer algebra. One important contribution to this field which is the subject of this work is the theory of Gröbner bases – the result of Buchberger's algorithm for manipulating systems of polynomials.

1.1 The History of Gröbner Bases

In 1965 Buchberger introduced the theory of Gröbner bases[1] for polynomial ideals in commutative polynomial rings over fields [Buc65, Buc70]. Let $\mathbb{K}[X_1, \ldots, X_n]$ be a polynomial ring over a computable field $\mathbb{K}$ and $\mathfrak{i}$ an ideal in $\mathbb{K}[X_1, \ldots, X_n]$. Then the quotient $\mathbb{K}[X_1, \ldots, X_n]/\mathfrak{i}$ is a $\mathbb{K}$-algebra. If this quotient is zero-dimensional the algebra has a finite basis consisting of power products $X_1^{i_1} \ldots X_n^{i_n}$. This was the starting point for Buchberger's PhD thesis. His advisor Wolfgang Gröbner wanted to compute the multiplication table and had suggested a procedure for zero-dimensional ideals, for which termination conditions were lacking. The result of Buchberger's studies then was a terminating algorithm which turned a basis of an ideal into a special basis which allowed to solve Gröbner's question of writing

[1]Note that similar concepts appear in a paper of Hironaka where the notion of a complete set of polynomials is called a standard basis [Hir64].

down an explicit multiplication for the multiplication table of the quotient in the zero-dimensional case and was even applicable to arbitrary polynomial ideals. Buchberger called these special bases of ideals Gröbner bases.

1.2 Two Definitions of Gröbner Bases

In literature there are two main ways to define Gröbner bases in polynomial rings over fields. They both require an admissible[2] ordering on the set of terms. With respect to such an ordering, given a polynomial f the maximal term occurring in f is called the head term denoted by $\mathsf{HT}(f)$.

One way to characterize Gröbner bases in an algebraic fashion is to use the concept of term division: A term $X_1^{i_1} \dots X_n^{i_n}$ is said to divide another term $X_1^{j_1} \dots X_n^{j_n}$ if and only if $i_l \leq j_l$ for all $1 \leq l \leq n$. Then a set G of polynomials is called a Gröbner basis of the ideal $\mathfrak{i}$ it generates if and only if for every f in $\mathfrak{i}$ there exists a polynomial $g \in G$ such that $\mathsf{HT}(g)$ divides $\mathsf{HT}(f)$.

Another way to define Gröbner bases in polynomial rings is to establish a rewriting approach to the theory of polynomial ideals. Polynomials can be used as rules by using the largest monomial according to the admissible ordering as a left hand side of a rule. Then a term is reducible by a polynomial as a rule if the head term of the polynomial divides the term. A Gröbner basis G then is a set of polynomials such that every polynomial in the polynomial ring has a unique normal form with respect to this reduction relation using the polynomials in G as rules (especially the polynomials in the ideal generated by G reduce to zero using G).

Of course both definitions coincide for polynomial rings since the reduction relation defined by Buchberger can be compared to division of one polynomial by a set of finitely many polynomials.

1.3 Applications of Gröbner Bases

The method of Gröbner bases allows to solve many problems related to polynomial ideals in a computational fashion. It was shown by Hilbert (compare Hilbert's basis theorem) that every ideal in a polynomial ring has a finite generating set. However, an arbitrary finite generating set need not provide much insight into the nature of the ideal. Let $f_1 = X_1^2 + X_2$ and $f_2 = X_1^2 + X_3$ be two polynomials in the polynomial ring[3] $\mathbb{Q}[X_1, X_2, X_3]$. Then $\mathfrak{i} = \{f_1 * g_1 + f_2 * g_2 \mid g_1, g_2 \in \mathbb{Q}[X_1, X_2, X_3]\}$ is the ideal they generate and it is not hard to see that

[2]An ordering $\succeq$ on the set of terms is called an admissible term ordering 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 $\circ$.

[3]$\mathbb{Q}$ denotes the rational numbers.

the polynomial $X_2 - X_3$ belongs to $\mathfrak{i}$ since $X_2 - X_3 = f_1 - f_2$. But what can be said about the polynomial $f = X_3^3 + X_1 + X_3$? Does it belong to $\mathfrak{i}$ or not?

The problem to decide whether a given polynomial lies in a given ideal is called the membership problem for ideals. In case the generating set is a Gröbner basis this problem becomes immediately decidable, as the membership problem then reduces to checking whether the polynomial reduces to zero using the elements of the Gröbner basis for reduction.

In our example the set $\{X_1^2 + X_3, X_2 - X_3\}$ is a generating set of $\mathfrak{i}$ which is in fact a Gröbner basis. Now returning to the polynomial $f = X_3^3 + X_1 + X_3$ we find that it cannot belong to $\mathfrak{i}$ since neither X_1^2 nor X_2 is a divisor of a term in f and hence f cannot be reduced to zero using the polynomials in the Gröbner basis as rules.

The terms $X_1^{i_1}X_2^{i_2}X_3^{i_3}$ which are not reducible by the set $\{X_1^2 + X_3, X_2 - X_3\}$ form a basis of the $\mathbb{Q}$-algebra $\mathbb{Q}[X_1, X_2, X_3]/\mathfrak{i}$. By inspecting the head terms X_1^2 and X_2 of the Gröbner basis we find that the (infinite) set $\{X_3^i, X_1X_3^i \mid i \in \mathbb{N}\}$ is such a basis. Moreover, an ideal is zero-dimensional, i.e. this set is finite, if and only if for each variable X_i the Gröbner basis contains a polynomial with head term $X_i^{k_i}$ for some $k_i \in \mathbb{N}^+$. Similarly the form of the Gröbner basis reveals whether the ideal is trivial: $\mathfrak{i} = \mathbb{K}[X_1, \ldots, X_n]$ if and only if every[4] Gröbner basis contains an element from $\mathbb{K}$.

Further applications of Gröbner bases come from areas as widespread as robotics, computer vision, computer-aided design, geometric theorem proving, Petrie nets and many more. More details can be found e.g. in Buchberger [Buc87], or the books of Becker and Weispfenning [BW92], Cox, Little and O'Shea [CLO92], and Adams and Loustaunau [AL94].

1.4 Generalizations of Gröbner Bases

In the last years, the method of Gröbner bases and its applications have been extended from commutative polynomial rings over fields to various types of algebras over fields and other rings. In general for such rings arbitrary finitely generated ideals will not have finite Gröbner bases. Nevertheless, there are interesting classes for which every finitely generated (left, right or even two-sided) ideal has a finite Gröbner basis which can be computed by appropriate variants of completion based algorithms.

First successful generalizations were extensions to commutative polynomial rings over coefficient domains other than fields. It was shown by several authors including Buchberger, Kandri-Rody, Kapur, Narendran, Lauer, Stifter, and Weispfenning that Buchberger's approach remains valid for polynomial

[4] Notice that if one Gröbner basis contains an element from $\mathbb{K}$ so will all the others.

rings over the integers, or even Euclidean rings, and over regular rings (see e.g. [Buc83, Buc85, KRK84, KRK88, KN85, Lau76, Sti87, Wei87b]). For regular rings Weispfenning has to deal with the situation that zero-divisors in the coefficient domain have to be considered. He uses a technique he calls Boolean closure to repair this problem and this technique can be regarded as a special saturating process[5]. We will later on see how such saturating techniques become important ingredients of Gröbner basis methods in many algebraic structures.

Since the development of computer algebra systems for commutative algebras made it possible to perform tedious calculations using computers, attempts to generalize such systems and especially Buchberger's ideas to non-commutative algebras followed. Originating from special problems in physics, Lassner in [Las85] suggested how to extend existing computer algebra systems in order to additionally handle special classes of non-commutative algebras, e.g. Weyl algebras. He studied structures where the elements could be represented using the usual representations of polynomials in commutative variables and the non-commutative multiplication could be performed by a so-called "twisted product" which required only procedures involving commutative algebra operations and differentiation. Later on together with Apel he extended Buchberger's algorithm to enveloping fields of Lie algebras [AL88]. Because these ideas use representations of the elements by commutative polynomials, Dickson's Lemma[6] can be carried over. By this the existence and construction of finite Gröbner bases for finitely generated left ideals can be ensured using the same arguments as in the original approach.

On the other hand, Mora gave a concept of Gröbner bases for a class of non-commutative algebras by saving an other property of the commutative polynomial ring – admissible orderings – while losing the validity of Dickson's Lemma. The usual polynomial ring can be viewed as a monoid ring where the monoid is a finitely generated free commutative monoid. Mora studied the class where the free commutative monoid is substituted by a free monoid – the class of finitely generated free monoid rings (compare e.g. [Mor85, Mor94]). The ring operations are mainly performed in the coefficient domain while the terms are treated like words, i.e., the variables no longer commute with each other and multiplication is concatenation. The definitions of (one- and two-sided) ideals, reduction and Gröbner bases are carried over from the commutative case to establish a similar theory of Gröbner bases in "free non-commutative polynomial rings over fields". But these rings are no longer Noetherian if they are generated by more than one variable. Mora presented a terminating completion procedure for finitely generated one-sided ideals and an enumeration procedure for finitely generated two-sided ideals with respect to some term ordering in free monoid rings. For

[5]Saturation techniques are used in various fields to enrich a generating set of a structure in such a way, that the new set still describes the same structure but allows more insight. For example symmetrization in groups can be regarded as such a saturating process.

[6]Dickson's Lemma in the context of commutative terms is as follows: For every infinite sequence of terms t_s, $s \in \mathbb{N}$, there exists an index $k \in \mathbb{N}$ such that for every index $i > k$ there exists an index $j \leq k$ and a term w such that $t_i = t_j w$.

the special instance of ideals generated by bases of the restricted form $\{\ell_i - r_i \mid \ell_i, r_i \text{ words}, 1 \leq i \leq n\}$, Mora's procedure coincides with Knuth-Bendix completion for string rewriting systems and the one-sided cases can be related to prefix respectively suffix rewriting [MR98d, MR98c]. Hence many results known for finite string rewriting systems and their completion carry over to finitely generated ideals and the computation of their Gröbner bases. Especially the undecidability of the word problem yields non-termination for Mora's general procedure (see also [Mor87]).

Gröbner bases and Mora's procedure have been generalized to path algebras (see [FCF93, Kel98]); free non-commutative polynomial rings are in fact a particular instance of path algebras.

Another class of non-commutative rings where the elements can be represented by the usual polynomials and which allow the construction of finite Gröbner bases for arbitrary ideals are the solvable polynomial rings, a class intermediate between commutative and general non-commutative polynomial rings. They were studied by Kandri-Rody, Weispfenning and Kredel [KRW90, Kre93]. Solvable polynomial rings can be described by ordinary polynomial rings $\mathbb{K}[X_1, \ldots, X_n]$ provided with a "new" definition of multiplication which coincides with the ordinary multiplication except for the case that a variable X_j is multiplied with a variable X_i with lower index, i.e., $i < j$. In the latter case multiplication can be defined by equations of the form $X_j \star X_i = c_{ij} X_i X_j + p_{ij}$ where c_{ij} lies in $\mathbb{K}^* = \mathbb{K} \backslash \{0\}$ and p_{ij} is a polynomial "smaller" than $X_i X_j$ with respect to a fixed admissible term ordering on the polynomial ring.

The more special case of twisted semi-group rings, where $c_{ij} = 0$ is possible, has been studied in [Ape88, Mor89].

In [Wei87a] Weispfenning showed the existence of finite Gröbner bases for arbitrary finitely generated ideals in non-Noetherian skew polynomial rings over two variables X, Y where a "new" multiplication $\star$ is introduced such that $X \star Y = XY$ and $Y \star X = X^e Y$ for some fixed e in $\mathbb{N}^+$.

Ore extensions have been successfully studied by Pesch in his PhD Thesis [Pes97] and his results on two-sided Gröbner bases are also presented in [Pes98].

Most of the results cited so far assume admissible well-founded orderings on the set of terms so that in fact the reduction relations can be defined by considering the head monomials mainly (compare the algebraic definition of Gröbner bases in Section 1.2). This is essential to characterize Gröbner bases in the respective ring with respect to the corresponding reduction relation[7] in a finitary manner and to enable to decide whether a finite set is a Gröbner basis by checking whether the s-polynomials are reducible to zero[8].

[7] These reduction relations are based on divisibility of terms, namely the term to be reduced is divisible by the head term of the polynomial used as rule for the reduction step.

[8] Note that we always assume that the reduction relation in the ring is effective.

There are rings combined with reduction relations where admissible well-founded orderings cannot be accomplished and, therefore, other concepts to characterize Gröbner bases have been developed. For example in case the ring contains zero-divisors a well-founded ordering on the ring is no longer compatible with the ring multiplication[9]. This phenomenon has been studied for the case of zero-divisors in the coefficient domain by Kapur and Madlener [KM89] and by Weispfenning for the special case of regular rings [Wei87b]. In his PhD thesis [Kre93], Kredel described problems occurring when dropping the axioms guaranteeing the existence of admissible orderings in the theory of solvable polynomial rings by allowing $c_{ij} = 0$ in the defining equations above. He sketched the idea of using saturation techniques to repair some of them. Saturation enlarges the generating sets of ideals in order to ensure that enough head terms exist to do all necessary reduction steps and this process can often be related to additional special critical pairs. Similar ideas can be found in the PhD thesis of Apel [Ape88]. For special cases, e.g. for the Grassmann (exterior) algebras, positive results can be achieved (compare the paper of Stokes [Sto90]).

Another important class of rings where reduction relations can be introduced and completion techniques can be applied to enumerate and sometimes compute Gröbner bases are monoid and group rings. They have been studied in detail by various authors, e.g. free group rings ([Ros93]), monoid and group rings ([MR93a, MR97a, Rei95, Rei96, MR98a]) (including finite and free monoids and finite, free, plain and polycyclic groups), and polycyclic group rings ([Lo98]). In this setting we again need saturation techniques to repair a severe defect due to the fact that in general we cannot expect the ordering on the set of terms (here of course now the monoid or group elements) to be both, well-founded and admissible. Let $\mathcal{F}$ be the free group generated by one element a. Then for the polynomial $a+1$ in $\mathbb{Q}[\mathcal{F}]$ we have $(a+1) * a^{-1} = 1 + a^{-1}$, i.e., after multiplication with the inverse element a^{-1} the largest term of the new polynomial no longer results from the largest one of the original polynomial. Moreover, assuming our ordering is well-founded, it cannot be compatible with the group multiplication[10].

All approaches cited in this section can be basically divided into two main streams: One extension was to study structures which still allow to present their elements by ordinary "commutative" polynomials. The advantage of this generalization is that Dickson's Lemma, which is essential in proving termination for Buchberger's algorithm, carries over. The other idea of generalization was to view the polynomial ring as a special monoid ring and to try to extend Buchberger's approach to other monoid and group rings. Since then in general Dickson's Lemma no longer holds, other ways to prove termination, if possible, have to be established.

[9] When studying monoid rings over reduction rings it is possible that the ordering on the ring is not compatible with scalar multiplication as well as with multiplication with monomials or polynomials.

[10] Assuming $a \succ 1$ compatibility with multiplication would imply $1 \succ a^{-1}$ giving rise to an infinite descending chain $a^{-1} \succ a^{-2} \succ \ldots$ contradicting the well-foundedness of the ordering. On the other hand for $1 \succ a$ compatibility with multiplication immediately gives us an infinite descending chain $a \succ a^2 \succ \ldots$.

Notice that solvable rings, skew-polynomial rings and arbitrary quotients of non-commutative polynomial rings cannot be interpreted as monoid rings. Hence to find a generalization which will subsume *all* results cited here, a more general setting is needed. In his habilitation thesis [Ape98], Apel provides one generalization which basically extends the first one of these two in such a way that Mora's approach can be incorporated. He uses an abstraction of graded structures which needs admissible well-founded orderings. Hence he cannot deal with group rings and many cases of monoid rings where such orderings cannot exists. On the other hand he is much more interested in algebraic characterizations of Gröbner bases and the division algorithms associated to them.

In order to characterize structures where the well-founded ordering is no longer admissible, we extend Gröbner basis techniques to an abstract setting called function rings.

1.5 Gröbner Bases in Function Rings – A Guide for Introducing Reduction Relations to Algebraic Structures

The aim of this work is to give a general setting which comprises *all* generalizations mentioned above and which is a basis for studying further structures in the light of introducing reduction relations and Gröbner basis techniques. All structures mentioned so far can be viewed as rings of functions with finite support. For such rings we introduce the familiar concepts of polynomials, (right) ideals, standard representations, standard bases, reduction relations and Gröbner bases. A general characterization of Gröbner bases in an "algorithmic fashion" is provided. It is shown that in fact polynomial rings, solvable polynomial rings, free respectively finite monoid rings, and free, finite, plain, respectively polycyclic group rings are examples of our generalization where finite Gröbner bases can be computed. While most of the examples cited above are presented in the literature as rings over fields we will here also present the more general concept of function rings over reduction rings (compare [Mad86, Rei95, MR98b]) and the impotant special case of function rings over the integers.

1.6 Applications of Gröbner Bases Generalized to Function Rings

For polynomial rings over fields many algebraic questions related to ideals can be solved using Gröbner bases and their associated reduction relations. Hence the question arises which of these applications can be extended to more general settings. While some questions e.g. concerning algebraic geometry are strongly connected to polynomial rings over fields, many other applications carry over. They include natural ones such as the membership problem for ideals, as well as special techniques such as elimination theory or the treatment of systems of linear equations.

1.7 Organization of the Contents

Chapter 2 introduces some of the basic themes of this book. We need some basic notions from the theory of algebra as well as from the theory of rewriting systems. Furthermore, as the aim of this book is to provide a systematic study of Gröbner basis methods, a short introduction to the original case of Gröbner bases in polynomial rings over fields is presented.

Chapter 3 concentrates on rings with reduction relations, which are studied with regard to the existence of Gröbner bases. They are called reduction rings in case they allow finite Gröbner bases for finitely generated ideals. Moreover, special ring constructions are presented, which in many cases preserve the existence of Gröbner bases. These constructions include quotients and sums of reduction rings as well as modules and polynomial rings over reduction rings. Many structures with reduction relations allowing Gröbner bases can already be found in this setting. For example knowing that the integers $\mathbb{Z}$ for certain reduction relations allow finite Gröbner bases, using the results of this chapter, we can conclude that the module $\mathbb{Z}^k$ as well as the polynomial rings $\mathbb{Z}[X_1, \ldots, X_n]$ and $\mathbb{Z}^k[X_1, \ldots, X_n]$ allow the computation of finite Gröbner bases.

Chapter 4 is the heart of this book. It establishes a generalizing framework for structures enriched with reduction relations and studied with respect to the existence of Gröbner bases in the literature. Reduction relations are defined for the setting of function rings over fields and later on generalized to reduction rings. Definitions for terms such as variations of standard representations, standard bases and Gröbner bases are given and compared to the known terms from the theory of Gröbner bases over polynomial rings. It turns out that while completion procedures will still involve equivalents to s-polynomials or the more general concept of g- and m-polynomials for the ring case, these situations are no longer sufficient to characterize Gröbner bases. Saturation techniques, which enrich the bases by additional polynomials, are needed. Moreover, for function rings over reduction rings the characterizations no longer describe Gröbner bases but only weak[11] Gröbner bases, since the Translation Lemma[12] no longer holds. Since the

[11] Weak Gröbner bases are bases such that any polynomial in the ideal they generate can be reduced to zero. For fields this property already characterizes Gröbner bases as the Translation Lemma holds. In general this is not true and while weak Gröbner bases allows to solve the ideal membership problem they no longer guarantee the existence of unique normal forms for elements of the quotient.

[12] The Translation Lemma establishes that if for two polynomials f, g we have that $f - g$ reduces to zero, both polynomials reduce to the same normal form.

ring of integers viewed as a reduction ring is of special interest in the literature and allows more insight into the respective chosen reduction relations, this special case is studied.

Chapter 5 outlines how some applications known for Gröbner bases in the literature carry over to function rings. These applications include natural ones such as the ideal membership problem, representation problems, the ideal inclusion problem, the ideal triviality problem, and many more. Another focus is on doing computations in quotient rings using Gröbner bases. The powerful elimination methods are also generalized. One of their applications to study polynomial mappings is outlined. Finally solutions for linear equations over function rings in terms of Gröbner bases are provided.

Chapter 2

Basic Definitions

After introducing the necessary definitions required from algebra we focus on the subject of this book — Gröbner bases. One way of characterizing Gröbner bases is in terms of algebraic simplification or reduction. The aim of this chapter is to introduce an abstract concept for the notion of reduction which is the basis of many syntactical methods for studying structures in mathematics or theoretical computer science in Section 2.2. It is the foundation for e.g. term rewriting and string rewriting and we introduce a reduction relation for polynomials in the commutative polynomial ring over a field in a similar fashion. Gröbner bases then arise naturally when doing completion in this setting in Section 2.3.

2.1 Algebra

Mathematical theories are closely related with the study of two objects, namely sets and functions. Algebra can be regarded as the study of algebraic operations on sets, i.e., functions that take elements from a set to the set itself. Certain algebraic operations on sets combined with certain axioms are again the objects of independent theories. This chapter is a short introduction to some of the algebraic systems used later on: monoids, groups, rings, fields, ideals and modules.

Definition 2.1.1
A non-empty set of elements $\mathcal{M}$ together with a binary operation $\circ_{\mathcal{M}}$ is said to form a **monoid**, if for all α, β, γ in $\mathcal{M}$

1. $\mathcal{M}$ is closed under $\circ_{\mathcal{M}}$, i.e., $\alpha \circ_{\mathcal{M}} \beta \in \mathcal{M}$,
2. the associative law holds for $\circ_{\mathcal{M}}$, i.e., $\alpha \circ_{\mathcal{M}} (\beta \circ_{\mathcal{M}} \gamma) =_{\mathcal{M}} (\alpha \circ_{\mathcal{M}} \beta) \circ_{\mathcal{M}} \gamma$, and
3. there exists $1_{\mathcal{M}} \in \mathcal{M}$ such that $\alpha \circ_{\mathcal{M}} 1_{\mathcal{M}} =_{\mathcal{M}} 1_{\mathcal{M}} \circ_{\mathcal{M}} \alpha =_{\mathcal{M}} \alpha$. The element $1_{\mathcal{M}}$ is called **identity**. $\diamond$

For simplicity of notation we will henceforth drop the index $\mathcal{M}$ and write $\circ$ respectively $=$ if no confusion is likely to arise. Furthermore, we will often talk about a monoid without mentioning its binary operation explicitly. The monoid operation will often be called multiplication or addition. Since the algebraic operation is associative we can omit brackets, hence the product $\alpha_1 \circ \ldots \circ \alpha_n$ is uniquely defined.

Example 2.1.2
Let $\Sigma = \{a_1, \ldots, a_n\}$ be a set of letters. Then Σ^* denotes the set of words over this alphabet. For two words $u, v \in \Sigma^*$ we define $u \circ v = uv$, i.e., the word which arises from concatenating the two words u and v. Then Σ^* is a monoid with respect to this binary operation and its identity element is the empty word, i.e., the word containing no letters. This monoid is called the **free monoid** over the alphabet Σ. $\diamond$

For some n in $\mathbb{N}$[1] the product of n times the same element α is called the **n-th power of** α and will be denoted by α^n, where $\alpha^0 = 1$.

Definition 2.1.3
An element α of a monoid $\mathcal{M}$ is said to have **infinite order** in case for all $n, m \in \mathbb{N}$, $\alpha^n = \alpha^m$ implies $n = m$. We say that α has **finite order** in case the set $\{\alpha^n \mid n \in \mathbb{N}^+\}$ is finite and the cardinality of this set is then called the **order** of α. $\diamond$

A subset of a monoid $\mathcal{M}$ which is again a monoid is called a **submonoid** of $\mathcal{M}$. Other special subsets of monoids are (one-sided) ideals.

Definition 2.1.4
For a subset S of a monoid $\mathcal{M}$ we call

1. $\mathsf{ideal}_r^{\mathcal{M}}(S) = \{\sigma \circ \alpha \mid \sigma \in S, \alpha \in \mathcal{M}\}$ the right ideal,
2. $\mathsf{ideal}_l^{\mathcal{M}}(S) = \{\alpha \circ \sigma \mid \sigma \in S, \alpha \in \mathcal{M}\}$ the left ideal, and
3. $\mathsf{ideal}^{\mathcal{M}}(S) = \{\alpha \circ \sigma \circ \alpha' \mid \sigma \in S, \alpha, \alpha' \in \mathcal{M}\}$ the ideal

generated by S in $\mathcal{M}$. $\diamond$

A monoid $\mathcal{M}$ is called **commutative (Abelian)** if we have $\alpha \circ \beta = \beta \circ \alpha$ for all elements α, β in $\mathcal{M}$. A natural example for a commutative monoid are the integers together with multiplication or addition. Another example which will be of interest later on is the set of terms.

[1] In the following $\mathbb{N}$ denotes the set of natural numbers including zero and $\mathbb{N}^+ = \mathbb{N} \backslash \{0\}$.

Example 2.1.5
Let $X_1, \ldots, X_n$ be a set of (ordered) variables. Then $\mathcal{T} = \{X_1^{i_1} \ldots X_n^{i_n} \mid i_1, \ldots i_n \in \mathbb{N}\}$ is called the set of **terms** over these variables. The multiplication $\circ$ is defined as $X_1^{i_1} \ldots X_n^{i_n} \circ X_1^{j_1} \ldots X_n^{j_n} = X_1^{i_1+j_1} \ldots X_n^{i_n+j_n}$. The identity is the empty term $1_{\mathcal{T}} = X_1^0 \ldots X_n^0$. $\diamond$

A mapping ϕ from one monoid $\mathcal{M}_1$ to another monoid $\mathcal{M}_2$ is called a **homomorphism**, if $\phi(1_{\mathcal{M}_1}) = 1_{\mathcal{M}_2}$ and for all α, β in $\mathcal{M}_1$, $\phi(\alpha \circ_{\mathcal{M}_1} \beta) = \phi(\alpha) \circ_{\mathcal{M}_2} \phi(\beta)$. In case ϕ is surjective we call it an **epimorphism**, in case ϕ is injective a **monomorphism** and in case it is both an **isomorphism**. The fact that two structures S_1, S_2 are isomorphic will be denoted by $S_1 \cong S_2$.

A monoid is called **left-cancellative** (respectively **right-cancellative**) if for all α, β, γ in $\mathcal{M}$, $\gamma \circ \alpha = \gamma \circ \beta$ (respectively $\alpha \circ \gamma = \beta \circ \gamma$) implies $\alpha = \beta$. In case a monoid is both, left- and right-cancellative, it is called **cancellative**. In case $\alpha \circ \gamma = \beta$ we say that α is a **left divisor** of β and γ is called a **right divisor** of b. If $\gamma \circ \alpha \circ \delta = \beta$ then α is called a **divisor** of β. A special class of monoids fulfill that for all α, β in $\mathcal{M}$ there exist γ, δ in $\mathcal{M}$ such that $\alpha \circ \gamma = \beta$ and $\delta \circ \alpha = \beta$, i.e., right and left divisors always exist. These structures are called groups and they can be specified by extending the definition of monoids and we do so by adding one further axiom.

Definition 2.1.6
A monoid $\mathcal{M}$ together with its binary operation $\circ$ is said to form a **group** if additionally

4. for every $\alpha \in \mathcal{M}$ there exists an element $\mathsf{inv}(\alpha) \in \mathcal{M}$ (called **inverse** of α) such that $\alpha \circ \mathsf{inv}(\alpha) = \mathsf{inv}(\alpha) \circ \alpha = 1$. $\diamond$

Obviously, the integers form a group with respect to addition, but this is no longer true for multiplication.

A subset of a group $\mathcal{G}$ which is again a group is called a **subgroup** of $\mathcal{M}$. A subgroup $\mathcal{H}$ of a group $\mathcal{G}$ is called **normal** if for each α in $\mathcal{G}$ we have $\alpha\mathcal{H} = \mathcal{H}\alpha$ where $\alpha\mathcal{H} = \{\alpha \circ \beta \mid \beta \in \mathcal{H}\}$ and $\mathcal{H}\alpha = \{\beta \circ \alpha \mid \beta \in \mathcal{H}\}$.

We end this section by briefly introducing some more algebraic structures that will be used throughout.

Definition 2.1.7
A nonempty set R is called an **(associative) ring (with unit element)** if there are two binary operations $+$ (addition) and $\star$ (multiplication) such that for all α, β, γ in R

1. R together with $+$ is an Abelian group with zero element 0 and inverse $-\alpha$,

2. R is closed under $\star$, i.e., $\alpha \star \beta \in \mathsf{R}$,
3. $\star$ is associative, i.e., $\alpha \star (\beta \star \gamma) = (\alpha \star \beta) \star \gamma$,
4. the distributive laws hold, i.e., $\alpha \star (\beta + \gamma) = \alpha \star \beta + \alpha \star \gamma$ and $(\beta + \gamma) \star \alpha = \beta \star \alpha + \gamma \star \alpha$,
5. there is an element $1 \in \mathsf{R}$ (called **unit**) such that $1 \star \alpha = \alpha \star 1 = \alpha$. $\diamond$

A ring is called **commutative (Abelian)** if $\alpha \star \beta = \beta \star \alpha$ for all α, β in R. The integers together with addition and multiplication are a well-known example of a ring. Other rings which will be of interest later on are monoid rings.

Example 2.1.8
Let $\mathbb{Z}$ be the ring of integers and $\mathcal{M}$ a monoid. Further let $\mathbb{Z}[\mathcal{M}]$ denote the set of all mappings $f : \mathcal{M} \longrightarrow \mathbb{Z}$ where the sets $\mathsf{supp}(f) = \{\alpha \in \mathcal{M} \mid f(\alpha) \neq 0\}$ are finite. We call $\mathbb{Z}[\mathcal{M}]$ the **monoid ring** of $\mathcal{M}$ over $\mathbb{Z}$. The **sum** of two elements f and g is denoted by $f + g$ where $(f + g)(\alpha) = f(\alpha) + g(\alpha)$. The **product** is denoted by $f \star g$ where $(f \star g)(\alpha) = \sum_{\beta \circ \gamma = \alpha} f(\beta) \star g(\gamma)$.

Polynomial rings are a special case of monoid rings namely over the set of terms as defined in Example 2.1.5.

A ring R is said to contain **zero-divisors**, if there exist not necessarily different elements α, β in R such that $\alpha \neq 0$ and $\beta \neq 0$, but $\alpha \star \beta = 0$. Then α is called a left zero-divisor and β is called a right zero-divisor.

Definition 2.1.9
A commutative ring is called a **field** if its non-zero elements form a group under multiplication. $\diamond$

Similar to our proceeding in group theory we will now look at subsets of a ring R. For a subset $U \subseteq \mathsf{R}$ to be a **subring** of R with the operations $+$ and $\star$ it is necessary and sufficient that

1. U is a subgroup of $(\mathsf{R}, +)$, i.e., for $a, b \in U$ we have $a - b \in U$, and
2. for all $\alpha, \beta \in U$ we have $\alpha \star \beta \in U$.

We will now take a closer look at special subrings that play a role similar to normal subgroups in group theory.

Definition 2.1.10
A nonempty subset $\mathfrak{i}$ of a ring R is called a **right (left) ideal** of R, if

1. for all $\alpha, \beta \in \mathfrak{i}$ we have $\alpha - \beta \in \mathfrak{i}$, and

2. for every $\alpha \in \mathfrak{i}$ and $\rho \in \mathsf{R}$, the element $\alpha \star \rho$ (respectively $\rho \star \alpha$) lies in $\mathfrak{i}$.

A subset that is both, a right and a left ideal, is called a **(two-sided) ideal** of R. ◇

For each ring the sets $\{0\}$ and R are trivial ideals. Similar to subgroups, ideals can be described in terms of generating sets.

Lemma 2.1.11
Let F be a non-empty subset of R. Then

1. $\mathsf{ideal}^{\mathsf{R}}(F) = \{\sum_{i=1}^{n} \rho_i \star \alpha_i \star \sigma_i \mid \alpha_i \in F, \rho_i, \sigma_i \in \mathsf{R}, n \in \mathbb{N}\}$ *is an ideal of* R,
2. $\mathsf{ideal}_r^{\mathsf{R}}(F) = \{\sum_{i=1}^{n} \alpha_i \star \rho_i \mid \alpha_i \in F, \rho_i \in \mathsf{R}, n \in \mathbb{N}\}$ *is a right ideal of* R, *and*
3. $\mathsf{ideal}_l^{\mathsf{R}}(F) = \{\sum_{i=1}^{n} \rho_i \star \alpha_i \mid \alpha_i \in F, \rho_i \in \mathsf{R}, n \in \mathbb{N}\}$ *is a left ideal of* R. ◇

Notice that the empty sum $\sum_{i=1}^{0} \alpha_i$ is zero.

We will simply write $\mathsf{ideal}(F)$, $\mathsf{ideal}_r(F)$ and $\mathsf{ideal}_l(F)$ if the context is clear. Many algebraic problems for rings are related to ideals and we will close this section by stating two of them[2].

The Ideal Membership Problem

Given: An element $\alpha \in \mathsf{R}$ and a set of elements $F \subseteq \mathsf{R}$.
Question: Is α in the ideal generated by F?

Definition 2.1.12
Two elements $\alpha, \beta \in \mathsf{R}$ are said to be **congruent modulo** $\mathsf{ideal}(F)$, denoted by $\alpha \equiv_{\mathsf{ideal}(F)} \beta$, if $\alpha = \beta + \rho$ for some $\rho \in \mathsf{ideal}(F)$, i.e., $\alpha - \beta \in \mathsf{ideal}(F)$. ◇

The Congruence Problem

Given: Two elements $\alpha, \beta \in \mathsf{R}$ and a set of elements $F \subseteq \mathsf{R}$.
Question: Are α and β congruent modulo the ideal generated by F?

Note that both problems can similarly be specified for left and right ideals.

We have seen that a non-empty subset of R is an ideal if it is closed under addition and closed under multiplication with arbitrary elements of R. Modules now can be viewed as a natural generalization of the concept of ideals to arbitrary commutative groups.

[2]For more information on such problems in the special case of commutative polynomial rings see e.g. [Buc87].

Definition 2.1.13
Let R be a ring. A **left R-module** M is an additive commutative group with an additional operation $\cdot : \mathsf{R} \times M \longrightarrow M$, called scalar multiplication, such that for all $\alpha, \beta \in \mathsf{R}$ and $a, b \in M$, the following hold:

1. $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$,
2. $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$,
3. $(\alpha \star \beta) \cdot a = \alpha \cdot (\beta \cdot a)$, and
4. $1 \cdot a = a$. ◇

We can define right R-modules and (two-sided) R-modules (also called R-bimodules) in a similar fashion.

Notice that a (left, right) ideal $\mathfrak{i} \subseteq \mathsf{R}$ forms a (left, right) R-module with respect to the addition and multiplication in R. This obviously holds for the trivial (left, right) ideals $\{0\}$ and R of R.

Another example of (left, right) R-modules we will study are the finite direct products of the ring called free (left, right) R-modules R^k, $k \in \mathsf{R}$.

An additive subset of a (left, right) R-module is called a **(left, right) submodule** if it is closed under scalar multiplication with elements of R. For a subset $F \subseteq M$ let $\langle F \rangle$ denote the submodule generated by F in M.

The Submodule Membership Problem

Given: An element $a \in M$ and a set of elements $F \subseteq M$.
Question: $a \in \langle F \rangle$?

Similar to the congruence problem for ideals we can specify the congruence problem for submodules as follws:

Definition 2.1.14
Two elements $a, b \in \mathsf{R}$ are said to be **congruent modulo** the submodule $\langle F \rangle$ for some $F \subseteq M$, denoted by $a \equiv_{\langle F \rangle} b$, if $a - b \in \langle F \rangle$. ◇

The Congruence Problem for submodules

Given: Two elements $a, b \in \mathsf{R}$ and a set of elements $F \subseteq M$.
Question: $a \equiv_{\langle F \rangle} b$?

2.2 The Notion of Reduction

This section summarizes some important notations and definitions of reduction relations and basic properties related to them, as can be found more explicitly for example in the work of Huet or Book and Otto ([Hue80, Hue81, BO93]).

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**. Then we can expand the binary relation as follows:

$\xrightarrow{0}$	denotes the identity on $\mathcal{E}$,
$\longleftarrow$	denotes the inverse relation for $\longrightarrow$,
$\xrightarrow{n+1} := \xrightarrow{n} \circ \longrightarrow$	where $\circ$ denotes composition of relations and $n \in \mathbb{N}$,
$\xrightarrow{\leq n} := \bigcup_{0 \leq i \leq n} \xrightarrow{i}$,	
$\xrightarrow{+} := \bigcup_{n > 0} \xrightarrow{n}$	denotes the transitive closure of $\longrightarrow$,
$\xrightarrow{*} := \xrightarrow{+} \cup \xrightarrow{0}$	denotes the reflexive transitive closure of $\longrightarrow$,
$\longleftrightarrow := \longleftarrow \cup \longrightarrow$	denotes the symmetric closure of $\longrightarrow$,
$\xleftrightarrow{+}$	denotes the symmetric transitive closure of $\longrightarrow$,
$\xleftrightarrow{*}$	denotes the reflexive symmetric transitive closure of $\longrightarrow$.

A well-known decision problem related to a reduction system is the word problem.

Definition 2.2.1
The **word problem** for a reduction system $(\mathcal{E}, \longrightarrow)$ is to decide for a, b in $\mathcal{E}$, whether $a \xleftrightarrow{*} b$ holds. $\diamond$

Instances of this problem are well-known in the literature and undecidable in general. In the following we will outline sufficient conditions such that a reduction system $(\mathcal{E}, \longrightarrow)$ has solvable word problem.

An element $a \in \mathcal{E}$ is said to be **reducible** (with respect to $\longrightarrow$) if there exists an element $b \in \mathcal{E}$ such that $a \longrightarrow b$. All elements $b \in \mathcal{E}$ such that $a \xrightarrow{*} b$ are called **successors** of a and in case $a \xrightarrow{+} b$ they are called **proper successors**. An element which has no proper successors is called **irreducible**. In case $a \xrightarrow{*} b$ and b is irreducible, b is called a **normal form** of a. Notice that for an element a in $\mathcal{E}$ there can be no, one or many normal forms.

Definition 2.2.2
A reduction system $(\mathcal{E}, \longrightarrow)$ is said to be **Noetherian** (or **terminating**) in case there are no infinitely descending reduction chains $a_0 \longrightarrow a_1 \longrightarrow \ldots$, with $a_i \in \mathcal{E}$, $i \in \mathbb{N}$. $\diamond$

In case a reduction system $(\mathcal{E}, \longrightarrow)$ is Noetherian every element in $\mathcal{E}$ has at least one normal form.

Definition 2.2.3
A reduction system $(\mathcal{E}, \longrightarrow)$ is called **confluent**, if for all $a, a_1, a_2 \in \mathcal{E}$, $a \xrightarrow{*} a_1$ and $a \xrightarrow{*} a_2$ implies the existence of $a_3 \in \mathcal{E}$ such that $a_1 \xrightarrow{*} a_3$ and $a_2 \xrightarrow{*} a_3$, and a_1, a_2 are called **joinable**. $\diamond$

In case a reduction system $(\mathcal{E}, \longrightarrow)$ is confluent every element has at most one normal form. We can combine these two properties to give sufficient conditions for the solvability of the word problem.

Definition 2.2.4
A reduction system $(\mathcal{E}, \longrightarrow)$ is said to be **complete** (or **convergent**) in case it is both, Noetherian and confluent. $\diamond$

Complete reduction systems with effective or computable[3] reduction relations have solvable word problem, as every element has a unique normal form and two elements are equal if and only if their normal forms are equal. Of course we cannot always expect $(\mathcal{E}, \longrightarrow)$ to be complete. Even worse, both properties – termination and confluence – are undecidable in general. Nevertheless, there are weaker conditions which guarantee completeness.

Definition 2.2.5
A reduction system $(\mathcal{E}, \longrightarrow)$ is said to be **locally confluent**, if for all $a, a_1, a_2 \in \mathcal{E}$, $a \longrightarrow a_1$ and $a \longrightarrow a_2$ implies the existence of an element $a_3 \in \mathcal{E}$ such that $a_1 \xrightarrow{*} a_3$ and $a_2 \xrightarrow{*} a_3$. $\diamond$

I.e. local confluence is a special instance of confluence, namely a *localization* of confluence to one-reduction-step successors of elements only. The next lemma gives an important connection between local confluence and confluence.

Lemma 2.2.6 (Newman)
Let $(\mathcal{E}, \longrightarrow)$ be a Noetherian reduction system. Then $(\mathcal{E}, \longrightarrow)$ is confluent if and only if $(\mathcal{E}, \longrightarrow)$ is locally confluent.

To prove Newman's lemma we need the concept of Noetherian induction which is based on the following definition.

Definition 2.2.7
Let $(\mathcal{E}, \longrightarrow)$ be a reduction system. A predicate $\mathcal{P}$ on $\mathcal{E}$ is called **$\longrightarrow$-complete**, in case for every $a \in \mathcal{E}$ the following implication holds: if $\mathcal{P}(b)$ is true for all proper successors of a, then $\mathcal{P}(a)$ is true. $\diamond$

[3] By effective or computable we mean that given an element we can always construct a successor in case one exists.

The Principle of Noetherian Induction:
In case $(\mathcal{E}, \longrightarrow)$ is a Noetherian reduction system and $\mathcal{P}$ is a predicate that is $\longrightarrow$-complete, then for all $a \in \mathcal{E}$, $\mathcal{P}(a)$ is true.

Proof of Newman's lemma:
Suppose, first, that the reduction system $(\mathcal{E}, \longrightarrow)$ is confluent. This immediately implies the local confluence of $(\mathcal{E}, \longrightarrow)$ as a special case. To show the converse, since $(\mathcal{E}, \longrightarrow)$ is Noetherian we can apply the principle of Noetherian induction to the following predicate:

$$\mathcal{P}(a)$$
$$\text{if and only if}$$
$$\text{for all } a_1, a_2 \in \mathcal{E},\ a \xrightarrow{*} a_1 \text{ and } a \xrightarrow{*} a_2 \text{ implies that } a_1 \text{ and } a_2 \text{ are joinable.}$$

All we have to do now is to show that $\mathcal{P}$ is $\longrightarrow$-complete. Let $a \in \mathcal{E}$ and let $\mathcal{P}(b)$ be true for all proper successors b of a. We have to prove that $\mathcal{P}(a)$ is true. Suppose $a \xrightarrow{*} a_1$ and $a \xrightarrow{*} a_2$. In case $a = a_1$ or $a = a_2$ there is nothing to show. Therefore, let us assume $a \neq a_1$ and $a \neq a_2$, i.e., $a \longrightarrow \tilde{a}_1 \xrightarrow{*} a_1$ and $a \longrightarrow \tilde{a}_2 \xrightarrow{*} a_2$. Then we can deduce the following figure

$$\begin{tikzcd}
 & & a \arrow[dl] \arrow[dr] & & \\
 & \tilde{a}_1 \arrow[dl, "*"'] \arrow[dr, "*"] & & \tilde{a}_2 \arrow[dl, "*"'] \arrow[dr, "*"] & \\
a_1 \arrow[dr, "*"] & & b_0 \arrow[dl, "*"'] & & a_2 \arrow[ddll, "*"'] \\
 & b_1 \arrow[dr, "*"] & & & \\
 & & b & &
\end{tikzcd}$$

where b_0 exists, as $(\mathcal{E}, \longrightarrow)$ is locally confluent and b_1 and b exist by our induction hypothesis since a_1, b_0 as well as a_2, b_1 are proper successors of a. Hence a_1 and a_2 must be joinable, i.e., the reduction system $(\mathcal{E}, \longrightarrow)$ is confluent.

q.e.d.

Therefore, if the reduction system is terminating, a check for confluence can be reduced to a check for local confluence. The concept of completion then is based on two steps:

1. Check the system for local confluence.
   If it is locally confluent, then it is also complete.

2. Add new relations arising from situations where the system is not locally confluent.

For many reduction systems, e.g. string rewriting systems or term rewriting systems, the check for local confluence again can be localized, often to finite test sets of so-called critical pairs. The relations arising from such critical situations are either confluent or give rise to new relations which stay within the congruence described by the reduction system. Hence adding them in order to increase the descriptive power of the reduction system is correct. This can be done until a complete set is reached. If fair strategies are used in the test for local confluence, the limit system will be complete.

We close this section by providing sufficient conditions to ensure a reduction system $(\mathcal{E}, \longrightarrow)$ to be Noetherian.

Definition 2.2.8
A binary relation $\succeq$ on a set M is said to be a **partial ordering**, if for all a, b, c in M:

1. $\succeq$ is reflexive, i.e., $a \succeq a$,
2. $\succeq$ is transitive, i.e., $a \succeq b$ and $b \succeq c$ imply $a \succeq c$, and
3. $\succeq$ is anti-symmetrical, i.e., $a \succeq b$ and $b \succeq a$ imply $a = b$. $\diamond$

A partial ordering is called **total**, if for all $a, b \in M$ either $a \succeq b$ or $b \succeq a$ holds. Further a partial ordering $\succeq$ defines a transitive irreflexive ordering $\succ$, where $a \succ b$ if and only if $a \succeq b$ and $a \neq b$, which is often called a **proper** or **strict** ordering. We call a partial ordering $\succeq$ **well-founded**, if the corresponding strict ordering $\succ$ allows no infinite descending chains $a_0 \succ a_1 \succ \ldots$, with $a_i \in M$, $i \in \mathbb{N}$. Now we can give a sufficient condition for a reduction system to be terminating.

Lemma 2.2.9
Let $(\mathcal{E}, \longrightarrow)$ be a reduction system and suppose there exists a partial ordering $\succeq$ on $\mathcal{E}$ which is well-founded such that $\longrightarrow \ \subseteq \ \succ$. Then $(\mathcal{E}, \longrightarrow)$ is Noetherian.

Proof :
Suppose the reduction system $(\mathcal{E}, \longrightarrow)$ is not Noetherian. Then there is an infinite sequence $a_0 \longrightarrow a_1 \longrightarrow \ldots$, $a_i \in \mathcal{E}$, $i \in \mathbb{N}$. As $\longrightarrow \subseteq \succ$ this sequence gives us an infinite sequence $a_0 \succ a_1 \succ \ldots$, with $a_i \in \mathcal{E}$, $i \in \mathbb{N}$ contradicting our assumption that $\succeq$ is well-founded on $\mathcal{E}$.

q.e.d.

2.3 Gröbner Bases in Polynomial Rings

The main interest in this section is the study of ideals in polynomial rings over fields. Let $\mathbb{K}[X_1, \ldots, X_n]$ denote a polynomial ring over the (ordered) variables $X_1, \ldots, X_n$ and the computable field $\mathbb{K}$. By $\mathcal{T} = \{X_1^{i_1} \ldots X_n^{i_n} \mid i_1, \ldots i_n \in \mathbb{N}\}$ we define the set of **terms** in this structure. A polynomial then is a formal sum $\sum_{i=1}^{n} \alpha_i \cdot t_i$ with non-zero coefficients $\alpha_i \in \mathbb{K}\backslash\{0\}$ and terms $t_i \in \mathcal{T}$. The products $\alpha \cdot t$ for $\alpha \in \mathbb{K}$, $t \in \mathcal{T}$ are called monomials and will often be denoted as $m = \alpha \cdot t$. We recall that a subset F of $\mathbb{K}[X_1, \ldots, X_n]$ generates an ideal $\mathsf{ideal}(F) = \{\sum_{i=1}^{k} f_i * g_i \mid k \in \mathbb{N}, f_i \in F, g_i \in \mathbb{K}[X_1, \ldots, X_n]\}$ and F is called a basis of this ideal. It was shown by Hilbert using non-constructive arguments that every ideal in $\mathbb{K}[X_1, \ldots, X_n]$ in fact has a finite basis, but such a generating set need not allow algorithmic solutions for the membership or congruence problem related to the ideal as we have seen in the introduction. It was Buchberger who developed a special type of basis, namely the Gröbner basis, which allows algorithmic solutions for several algebraic problems concerning ideals. He introduced a reduction relation to $\mathbb{K}[X_1, \ldots, X_n]$ by transforming polynomials into "rules" and gave a terminating procedure to "complete" an ideal basis interpreted as a reduction system. This procedure is called Buchberger's algorithm in the literature. We will give a sketch of his approach below.

Let $\succeq$ be a total well-founded ordering on the set of terms $\mathcal{T}$, which is admissible, i.e., $t \succeq 1$, and $s \succ t$ implies $s \circ u \succ t \circ u$ for all s, t, u in $\mathcal{T}$. The latter property is called compatibility with the multiplication $\circ$. In this context $\circ$ denotes the multiplication in $\mathcal{T}$, i.e., $X_1^{i_1} \ldots X_n^{i_n} \circ X_1^{j_1} \ldots X_n^{j_n} = X_1^{i_1+j_1} \ldots X_n^{i_n+j_n}$. With respect to this multiplication we say that a term $s = X_1^{i_1} \ldots X_n^{i_n}$ divides a term $t = X_1^{j_1} \ldots X_n^{j_n}$, if for all $1 \leq l \leq n$ we have $i_l \leq j_l$. The **least common multiple** $\mathsf{LCM}(s, t)$ of the terms s and t is the term $X_1^{\max\{i_1,j_1\}} \ldots X_n^{\max\{i_n,j_n\}}$. Note that $\mathcal{T}$ can be interpreted as the free commutative monoid generated by $X_1, \ldots, X_n$ with the same multiplication $\circ$ as defined above and identity $1 = X_1^0 \ldots X_n^0$ (recall Example 2.1.5). We proceed to give an example for a total well-founded admissible ordering on the set of terms $\mathcal{T}$.

Example 2.3.1
A **total degree ordering** $\succ$ on $\mathcal{T}$ is specified as follows: $X_1^{i_1} \ldots X_n^{i_n} \succ X_1^{j_1} \ldots X_n^{j_n}$ if and only if $\sum_{s=1}^{n} i_s > \sum_{s=1}^{n} j_s$ or $\sum_{s=1}^{n} i_s = \sum_{s=1}^{n} j_s$ and there exists k such that $i_k > j_k$ and $i_s = j_s, 1 \leq s < k$. $\diamond$

Henceforth, let $\succeq$ denote a total admissible ordering on $\mathcal{T}$ which is of course well-founded.

Definition 2.3.2
Let $p = \sum_{i=1}^{k} \alpha_i \cdot t_i$ be a non-zero polynomial in $\mathbb{K}[X_1, \ldots, X_n]$ such that $\alpha_i \in \mathbb{K}^* = \mathbb{K}\backslash\{0\}$, $t_i \in \mathcal{T}$ and $t_1 \succ \ldots \succ t_n$. Then we let $\mathsf{HM}(p) = \alpha_1 \cdot t_1$ denote the **head monomial**, $\mathsf{HT}(p) = t_1$ the **head term** and $\mathsf{HC}(p) = \alpha_1$ the **head**

coefficient of p. $\mathsf{RED}(p) = p - \mathsf{HM}(p)$ stands for the **reductum** of p. We call p **monic** in case $\mathsf{HC}(p) = 1$. These definitions can be extended to sets F of polynomials by setting $\mathsf{HT}(F) = \{\mathsf{HT}(f) \mid f \in F\}$, $\mathsf{HC}(F) = \{\mathsf{HC}(f) \mid f \in F\}$, respectively $\mathsf{HM}(F) = \{\mathsf{HM}(f) \mid f \in F\}$. $\diamond$

Using the notions of this definition we can recursively extend $\succeq$ from $\mathcal{T}$ to a partial well-founded admissible ordering $\geq$ on $\mathbb{K}[X_1, \ldots, X_n]$.

Definition 2.3.3
Let p, q be two polynomials in $\mathbb{K}[X_1, \ldots, X_n]$. Then we say p is **greater** than q with respect to a total well-founded admissible ordering $\succeq$ on $\mathcal{T}$, i.e., $p > q$, if

1. $\mathsf{HT}(p) \succ \mathsf{HT}(q)$ or
2. $\mathsf{HM}(p) = \mathsf{HM}(q)$ and $\mathsf{RED}(p) > \mathsf{RED}(q)$. $\diamond$

Now one first specialization of right ideal bases in terms of the representations they allow can be given according to standard representations as introduced e.g. in [BW92] for polynomial rings over fields.

Definition 2.3.4
Let F be a set of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ and g a non-zero polynomial in $\mathsf{ideal}(F) \subseteq \mathbb{K}[X_1, \ldots, X_n]$. A representations of the form

$$g \;=\; \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i = \alpha_i \cdot t_i, \alpha_i \in \mathbb{K}, t_i \in \mathcal{T}, n \in \mathbb{N} \qquad (2.1)$$

where additionally $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i \star m_i)$ holds for $1 \leq i \leq n$ is called a **standard representation** of g in terms of F. If every $g \in \mathsf{ideal}(F)\backslash\{0\}$ has such a representation in terms of F, then F is called a **standard basis** of $\mathsf{ideal}(F)$. $\diamond$

What distinguishes an arbitrary representation from a standard representation is the fact that the former may contain polynomial multiples with head terms larger than the head term of the represented polynomial. For example let $f_1 = X_1 + X_2$, $f_2 = X_1 + X_3$ and $F = \{f_1, f_2\}$ in $\mathbb{Q}[X_1, X_2]$ with $X_1 \succ X_2 \succ X_3$. Then for the polynomial $g = X_2 - X_3$ we have the representation $g = f_1 + (-1) \cdot f_2$ which is no standard one as $\mathsf{HT}(g) = X_2 \prec \mathsf{HT}(f_1) = \mathsf{HT}(f_2) = X_1$. Obviously the larger head terms have to vanish in the sum. Therefore, in order to change an arbitrary representation into one fulfilling our additional condition (2.1) we have to deal with special sums of polynomials related to such situations.

Definition 2.3.5
Let F be a set of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ and t an element in $\mathcal{T}$. Then we define the set of **critical situations** $\mathcal{C}(t, F)$ related to t and F to contain all tuples of the form $(t, f_1, \ldots, f_k, m_1, \ldots, m_k)$, $k \in \mathbb{N}$, $f_1, \ldots, f_k \in F$[4], $m_i = \alpha_i \cdot t_i$, such that

[4]Notice that $f_1, \ldots, f_k$ are not necessarily different polynomials from F.

1. $\mathsf{HT}(f_i \star m_i) = t$, $1 \leq i \leq k$, and
2. $\sum_{i=1}^{k} \mathsf{HM}(f_i \star m_i) = 0$.

We set $\mathcal{C}(F) = \bigcup_{t \in \mathcal{T}} \mathcal{C}(t, F)$. $\diamond$

In our example the tuple $(X_1, f_1, f_2, 1, -1)$ is an elements of the critical set $\mathcal{C}(X_1, F)$. We can characterize standard bases using these special sets.

Theorem 2.3.6
Let F be a set of polynomials in $\mathbb{K}[X_1, \ldots, X_n] \backslash \{0\}$. Then F is a standard basis of $\mathsf{ideal}(F)$ if and only if for every tuple $(t, f_1, \ldots, f_k, m_1, \ldots, m_k)$ in $\mathcal{C}(F)$ as specified in Definition 2.3.5 the polynomial $\sum_{i=1}^{k} f_i \star m_i$ has a standard representation with respect to F.

Proof :
In case F is a standard basis since these polynomials are all elements of $\mathsf{ideal}(F)$ they must have standard representations with respect to F.
To prove the converse, it remains to show that every element in $\mathsf{ideal}(F)$ has a standard representation with respect to F. Hence, let $g = \sum_{j=1}^{m} f_j \star m_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}(F)$ such that $f_j \in F$, and $m_j = \alpha_j \cdot t_j$ with $\alpha_j \in \mathbb{K}$, $t_j \in \mathcal{T}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star t_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star t_j$ with head term t. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that this representation is already a standard representation. Else we proceed by induction on the term t. Without loss of generality let $f_1, \ldots, f_K$ be the polynomials in the corresponding representation such that $t = \mathsf{HT}(f_i \star t_i)$, $1 \leq i \leq K$. Then the tuple $(t, f_1, \ldots, f_K, m_1, \ldots, m_K)$ is in $\mathcal{C}(F)$ and let $h = \sum_{i=1}^{K} f_i \star m_i$. We will now change our representation of g in such a way that for the new representation of g we have a smaller maximal term. Let us assume h is not 0[5]. By our assumption, h has a standard representation with respect to F, say $\sum_{j=1}^{n} h_j \star n_j$, where $h_j \in F$, and $n_j = \beta_j \cdot s_j$ with $\beta_j \in \mathbb{K}$, $s_j \in \mathcal{T}$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$ as $\sum_{i=1}^{K} \mathsf{HM}(f_i \star m_i) = 0$. This gives us:

$$\begin{aligned} g &= \sum_{i=1}^{K} f_i \star m_i + \sum_{i=K+1}^{m} f_i \star m_i \\ &= \sum_{j=1}^{n} h_j \star n_j + \sum_{i=K+1}^{m} f_i \star m_i \end{aligned}$$

[5] In case $h = 0$, just substitute the empty sum for the representation of h in the equations below.

which is a representation of g where the maximal term is smaller than t.

q.e.d.

In fact for the case of polynomial rings over fields one can show that it is sufficient to consider critical sets for subsets of F of size 2 and we can restrict the terms to the least common multiples of the head terms of the respective two polynomials. These sets then correspond to the concept of s-polynomials used to characterize Gröbner bases which will be introduced later on.

Reviewing our example on page 22 we find that the set $F = \{X_1+X_2, X_1+X_3\}$ is no standard basis as the polynomial $g = X_2 - X_3$ has no standard representation although it is an elements of $\mathsf{ideal}(F)$. However the set $F \cup \{g\}$ then is a standard basis of $\mathsf{ideal}(F)$.

In the literature standard representations in $\mathbb{K}[X_1, \ldots, X_n]$ are closely related to reduction relations based on the divisibility of terms and standard bases are in fact Gröbner bases. Here we want to introduce Gröbner bases in terms of rewriting. Hence we continue by introducing the concept of reduction to $\mathbb{K}[X_1, \ldots, X_n]$.

We can split a non-zero polynomial p into a **rule** $\mathsf{HM}(p) \longrightarrow -\mathsf{RED}(p)$ and we have $\mathsf{HM}(p) > -\mathsf{RED}(p)$. Therefore, a set of polynomials gives us a binary relation $\longrightarrow$ on $\mathbb{K}[X_1, \ldots, X_n]$ which induces a one-step reduction relation as follows.

Definition 2.3.7
Let p, f be two polynomials in $\mathbb{K}[X_1, \ldots, X_n]$. We say f **reduces** p to q at a monomial $m = \alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{b}}_{f} q$, if

(a) $\mathsf{HT}(f) \circ u = t$ for some $u \in \mathcal{T}$, i.e., $\mathsf{HT}(f)$ divides t, and

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

We write $p \longrightarrow^{\mathrm{b}}_{f}$ if there is a polynomial q as defined above and p is then called reducible by f. Further, we can define $\xrightarrow{*}^{\mathrm{b}}$, $\xrightarrow{+}^{\mathrm{b}}$, and $\xrightarrow{n}^{\mathrm{b}}$ as usual. Reduction by a set $F \subseteq \mathbb{K}[X_1, \ldots, X_n]$ is denoted by $p \longrightarrow^{\mathrm{b}}_{F} q$ and abbreviates $p \longrightarrow^{\mathrm{b}}_{f} q$ for some $f \in F$, which is also written as $p \longrightarrow^{\mathrm{b}}_{f \in F} q$. $\diamond$

Note that if f **reduces** p to q at a monomial $m = \alpha \cdot t$ then t is no longer among the terms of q. We call a set of polynomials $F \subseteq \mathbb{K}[X_1, \ldots, X_n]$ **interreduced**, if no $f \in F$ is reducible by a polynomial in $F \backslash \{f\}$.

In the classical case of polynomial rings over fields the existence of a standard representation for a polynomial immediately implies reducibility of the head monomial of the polynomial by any reduction relation based on divisibility of terms, hence by the reduction relation defined here. This is due to the fact that if a polynomial g has a standard representation in terms of a set of polynomials F for at least one polynomial f in F and some term t in $\mathcal{T}$ we have

$\mathsf{HT}(g) = \mathsf{HT}(f \star t) = \mathsf{HT}(f) \circ t$ and hence g is reducible at the monomial $\mathsf{HM}(g)$ by f. Notice that this is no longer true for polynomial rings over the integers. Let $F = \{3 \cdot X^2 + X, 2 \cdot X^2 + X\}$ be a subset of $\mathbb{Z}[X]$. Then the polynomial $g = (3 \cdot X^2 + X) - (2 \cdot X^2 + X) = X^2$ has a standard representation in terms of F but neither $3 \cdot X^2$ nor $2 \cdot X^2$ are divisors of the monomial X^2 as neither 3 nor 2 devide 1 in $\mathbb{Z}$.

Notice that we have $\longrightarrow \subseteq\ >$ and indeed one can show that our reduction relation on $\mathbb{K}[X_1, \ldots, X_n]$ is Noetherian. Therefore, we can restrict ourselves to ensuring local confluence when describing a completion procedure to compute Gröbner bases later on. But first we have to provide a definition of Gröbner bases in the context of rewriting.

Definition 2.3.8
A set $G \subseteq \mathbb{K}[X_1, \ldots, X_n]$ is said to be a **Gröbner basis** of the ideal it generates, if

1. $\overset{*}{\longleftrightarrow}{}^{\mathrm{b}}_{G} \; = \; \equiv_{\mathsf{ideal}(G)}$, and
2. $\longrightarrow^{\mathrm{b}}_{G}$ is confluent. ◇

The first statement expresses that the reduction relation describes the ideal congruence. It holds for any basis of an ideal in $\mathbb{K}[X_1, \ldots, X_n]$ and is hence normally omitted in the definitions provided in the literature. However, when generalizing the concept of Gröbner bases to other structures it is no longer guaranteed and hence we have included it in our definition. The second statement ensures the existence of unique normal forms. If we additionally require a Gröbner basis to be interreduced, such a basis is unique in case we assume that the polynomials are monic, i.e., their head coefficients are 1. The following lemma gives some properties of the reduction relation, which are essential in giving a constructive description of a Gröbner basis not only in the setting of commutative polynomial rings over fields.

Lemma 2.3.9
Let F be a set of polynomials and p, q, h some polynomials in $\mathbb{K}[X_1, \ldots, X_n]$. Then the following statements hold:

1. *Let $p - q \longrightarrow^{\mathrm{b}}_{F} h$. Then there are polynomials $p', q' \in \mathbb{K}[X_1, \ldots, X_n]$ such that $p \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{F} p'$, $q \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{F} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to F. Then there exists a polynomial $g \in \mathbb{K}[X_1, \ldots, X_n]$ such that $p \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{F} g$ and $q \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{F} g$.*
3. *$p \overset{*}{\longleftrightarrow}{}^{\mathrm{b}}_{F} q$ if and only if $p - q \in \mathsf{ideal}(F)$.*
4. *$p \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{F} 0$ implies $\alpha \cdot p * u \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{F} 0$ for all $\alpha \in \mathbb{K}$ and $u \in \mathcal{T}$.*

5. *$\alpha \cdot p * u \longrightarrow^{\mathrm{b}}_{p} 0$ for all $\alpha \in \mathbb{K}^*$ and $u \in \mathcal{T}$.*

The second statement of this lemma is often called the **Translation Lemma** in the literature. Statement 3 shows that Buchberger's reduction relation always captures the ideal congruence. Statement 4 is connected to the important fact that reduction steps are preserved under multiplication with monomials.

The set $F = \{X_1 + X_2, X_1 + X_3\}$ of polynomials in $\mathbb{Q}[X_1, X_2, X_3]$ from page 22 is an example of an ideal basis which is not complete, i.e. the reduction relation is not complete[6]. This follows as the polynomial X_1 can be reduced by $\longrightarrow^{\mathrm{b}}_{F}$ to $-X_2$ as well as to $-X_3$ and the latter two polynomials cannot be joined using $\longrightarrow^{\mathrm{b}}_{F}$.

Of course we cannot expect an arbitrary ideal basis to be complete. But Buchberger was able to show that in order to "complete" a given basis one only has to add finitely many special polynomials which arise from critical situations as described in the context of reduction systems in the previous section and Definition 2.3.5.

The term X_1 in our example describes such a critical situation which is in fact the only one relevant for completing the set F.

Definition 2.3.10
The **s-polynomial** for two non-zero polynomials $p, q \in \mathbb{K}[X_1, \ldots, X_n]$ is defined as

$$\mathsf{spol}(p, q) = \mathsf{HC}(p)^{-1} \cdot p * u - \mathsf{HC}(q)^{-1} \cdot q * v,$$

where $\mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)) = \mathsf{HT}(p) \circ u = \mathsf{HT}(q) \circ v$ for some $u, v \in \mathcal{T}$. $\diamond$

An s-polynomial will be called **non-trivial** in case it is not zero and notice that for non-trivial s-polynomials we always have $\mathsf{HT}(\mathsf{spol}(p, q)) \prec \mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q))$. The s-polynomial for p and q belongs to the set of critical situations $\mathcal{C}(\mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)), \{p, q\})$.

In our example we find $\mathsf{spol}(X_1 + X_2, X_1 + X_3) = X_1 + X_2 - (X_1 + X_3) = X_2 - X_3$.

Why are s-polynomials related to testing for local confluence? To answer this question we have to look at critical situations related to the reduction relation as defined in Definition 2.3.7. Given two polynomials $p, q \in \mathbb{K}[X_1, \ldots, X_n]$ the smallest situation where both of them can be applied as rules is the least common multiple of their head terms. Let $\mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)) = \mathsf{HT}(p) \circ u = \mathsf{HT}(q) \circ v = t$ for some $u, v \in \mathcal{T}$. This gives us the following situation:

$$\begin{tikzcd}
 & \mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)) = t \arrow[dl, "q"'] \arrow[dr, "p"] & \\
\begin{array}{c} t - \mathsf{HC}(q)^{-1} \cdot q * v \\ = p' \end{array} & & \begin{array}{c} t - \mathsf{HC}(p)^{-1} \cdot p * u \\ = q' \end{array}
\end{tikzcd}$$

[6]Note that we call a set of polynomials complete (confluent, etc.) if the reduction relation induced by these polynomials used as rules is complete (confluent, etc.).

Then we get $p' - q' = t - \mathsf{HC}(q)^{-1} \cdot q * v - (t - \mathsf{HC}(p)^{-1} \cdot p * u) = \mathsf{HC}(p)^{-1} \cdot p * u - \mathsf{HC}(q)^{-1} \cdot q * v = \mathsf{spol}(p, q)$, i.e., the s-polynomial is derived from the two one-step successors by subtraction. Now by Lemma 2.3.9 we know that $\mathsf{spol}(p, q) \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ implies the existence of a common normal form for the polynomials p' and q'. Since the reduction relation based on Definition 2.3.7 is terminating, the confluence test can hence be reduced to checking whether all s-polynomials reduce to zero. The following theorem now gives a constructive characterization of Gröbner bases based on these ideas.

Theorem 2.3.11
For a set of polynomials F in $\mathbb{K}[X_1, \ldots, X_n]$, the following statements are equivalent:

1. *F is a Gröbner basis.*
2. *For all polynomials $g \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$.*
3. *For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$.*

Proof :
$1 \Longrightarrow 2$: Let F be a Gröbner basis and $g \in \mathsf{ideal}(F)$. Then g is congruent to 0 modulo the ideal generated by F, i.e., $g \xleftrightarrow{*}{}^{\mathrm{b}}_{F} 0$. Thus, as 0 is irreducible and G is confluent, we get $g \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$.
$2 \Longrightarrow 1$: By Lemma 2.3.9 3 we know $\xleftrightarrow{*}{}^{\mathrm{b}}_{G} \; = \; \equiv_{\mathsf{ideal}(G)}$. Hence it remains to show that reduction with respect to F is confluent. Since our reduction is terminating it is sufficient to show local confluence. Thus, suppose there are three different polynomials g, h_1, h_2 such that $g \longrightarrow^{\mathrm{b}}_{F} h_1$ and $g \longrightarrow^{\mathrm{b}}_{F} h_2$. Then we know $h_1 \equiv_{\mathsf{ideal}(F)} g \equiv_{\mathsf{ideal}(F)} h_2$ and hence $h_1 - h_2 \in \mathsf{ideal}(F)$. Now by lemma 2.3.9 (the translation lemma), $h_1 - h_2 \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ implies the existence of a polynomial $h \in \mathbb{K}[X_1, \ldots, X_n]$ such that $h_1 \xrightarrow{*}{}^{\mathrm{b}}_{F} h$ and $h_2 \xrightarrow{*}{}^{\mathrm{b}}_{F} h$. Hence, h_1 and h_2 are joinable.
$2 \Longrightarrow 3$: By definition 2.3.10 the s-polynomial for two non-zero polynomials $f_k, f_l \in \mathbb{K}[X_1, \ldots, X_n]$ is defined as

$$\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * u - \mathsf{HC}(f_l)^{-1} \cdot f_l * v,$$

where $\mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)) = \mathsf{HT}(p) \circ u = \mathsf{HT}(q) \circ v$ and, hence, $\mathsf{spol}(f_k, f_l) \in \mathsf{ideal}(F)$. Therefore, $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ follows immediately.
$3 \Longrightarrow 2$: We have to show that every $g \in \mathsf{ideal}(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{b}}_{F}$-reducible to zero. Remember that for $h \in \mathsf{ideal}(F)$, $h \longrightarrow^{\mathrm{b}}_{F} h'$ implies $h' \in \mathsf{ideal}(F)$. As $\longrightarrow^{\mathrm{b}}_{F}$ is Noetherian, thus it suffices to show that every $g \in \mathsf{ideal}(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{b}}_{F}$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be an arbitrary representation of g with $\alpha_j \in \mathbb{K}^*$, $f_j \in F$, and $w_j \in \mathcal{T}$. Depending on this representation of g and a total well-founded admissible ordering $\succeq$ on $\mathcal{T}$ we define

$t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \ldots, m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{b}}_{F}$-reducible. Thus we will prove that g has a representation where every occurring term is less or equal to $\mathsf{HT}(g)$, i.e., there exists a representation such that $t = \mathsf{HT}(g)$[7]. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[8]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[9] such that $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l = t$. By definition 2.3.10 we have an s-polynomial $\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * z_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * z_l$ such that $\mathsf{HT}(f_k) \circ z_k = \mathsf{HT}(f_l) \circ z_l = \mathsf{LCM}(\mathsf{HT}(f_k), \mathsf{HT}(f_l))$. Since $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l$ there exists an element $z \in \mathcal{T}$ such that $w_k = z_k \circ z$ and $w_l = z_l \circ z$. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume that $\mathsf{spol}(f_k, f_l)$ is not trivial[10]. Then the reduction sequence $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ results in a representation of the form $\mathsf{spol}(f_k, f_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbb{K}^*, h_i \in F, v_i \in \mathcal{T}$. As the h_i are due to the reduction of the s-polynomial, all terms occurring in the sum are bounded by the term $\mathsf{HT}(\mathsf{spol}(f_k, f_l))$. Moreover, since $\succeq$ is admissible on $\mathcal{T}$ this implies that all terms of the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * z$ are bounded by $\mathsf{HT}(\mathsf{spol}(f_k, f_l)) \circ z \prec t$, i.e., they are strictly bounded by t[11]. We can now do the following transformations:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \quad & \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \quad & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}(f_k, f_l) * z} \\
= \quad & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * (v_i \circ z)) \qquad (2.2)
\end{aligned}$$

where, $\beta_k = \mathsf{HC}(f_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l)^{-1}$, and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (2.2) in our representation of g either t disappears or K is decreased.

q.e.d.

[7]Such representations are often called standard representations in the literature (compare [BW92]).

[8]Note that this ordering is well-founded since $\succ$ is well-founded on $\mathcal{T}$ and $K \in \mathbb{N}$.

[9]Not necessarily $f_l \neq f_k$.

[10]In case $\mathsf{spol}(f_k, f_l) = 0$, just substitute 0 for the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i$ in the equations below.

[11]This can also be concluded by statement four of lemma 2.3.9 since $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ implies $\mathsf{spol}(f_k, f_l) * z \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ and $\mathsf{HT}(\mathsf{spol}(f_k, f_l) * z) \prec t$.

The second item of this theorem immediately implies the correctness of the algebraic definition of Gröbner bases, which is equivalent to Definition 2.3.8.

Definition 2.3.12
A set G of polynomials in $\mathbb{K}[X_1, \ldots, X_n] \backslash \{0\}$ is said to be a **Gröbner basis**, if $\mathsf{HT}(\mathsf{ideal}(G)) = \{\mathsf{HT}(g) * t \mid g \in G, t \in \mathcal{T}\}$. $\diamond$

Remark 2.3.13
A closer inspection of the proof of $3 \Longrightarrow 2$ given above reveals a concept which is essential in the proofs of similar theorems for specific function rings in the following chapters. The heart of this proof consists in transforming an arbitrary representation of an element g belonging to the ideal generated by the set F in such a way that we can deduce a top reduction sequence for g to zero, i.e., a reduction sequence where the reductions only take place at the respective head term. Such a representation of g then is a standard representation and Gröbner bases are standard bases. $\diamond$

As a consequence of Theorem 2.3.11 it is decidable whether a finite set of polynomials is a Gröbner basis. Moreover, this theorem gives rise to the following completion procedure for sets of polynomials.

Procedure: BUCHBERGER'S ALGORITHM

Given: A finite set of polynomials $F \subseteq \mathbb{K}[X_1, \ldots, X_n]$.
Find: $\mathrm{GB}(F)$, a Gröbner basis of F.

$G := F$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do**
    $(q_1, q_2) := \mathrm{remove}(B)$;
    % Remove an element from the set B
    $h := \mathrm{normalform}(\mathsf{spol}(q_1, q_2), \xrightarrow{\mathrm{b}}_G)$
    % Compute a normal form of $\mathsf{spol}(q_1, q_2)$ with respect to $\xrightarrow{\mathrm{b}}_G$
    if $h \neq 0$
        then $B := B \cup \{(f, h) \mid f \in G\}$;
            $G := G \cup \{h\}$;
    endif
endwhile
$\mathrm{GB}(F) := G$

Applying this procedure to our example $F = \{X_1 + X_2, X_1 + X_3\}$ from page 22 gives us $h = X_2 - X_3$ and $G = F \cup \{h\}$ is a Gröbner basis as all other critical situations are resolvable.

Termination of the procedure can be shown by using a slightly different characterization of Gröbner bases (see Section 1.2): A subset G of $\mathsf{ideal}^{\mathbb{K}[X_1,\ldots,X_n]}(F)$ is a Gröbner basis of $\mathsf{ideal}^{\mathbb{K}[X_1,\ldots,X_n]}(F)$ if and only if $\mathsf{HT}(\mathsf{ideal}^{\mathbb{K}[X_1,\ldots,X_n]}(F)\backslash\{0\}) = \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G))$, i.e., the set of the head terms of the polynomials in the ideal generated by F in $\mathbb{K}[X_1,\ldots,X_n]$ coincides with the ideal (in $\mathcal{T}$) generated by the head terms of the polynomials in G. Reviewing the procedure, we find that every polynomial added in the **while** loop has the property that its head term cannot be divided by the head terms of the polynomials already in G. By Dickson's Lemma or Hilbert's Basis Theorem, the head terms of the polynomials in G will at some step form a basis for the set of head terms of the polynomials of the ideal generated by F which itself is the ideal in $\mathcal{T}$ generated by the head terms of the polynomials in G. From this time on for every new polynomial h computed by the algorithm the head term $\mathsf{HT}(h)$ must lie in this ideal. Therefore, its head term must be divisible by at least one of the head terms of the polynomials in G, i.e., $\mathsf{HT}(h)$ and hence h cannot be in normal form with respect to G unless it is zero.

Chapter 3

Reduction Rings

In this chapter we proceed to distinguish sufficient conditions, which allow 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, 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 $\mathbb{Z}$ are 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 $\mathbb{Z}[X_1, \ldots, X_n]$ is a reduction ring. Similarly, as sums of reduction rings are again reduction rings, we can directly conclude that $\mathbb{Z}^k[X_1, \ldots, X_n]$ or even $(\mathbb{Z}[Y_1, \ldots, Y_m])^k[X_1, \ldots, X_n]$ 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, Madlener, and Stifter in [Buc83, Mad86, Sti87].

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 in [Pes97].

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 [MR98b]. Here we extend this framework by giving more details and insight. Additionally, we add a section on modules over reduction rings, as this concept arises naturally as a generalization of ideals in rings.

Of course there are also rings of interest, which can be enriched by a reduction relation, but will not allow finite Gröbner bases for all ideals. Monoid and group rings provide such a setting. For such structures still many of the properties studied here are of interest and can be shown in weaker forms, e.g. provided a monoid ring with a reduction relation we can define a reduction relation for the polynomial ring with one variable over the monoid ring.

The chapter is organized as follows: In Section 3.1 we introduce axioms for specifying reduction relations in rings and give two concepts involving special forms of ideal bases – weak reduction rings and reduction rings. In Section 3.2 – 3.5 we study quotients, sums, modules, and polynomial rings of these structures.

3.1 Reduction Rings

Let R be a ring with unit 1 and a (not necessarily effective) reduction relation $\Longrightarrow_B \subseteq \mathsf{R} \times \mathsf{R}$ 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 $\alpha \in \mathsf{R}\backslash\{0\}$.

Part one of Axiom (A1) states how a reduction relation using sets is defined in terms of a reduction relation using elements of R and is hence applicable to arbitrary sets $B \subseteq \mathsf{R}$. However, Axiom (A1) does *not* imply termination of reduction with respect to arbitrary sets: Just assume 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 $X_1 \succ X_2 \succ \ldots$. Then although reduction when using a finite set of polynomials is terminating, this is no longer true for infinite sets. For example the infinite set $\{X_i - X_{i+1} \mid i \in \mathbb{N}\}$ gives rise to an infinite reduction sequence $X_1 \Longrightarrow_{X_1 - X_2} X_2 \Longrightarrow_{X_2 - X_3} X_3 \ldots$. This phenomenon of course has many consequences. Readers familiar with Gröbner bases in polynomial rings know that when proving that a set of polynomials is a Gröbner basis if and only if all ideal elements reduce to zero using the set, this is shown by proving that every ideal element is reducible by some element in the set (compare Theorem 2.3.11). Unfortunately, this only implies reducibility to zero in case the reduction relation is terminating. Without this property other methods have to be applied.

In order to ensure termination for arbitrary subsets of R 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 sequences are always terminating and many additional restrictions, which we have to add later, are no longer necessary. Still we prefer the more general formulation of the axiom since it allows to state more clearly why and where termination is needed and how it can be achieved.

Axiom (A2) states how reduction steps are related to the ideal congruence, namely that 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 $\stackrel{*}{\Longleftrightarrow}_B$ 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 ρ in 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 $\rho_{i1}, \rho_{i2} \in \mathsf{R}$, $1 \leq i \leq k$, hence possibly 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 on the converse Axiom (A2) does *not* provide any information on how $\alpha, \gamma \in \mathsf{R}$ with $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\beta)$ are related with respect to the reduction relation $\Longrightarrow_{\{\beta\}}$. As a consequence many properties of specialized reduction relations as known from the literature, e.g. the useful Translation Lemma, cannot be shown to hold in this general setting.

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

(A2r) $\alpha \Longrightarrow_\beta \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}_r^{\mathsf{R}}(\beta)$, respectively

(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 a set $B \subseteq \mathsf{R}$ and let $\equiv_{\mathfrak{i}}$ denote the congruence generated by the ideal $\mathfrak{i} = \mathsf{ideal}(B)$, i.e., $\alpha \equiv_{\mathfrak{i}} \beta$ if and only if $\alpha - \beta \in \mathfrak{i}$. Then (A1)[1] and (A2) immediately imply $\stackrel{*}{\Longleftrightarrow}_B \subseteq \equiv_{\mathfrak{i}}$. 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'

[1]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.

still generates $\mathfrak{i}$ and $\Longrightarrow_{B'}$ is confluent on $\mathfrak{i}$. Notice that 0 has to be irreducible[2] for all $\Longrightarrow_\alpha$, $\alpha \in \mathsf{R}$. Therefore, 0 has to be *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 in [Pan85] does not have this property but is still sufficient to decide $\equiv_\mathfrak{i}$-equivalence of two elements because $\alpha \equiv_\mathfrak{i} \beta$ if and 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. This phenomenon is illustrated in the next example.

Example 3.1.1
Let us look at different ways of introducing reduction relations for the ring of integers $\mathbb{Z}$. For $\alpha, \beta, \gamma \in \mathbb{Z}$ we define:

- $\alpha \Longrightarrow_\beta \gamma$ if and only if $\alpha = \kappa \cdot |\beta| + \gamma$ where $0 \leq \gamma < |\beta|$ and $\kappa \in \mathbb{Z}$ (division with remainder),
- $\alpha \Longrightarrow^{\mathrm{D}}_\beta 0$ if and only if $\alpha = \kappa \cdot \beta$, i.e. β is a proper divisor of α (D-reduction).

Then for example we have $5 \Longrightarrow_4 1$ but $5 \not\Longrightarrow^{\mathrm{D}}_4$.
It is easy to show that both reduction relations satisfy (A1) – (A3). Moreover, all 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 $\Longrightarrow$-reduction the normal forms are unique representatives of the quotient $\mathbb{Z}/\mathsf{ideal}(4)$. This is no longer true for $\Longrightarrow^D$-reduction, since e.g. $3 \equiv_{\mathsf{ideal}(4)} 7$ since $7 = 3 + 4$, but both are $\Longrightarrow^D$-irreducible. On the other hand, as $\Longrightarrow^D_\alpha$ is only applicable to multiples $\kappa \cdot \alpha$ and then reduces them to zero, $\Longrightarrow^D_4$ is confluent everywhere on $\mathbb{Z}$. ⋄

Since confluence of a reduction relation on the ideal is already sufficient to solve its membership problem, bases with this property called weak Gröbner bases have been studied in the literature. We proceed here by defining such weak Gröbner bases in our context.

Definition 3.1.2
A subset B of R is called a **weak Gröbner basis** of the ideal $\mathfrak{i} = \mathsf{ideal}(B)$ it generates, if $\Longrightarrow_B$ is terminating and $\alpha \overset{*}{\Longrightarrow}_B 0$ for all $\alpha \in \mathfrak{i}$. ⋄

Notice that in Theorem 2.3.11 this property was one way of characterizing Gröbner bases in $\mathbb{K}[X_1, \ldots, X_n]$. We will later on see why in polynomial rings the terms weak Gröbner basis and Gröbner basis coincide.

[2] 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).

Definition 3.1.3
A ring $(\mathsf{R}, \Longrightarrow)$ satisfying (A1) – (A3) is called a **weak reduction ring** if every finitely generated ideal in R has a finite weak Gröbner basis. $\diamond$

As stated before such a weak Gröbner basis is sufficient to decide the ideal membership problem in case the reduction relation is effective. However, if we want unique normal forms for *all* elements in R such that each congruence has one unique representative we need a stronger kind of ideal basis.

Definition 3.1.4
A subset B of R is called a **Gröbner basis** of the ideal $\mathfrak{i} = \mathsf{ideal}(B)$ it generates, if $\stackrel{*}{\Longleftrightarrow}_B \; = \; \equiv_{\mathfrak{i}}$ and $\Longrightarrow_B$ is complete[3]. $\diamond$

Of course Gröbner bases are also weak Gröbner bases. This can be shown by induction on k, where for $\alpha \in \mathsf{ideal}(B)$ we have $\alpha \stackrel{k}{\Longleftrightarrow}_B 0$. In case $k = 1$ we immediately get that $\alpha \Longrightarrow_B 0$ must hold as 0 is irreducible. In case $k > 1$ we find $\alpha \Longleftrightarrow_B \beta \stackrel{k-1}{\Longleftrightarrow}_B 0$ and by our induction hypothesis $\beta \stackrel{*}{\Longrightarrow}_B 0$ must hold. Now either $\alpha \Longrightarrow_B \beta$ and we are done or $\beta \Longrightarrow_B \alpha$. In the latter case the completeness of our reduction relation combined with the irreducibility of zero then must yield $\alpha \stackrel{*}{\Longrightarrow}_B 0$ and we are done.

The converse is not true. To see this let us review the definition of $\Longrightarrow^D$-reduction for $\mathbb{Z}$ as presented in Example 3.1.1. Then the set $\{2\}$ is a weak Gröbner basis of the ideal $2 \cdot \mathbb{Z} = \{2 \cdot \alpha \mid \alpha \in \mathbb{Z}\}$ as for every $\alpha \in (2 \cdot \mathbb{Z}) \backslash \{0\}$ we have $\alpha \Longrightarrow^D_{\{2\}} 0$. On the other hand elements in $\mathbb{Z} \backslash (2 \cdot \mathbb{Z})$ are irreducible and hence 3 and 5 are in normal form with respect to $\Longrightarrow^D_{\{2\}}$. Therefore, $3 \stackrel{*}{\not\Longleftrightarrow}{}^{\mathrm{D}}_{\{2\}} 5$ although $5 \equiv_{2 \cdot \mathbb{Z}} 3$ as $5 = 3 + 1 \cdot 2$.

However, for many rings as e.g. polynomial rings over fields, weak Gröbner bases are also Gröbner bases. This is due to the fact that many rings with reduction relations studied in the literature fulfill a certain property for the reduction relation called the Translation Lemma (compare Lemma 2.3.9 (2)). Rephrased in our context the Translation Lemma states that for a set $F \subseteq \mathsf{R}$ and for all $\alpha, \beta \in \mathsf{R}$, $\alpha - \beta \stackrel{*}{\Longrightarrow}_F 0$ implies the existence of $\gamma \in \mathsf{R}$ such that $\alpha \stackrel{*}{\Longrightarrow}_F \gamma$ and $\beta \stackrel{*}{\Longrightarrow}_F \gamma$. As mentioned before, the validity of this lemma for a reduction relation in a ring has consequences on the relation between weak Gröbner bases and Gröbner bases.

[3] Notice that in the literature definitions of Gröbner bases normally only 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 completeness. Hence here we have a point where the weaker form (A1) demands more care in defining the term "Gröbner basis". In rings where the reduction relation using an arbitrary set of elements is always Noetherian, the weaker demand for (local) confluence is of course sufficient.

Theorem 3.1.5
Let R be a ring with a reduction relation $\Longrightarrow$ fulfilling (A1) – (A3). If additionally the Translation Lemma holds for the reduction relation $\Longrightarrow$ in R, then weak Gröbner bases are also Gröbner bases.

Proof :
Let R be a ring where the Translation Lemma holds for the reduction relation $\Longrightarrow$. Further let B be a weak Gröbner basis of the ideal $\mathfrak{i} = \mathsf{ideal}(B)$. In order to prove that B is in fact a Gröbner basis we have to show two properties:

1. $\overset{*}{\Longleftrightarrow}_B \; = \; \equiv_{\mathfrak{i}}$:
   The inclusion $\overset{*}{\Longleftrightarrow}_B \subseteq \equiv_{\mathfrak{i}}$ follows by (A1) and (A2). To see the converse let $\alpha \equiv_{\mathfrak{i}} \beta$. Then $\alpha - \beta \in \mathfrak{i}$, and $\alpha - \beta \overset{*}{\Longrightarrow}_B 0$, as B is a weak Gröbner basis. But then the Translation Lemma yields that α and β are joinable by $\Longrightarrow_B$ and hence $\alpha \overset{*}{\Longleftrightarrow}_B \beta$.

2. $\Longrightarrow_B$ is complete:
   Since $\Longrightarrow_B$ is terminating it suffices to show local confluence. Let $\alpha, \beta_1, \beta_2 \in \mathsf{R}$ such that $\alpha \Longrightarrow_B \beta_1$ and $\alpha \Longrightarrow_B \beta_2$. Then again $\beta_1 - \beta_2 \in \mathfrak{i}$, and $\beta_1 - \beta_2 \overset{*}{\Longrightarrow}_B 0$, since B is a weak Gröbner basis. As before the Translation Lemma yields that β_1 and β_2 are joinable by $\Longrightarrow_B$ and we are done.

q.e.d.

On the other hand, looking at proofs of variations of the Translation Lemma in the literature we find that in order to show this property for a ring with a reduction relation we need more information on the reduction step as is provided by the very general form of Axiom (A2). Hence in this general setting weak Gröbner bases and Gröbner bases have to be distinguished.

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

Definition 3.1.6
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. $\diamond$

The connection between weak reduction rings and reduction rings follows from Theorem 3.1.5.

Corollary 3.1.7
Let $(\mathsf{R}, \Longrightarrow)$ be a weak reduction ring. If additionally the Translation Lemma holds, then $(\mathsf{R}, \Longrightarrow)$ is a reduction ring.

To simplify notations sometimes we will identify $(\mathsf{R}, \Longrightarrow)$ with R in case $\Longrightarrow$ is known or irrelevant. The notion of **one-sided weak reduction rings** and **one-sided reduction rings** is straightforward[4].

Effective or **computable weak reduction rings** and **effective** or **computable reduction rings** can be defined similar to Buchberger's commutative reduction rings (see [Buc83, Sti87]), in our case by demanding that the ring operations are computable, the reduction relation is effective, and, additionally, Gröbner bases can be computed. Procedures which compute Gröbner bases are normally completion procedures based on effective tests for local confluence to decide whether a finite set is a Gröbner basis and to enrich that set if not. But of course other procedures are also possible, e.g. when using division with remainders as reduction relation in $\mathbb{Z}$ the Euclidean algorithm can be used for computing Gröbner bases of ideals.

Notice that Definition 3.1.6 does not imply that Noetherian rings satisfying the Axioms (A1), (A2) and (A3) are indeed reduction rings. This is due to the fact that while of course all ideals then have finite bases, the property of being a Gröbner basis strongly depends on the reduction ring which is of course itself strongly dependent on the reduction relation chosen for the ring. Hence the existence of finite ideal bases does not imply the existence of finite Gröbner bases as the following example shows: Given an arbitrary Noetherian ring R we can associate a (very simple) reduction relation to elements of R by defining for any $\alpha \in \mathsf{R}\backslash\{0\}$, $\alpha \Longrightarrow_{\beta}$ 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, as for any ideal $\mathfrak{i} \subseteq \mathsf{R}$ in this setting the set $\mathfrak{i}\backslash\{0\}$ is the only possible Gröbner basis.

Another interesting question concerns which changes to ideal bases preserve the property of being a Gröbner basis. Extensions of (weak) Gröbner bases by ideal elements are not critical[5].

Remark 3.1.8
If B is a finite (weak) Gröbner basis of $\mathfrak{i}$ and $\alpha \in \mathfrak{i}$, then $B' = B \cup \{\alpha\}$ is again a (weak) 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 hence β and γ have the same normal form with respect to $\Longrightarrow_B$. $\diamond$

[4] An example for a one-sided weak reduction ring which is not a one-sided reduction ring can be given using the two different reduction relations $\Longrightarrow$ and $\Longrightarrow^{\mathrm{D}}$ for the integers provided in Example 3.1.1. Then the free monoid ring $\mathbb{Z}[\{a, b\}]$ with prefix reduction induced by $\Longrightarrow$ is a one-sided reduction ring while for prefix reduction induced by $\Longrightarrow^{\mathrm{D}}$ we get a one-sided weak reduction ring.

[5] Extensions of (weak) Gröbner bases by elements not belonging to the ideal make no sense in our context as then the reduction relation no longer is a proper means for describing the original ideal congruence.

Hence, if B is a finite Gröbner basis of an ideal $\mathfrak{i}$ and $\beta \in B$ is reducible by $B\backslash\{\beta\}$ to α, then $B \cup \{\alpha\}$ is again a Gröbner basis of $\mathfrak{i}$. The same is true for weak Gröbner bases.

Removing elements from a set is critical as we might decrease the set of elements which are reducible with respect to the set. Hence if the set is a Gröbner basis, after removing elements the ideal elements might no longer reduce to zero using the remaining set. Reviewing the example presented in Section 1.3 we find that while the set $\{X_{,}^2 + X_2, X_1^2 + X_3, X_2 - X_3\}$ is a Gröbner basis in $\mathbb{Q}[X_1, X_2, X_3]$ the subset $\{X_{,}^2 + X_2, X_1^2 + X_3\}$, although it generates the same ideal, is none. In order to remove β from a Gröbner basis B without losing the Gröbner basis property it is important for the reduction relation $\Longrightarrow$ to satisfy an additional axiom:

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

It is not easy to give a simple example for a ring with a reduction relation fulfilling (A1) – (A3) but not (A4) as the reduction rings we have introduced so far all satisfy (A4)[6].

Lemma 3.1.9
Let $(\mathsf{R}, \Longrightarrow)$ *be a reduction ring satisfying (A4). Further let* $B \subseteq \mathsf{R}$ *be a (finite) Gröbner basis of a finitely generated ideal in* R *and* $B' \subseteq B$ *such that for all* $\beta \in B$, $\beta \stackrel{*}{\Longrightarrow}_{B'} 0$ *holds. Then* B' *is a Gröbner basis of* $\mathsf{ideal}^{\mathsf{R}}(B)$. *In particular, for all* $\alpha \in \mathsf{R}$, $\alpha \stackrel{*}{\Longrightarrow}_B 0$ *implies* $\alpha \stackrel{*}{\Longrightarrow}_{B'} 0$.

Proof :
In this proof let $\alpha\Downarrow_B$ denote a normal form of α with respect to $\Longrightarrow_B$ and let $\mathrm{IRR}(\Longrightarrow_B)$ 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 $\beta \stackrel{n}{\Longrightarrow}_{B'} 0$, 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 $\alpha \Longrightarrow_{\beta' \in B'}$.

[6] An example using a right reduction relation in a monoid ring can be found in Example 3.6 in [MR98d]: Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow 1, b^2 \longrightarrow 1, c^2 \longrightarrow 1\}$ be a monoid presentation of $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c$. For $p, f \in \mathbb{K}[\mathcal{M}]$ a (right) reduction relation is defined by $p \longrightarrow_f^{\mathrm{s}} q$ at a monomial $\alpha \cdot t$, if

(a) $\mathsf{HT}(f * w) = t$ for some $w \in \mathcal{M}$, and

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

Looking at $p = ba + b, q = bc + 1$ and $r = ac + b \in \mathbb{Q}[\mathcal{G}]$ we get $p \longrightarrow_q^{\mathrm{s}} p - q * ca = -ca + b$ and $q \longrightarrow_r^{\mathrm{s}} q - r * c = -a + 1 = q_1$, but $p \not\longrightarrow_{\{r,q_1\}}^{\mathrm{s}}$. Trying to reduce ba by r or q_1 we get $r * a = \underline{aca} + ba, r * caba = ba + \underline{bcaba}$ and $q_1 * aba = -ba + \underline{aba}, q_1 * ba = -\underline{aba} + ba$ all violating condition (a). Trying to reduce b we get the same problem as $r * cab = b + \underline{bcab}, q_1 * ab = -b + \underline{a}$ and $q_1 * b = -\underline{ab} + b$.

In the induction step we find $\beta \Longrightarrow_{\beta' \in B'} \delta \stackrel{n-1}{\Longrightarrow}_{B'} 0$ and either $\alpha \Longrightarrow_{\beta' \in B'}$ or $\alpha \Longrightarrow_{\delta}$ and our induction hypothesis yields $\alpha \Longrightarrow_{B'}$.
Hence we can conclude $\mathrm{IRR}(\Longrightarrow_{B'}) \subseteq \mathrm{IRR}(\Longrightarrow_{B})$. We want to show that B' is a Gröbner basis of $\mathsf{ideal}^{\mathsf{R}}(B)$: Assuming $\alpha \stackrel{*}{\Longrightarrow}_{B} \alpha\Downarrow_B$ but $\alpha \stackrel{*}{\Longrightarrow}_{B'} \alpha\Downarrow_{B'} \neq \alpha\Downarrow_B$, we find $\alpha\Downarrow_{B'} \in \mathsf{ideal}^{\mathsf{R}}(B)$ and $\alpha\Downarrow_{B'} \in \mathrm{IRR}(\Longrightarrow_{B'}) \subseteq \mathrm{IRR}(\Longrightarrow_{B})$, 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 $\stackrel{*}{\Longleftrightarrow}_{B} \subseteq \stackrel{*}{\Longleftrightarrow}_{B'}$ holds. This follows immediately, as for $\alpha \stackrel{*}{\Longleftrightarrow}_{B} \beta$ we have $\alpha\Downarrow_{B'} = \alpha\Downarrow_B = \beta\Downarrow_B = \beta\Downarrow_{B'}$ which implies $\alpha \stackrel{*}{\Longleftrightarrow}_{B'} \beta$.

q.e.d.

This result carries over for weak Gröbner bases.

Corollary 3.1.10
Let $(\mathsf{R}, \Longrightarrow)$ *be a weak reduction ring satisfying (A4). Further let* $B \subseteq \mathsf{R}$ *be a (finite) weak Gröbner basis of a finitely generated ideal in* R *and* $B' \subseteq B$ *such that for all* $\beta \in B$, $\beta \stackrel{*}{\Longrightarrow}_{B'} 0$ *holds. Then* B' *is a weak Gröbner basis of* $\mathsf{ideal}^{\mathsf{R}}(B)$. *In particular, for all* $\alpha \in \mathsf{R}$, $\alpha \stackrel{*}{\Longrightarrow}_{B} 0$ *implies* $\alpha \stackrel{*}{\Longrightarrow}_{B'} 0$.

Proof :
As in the proof of Lemma 3.1.9 we can conclude $\mathrm{IRR}(\Longrightarrow_{B'}) \subseteq \mathrm{IRR}(\Longrightarrow_{B})$. Hence assuming that $\alpha \stackrel{*}{\Longrightarrow}_{B} 0$ while $\alpha \stackrel{*}{\Longrightarrow}_{B'} \alpha\Downarrow_{B'} \neq 0$ would imply $\alpha\Downarrow_{B'} \in \mathrm{IRR}(\Longrightarrow_{B})$. As $B' \subseteq B$ this would give us a contradiction since then $\alpha \in \mathsf{ideal}^{\mathsf{R}}(B)$ would have two different normal forms at least one of them not equal to zero with respect to B contradicting the fact that B is supposed to be a weak Gröbner basis.

q.e.d.

Remark 3.1.8 and Lemma 3.1.9 are closely related to interreduction and reduced (weak) Gröbner bases. We call a (weak) Gröbner basis $B \subseteq \mathsf{R}$ **reduced** if no element $\beta \in B$ is reducible by $\Longrightarrow_{B\backslash\{\beta\}}$.

The results of this section carry over to rings with appropriate one-sided reduction relations.

In the remaining sections of this chapter we study the question which ring constructions preserve the property of being a (weak) reduction ring.

3.2 Quotients of Reduction Rings

Let R be a ring with a reduction relation $\Longrightarrow$ fulfilling (A1) – (A3) 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 relation can be defined on the quotient $\mathsf{R}/\mathfrak{i}$ as follows:

Definition 3.2.1
Let $\alpha, \beta, \gamma \in \mathsf{R}/\mathfrak{i}$. We say 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 $(\gamma')\Downarrow_B = \gamma$. $\diamond$

First we ensure that the Axioms (A1) – (A3) hold for the reduction relation in $\mathsf{R}/\mathfrak{i}$ based on Definition 3.2.1: $\longrightarrow_S = \bigcup_{s \in S} \longrightarrow_s$ 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 $\alpha \Longrightarrow_\beta \gamma' \stackrel{*}{\Longrightarrow}_B \gamma$, 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 $\alpha \in \mathsf{R} \backslash \{0\}$ 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 $\beta \Longrightarrow_\gamma \delta' \stackrel{*}{\Longrightarrow}_B \delta$ and since α is $\Longrightarrow_B$-irreducible[7] this implies $\alpha \Longrightarrow_{\{\gamma,\delta\}}$ and hence $\alpha \longrightarrow_{\{\gamma,\delta\}}$.

Theorem 3.2.2
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 $\mathsf{R}/\mathfrak{i}$ as defined above inherits (A1) – (A4) from R, it remains to show that every finitely generated ideal $\mathfrak{j} \subseteq \mathsf{R}/\mathfrak{i}$ has a finite Gröbner basis. Let $\mathfrak{j}_{\mathsf{R}} = \{\alpha \in \mathsf{R} \mid \alpha\Downarrow_B \in \mathfrak{j}\}$ be an ideal[8] in R corresponding to $\mathfrak{j}$. Then $\mathfrak{j}_{\mathsf{R}}$ is *finitely* generated as an ideal in R by its finite basis in $\mathsf{R}/\mathfrak{i}$ viewed as elements of R and the finite basis of $\mathfrak{i}$. Hence $\mathfrak{j}_{\mathsf{R}}$ has a finite Gröbner basis in R, say G_{R}. Then $G = \{\alpha\Downarrow_B \mid \alpha \in G_{\mathsf{R}}\} \backslash \{0\}$ is a finite Gröbner basis of $\mathfrak{j}$: If $\alpha \in \mathfrak{j}$ we have $\alpha \stackrel{*}{\longrightarrow}_G 0$ and $\mathsf{ideal}^{\mathsf{R}/\mathfrak{i}}(G) = \mathfrak{j}$, 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 $\mathfrak{j}_{\mathsf{R}}$ and $\longrightarrow_G \subseteq \stackrel{*}{\Longrightarrow}_{G \cup B}$, when restricted to elements in $\mathsf{R}/\mathfrak{i}$ we have $\mathrm{IRR}(\longrightarrow_G) = \mathrm{IRR}(\Longrightarrow_{G \cup B})$ and $\longrightarrow_G$ is confluent. Furthermore, since

[7] Remember that in the proof of Lemma 3.1.9 we have shown that $\alpha \Longrightarrow_\beta$ and $\beta \stackrel{*}{\Longrightarrow}_{B'} 0$ imply $\alpha \Longrightarrow_{B'}$. This carries over to our situation in the form that $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_\gamma \delta' \stackrel{*}{\Longrightarrow}_B \delta$ implies $\alpha \Longrightarrow_{\{\gamma,\delta',\delta\} \cup B}$ and using induction to $\alpha \Longrightarrow_{\{\gamma,\delta\} \cup B}$.

[8] $\mathfrak{j}_{\mathsf{R}}$ is an ideal in R since

1. $0 \in \mathfrak{j}_{\mathsf{R}}$ as $0 \in \mathfrak{j}$.
2. $\alpha, \beta \in \mathfrak{j}_{\mathsf{R}}$ implies $\alpha\Downarrow_B, \beta\Downarrow_B \in \mathfrak{j}$, hence $\alpha\Downarrow_B + \beta\Downarrow_B = (\alpha + \beta)\Downarrow_B \in \mathfrak{j}$ and $\alpha + \beta \in \mathfrak{j}_{\mathsf{R}}$.
3. $\alpha \in \mathfrak{j}_{\mathsf{R}}$ and $\gamma \in \mathsf{R}$ implies $\alpha\Downarrow_B \in \mathfrak{j}$ and $\gamma \cdot \alpha\Downarrow_B = (\gamma \cdot \alpha)\Downarrow_B \in \mathfrak{j}$, $\alpha\Downarrow_B \cdot \gamma = (\alpha \cdot \gamma)\Downarrow_B \in \mathfrak{j}$, hence $\gamma \cdot \alpha, \alpha \cdot \gamma \in \mathfrak{j}_{\mathsf{R}}$.

$\equiv_{\mathsf{j}} = \equiv_{\mathsf{j}_{\mathsf{R}}}$ when restricted to $\mathsf{R}/\mathfrak{i}$ we get $\overset{*}{\longleftrightarrow}_G = \equiv_{\mathsf{j}}$ on $\mathsf{R}/\mathfrak{i}$ implying that $\mathsf{R}/\mathfrak{i}$ is a reduction ring.

q.e.d.

In Example 3.1.1 we have seen how to associate the integers with a reduction relation $\Longrightarrow$ and in fact $(\mathbb{Z}, \Longrightarrow)$ is a reduction ring. Theorem 3.2.2 then states that for every $m \in \mathbb{Z}$ the quotient $\mathbb{Z}/\mathsf{ideal}(m)$ again is a reduction ring with respect to the reduction relation defined analogue to Definition 3.2.1. In particular reduction rings with zero divisors can be constructed in this way.

Of course if we only assume that R is a weak reduction ring we no longer have unique normal forms for the elements in the quotient. Still comparing elements is possible as $\alpha = \beta$ in $\mathsf{R}/\mathfrak{i}$ if and only if $\alpha - \beta \in \mathfrak{i}$ if and only if $\alpha - \beta \overset{*}{\Longrightarrow}_B 0$ for a weak Gröbner basis B of $\mathfrak{i}$. Hence the elements in the quotient are no longer given by unique elements but by the respective sets of all representatives with respect to the weak Gröbner basis chosen for the ideal[9].

Corollary 3.2.3
If $(\mathsf{R}, \Longrightarrow)$ *is a weak reduction ring with (A4), then for every finitely generated ideal* $\mathfrak{i}$ *the quotient* $(\mathsf{R}/\mathfrak{i}, \longrightarrow)$ *again is a weak reduction ring with (A4).*

Proof :
It remains to show that every finitely generated ideal $\mathsf{j} \subseteq \mathsf{R}/\mathfrak{i}$ has a finite weak Gröbner basis. Let B be a finite weak Gröbner basis of $\mathfrak{i}$ in R and B_{j} a finite generating set for the ideal j in $\mathsf{R}/\mathfrak{i}$.
Let $\mathsf{j}_{\mathsf{R}} = \bigcup_{\alpha\in\mathsf{j}}\{\beta \in \mathsf{R} \mid \beta \Longleftrightarrow^*_B \alpha\}$, be an ideal in R corresponding to j. Then j_{R} is *finitely* generated by the set $B \cup \tilde{B}_{\mathsf{j}}$ where for each element $\alpha \in B_{\mathsf{j}}$ the set $\tilde{B}_{\mathsf{j}}$ contains some $\tilde{\alpha} \in \{\beta \in \mathsf{R} \mid \beta \Longleftrightarrow^*_B \alpha\}$. Moreover, j_{R} has a finite weak Gröbner basis, say G_{R}. Then the set $G = \{\alpha\Downarrow_B \mid \alpha \in G_{\mathsf{R}}\}\backslash\{0\}$ containing for each $\alpha \in G_{\mathsf{R}}$ one not necessarily unique normal form $\alpha\Downarrow_B$ is a finite weak Gröbner basis of j: If $\alpha \in \mathsf{j}$ we have $\alpha \overset{*}{\longrightarrow}_G 0$ and $\mathsf{ideal}^{\mathsf{R}/\mathfrak{i}}(G) = \mathsf{j}$, as every element in j (i.e. in particular irreducible with respect to B) which is reducible with an element $\beta \in G_{\mathsf{R}}$ is also reducible with an element of G because (A4) holds[10].

q.e.d.

Now if $(\mathsf{R}, \Longrightarrow)$ is an effective reduction ring, then B can be computed and addition and multiplication in $\mathsf{R}/\mathfrak{i}$ as well as the reduction relation based on Definition 3.2.1 are computable operations. Moreover, Theorem 3.2.2 can be generalized:

[9]Such an element α in the quotient can be represented by any element which is equivalent to it. When doing computations then of course to decide whether $\alpha = \beta$ in $\mathsf{R}/\mathfrak{i}$ one has to check if $\alpha - \beta \overset{*}{\Longrightarrow}_B 0$ for a weak Gröbner basis B of $\mathfrak{i}$.

[10]Since $\alpha \in \mathsf{j}$ is irreducible by B, we have $\alpha \Longrightarrow_\beta \delta' \overset{*}{\Longrightarrow}_{G_{\mathsf{R}}} \delta$ and $\beta \notin B$. Then looking at the situation $\alpha \Longrightarrow_\beta$ and $\beta \overset{*}{\Longrightarrow}_{G_{\mathsf{R}}} \beta\Downarrow_B$, (A4) yields $\alpha \Longrightarrow_{\beta\Downarrow_B}$.

Corollary 3.2.4
If $(\mathsf{R}, \Longrightarrow)$ *is an effective reduction ring with (A4), then for every finitely generated ideal* $\mathfrak{i}$ *the quotient* $(\mathsf{R}/\mathfrak{i}, \longrightarrow)$ *again is an effective reduction ring with (A4).*

Proof :
Given R, B and a finite generating set F for an ideal $\mathfrak{j}$ in $\mathsf{R}/\mathfrak{i}$ we can compute a finite Gröbner basis for $\mathfrak{j}$ 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 $G = \{\alpha\Downarrow_B \mid \alpha \in G_{\mathsf{R}}\}$, where $\alpha\Downarrow_B$ is the normal form of g with respect to $\Longrightarrow_B$ in R and hence an element of $\mathsf{R}/\mathfrak{i}$, is a Gröbner basis of $\mathfrak{j}$ in $\mathsf{R}/\mathfrak{i}$.

q.e.d.

The same is true for effective weak reduction rings.

Finally the results carry over to the case of one-sided reduction rings with (A4) provided that the two-sided ideal has a finite right respectively left Gröbner basis.

3.3 Sums of Reduction Rings

Let $\mathsf{R}_1, \mathsf{R}_2$ be rings with reduction relations $\Longrightarrow^1$ respectively $\Longrightarrow^2$ fulfilling (A1) – (A3). 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 component wise, the unit is $(1_1, 1_2)$ where 1_i is the respective unit in R_i. A natural reduction relation can be defined on R as follows:

Definition 3.3.1
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 the reduction relation in R: $\longrightarrow_B = \bigcup_{\beta \in B} \longrightarrow_\beta$ is terminating for finite sets $B \subseteq \mathsf{R}$ since this property is inherited from the termination of the respective reduction relations in R_i. Hence (A1) holds. (A2) is satisfied since $\alpha \longrightarrow_\beta \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\beta)$. (A3) is true as $\alpha \longrightarrow_\alpha (0_1, 0_2)$ holds for all $\alpha \in \mathsf{R}\backslash\{(0_1, 0_2)\}$. Moreover, it is easy to see that if condition (A4) holds for $\Longrightarrow^1$ and $\Longrightarrow^2$ then this is inherited by $\longrightarrow$.

Theorem 3.3.2
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 the reduction relation in R as defined above inherits (A1) – (A3) respectively (A4) from the reduction relations 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 $\mathfrak{i} = \mathfrak{i}_1 \times \mathfrak{i}_2$. Then $\mathsf{ideal}(B) = \mathfrak{i}$ and $\alpha \in \mathfrak{i}$ implies $\alpha \xrightarrow{*}_B (0_1, 0_2)$ 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 $\xleftrightarrow{*}_B \; = \; \equiv_{\mathfrak{i}}$ 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 $\alpha_2 \overset{*}{\Longleftrightarrow}{}^2_{B_2} \beta_2$.

q.e.d.

Special regular rings as introduced by Weispfenning in [Wei87b] provide examples of such sums of reduction rings, e.g. any direct sum of fields.

Corollary 3.3.3
If $(\mathsf{R}_1, \Longrightarrow^1)$, $(\mathsf{R}_2, \Longrightarrow^2)$ *are weak reduction rings, then* $(\mathsf{R} = \mathsf{R}_1 \times \mathsf{R}_2, \longrightarrow)$ *is again a weak reduction ring.*

Proof :
Reviewing the proof of Theorem 3.3.2 it remains to show that every finitely generated ideal $\mathfrak{i} \subseteq \mathsf{R}$ has a finite weak Gröbner basis. Again we look at 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 $\mathfrak{i}_2 = \{\alpha_2 \mid (\alpha_1, \alpha_2) \in \mathfrak{i} \text{ for some } \alpha_1 \in \mathsf{R}_1\}$ which are finitely generated ideals in R_1 respectively R_2 and hence have finite weak 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 weak Gröbner basis of $\mathfrak{i}$. As before $\mathfrak{i} = \mathfrak{i}_1 \times \mathfrak{i}_2$ and $\mathsf{ideal}(B) = \mathfrak{i}$. Then $\alpha \in \mathfrak{i}$ implies $\alpha \xrightarrow{*}_B (0_1, 0_2)$ 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 $\alpha_2 \overset{*}{\Longrightarrow}{}^2_{B_2} 0_2$ as B_1 and B_2 are respective weak Gröbner bases, and we are done.

q.e.d.

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 relation based on Definition 3.3.1 are computable operations. Moreover, Theorem 3.3.2 can be generalized:

Corollary 3.3.4
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 $F = \{(\alpha_i, \beta_i) \mid 1 \leq i \leq k, \alpha_i \in \mathsf{R}_1, \beta_i \in \mathsf{R}_2\}$ 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 B_1 a Gröbner basis of the ideal generated by $\{\alpha_1, \ldots, \alpha_k\}$ in R_1 and B_2 a Gröbner basis of the ideal generated by $\{\beta_1, \ldots, \beta_k\}$ in R_2. Then $B = \{(\gamma_1, 0_2), (0_1, \gamma_2) \mid \gamma_1 \in B_1, \gamma_2 \in B_2\}$ is a finite Gröbner basis of the ideal generated by F in R.

q.e.d.

A similar result holds for effective weak reduction rings.

Due to the "simple" multiplication used when defining direct sums, Theorem 3.3.2 and Corollary 3.3.4 extend directly to one-sided reduction rings. More complicated multiplications are possible and have to be treated individually.

3.4 Modules over Reduction Rings

Another structure which can be studied by reduction techniques are modules and their submodules. Given a ring R with unit 1 and a natural number k, let $\mathsf{R}^k = \{\mathbf{a} = (\alpha_1, \ldots, \alpha_k) \mid \alpha_i \in \mathsf{R}\}$ be the set of all vectors of length k with coordinates in R. Obviously R^k is an additive commutative group with respect to ordinary vector addition and we denote the zero by $\mathbf{0}$. Moreover, R^k is an R-**module** for scalar multiplication defined as $\alpha * (\alpha_1, \ldots, \alpha_k) = (\alpha \cdot \alpha_1, \ldots, \alpha \cdot \alpha_k)$ and $(\alpha_1, \ldots, \alpha_k) * \alpha = (\alpha_1 \cdot \alpha, \ldots, \alpha_k \cdot \alpha)$. Additionally R^k is called **free** as it has a basis[11]. One such basis is the set of unit vectors $\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \mathbf{e}_k = (0, \ldots, 0, 1)$. Using this basis the elements of R^k can be written uniquely as $\mathbf{a} = \sum_{i=1}^{k} \alpha_i * \mathbf{e}_i$ where $\mathbf{a} = (\alpha_1, \ldots, \alpha_k)$.

Definition 3.4.1
A subset of R^k which is again an R-module is called a **submodule** of R^k. ◇

For example any ideal of R is an R-module and even a submodule of the R-module R^1. Provided a set of vectors $S = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ the set $\{\sum_{i=1}^{n} \sum_{j=1}^{m_i} \beta_{ij} * \mathbf{a}_i * \beta_{ij}' \mid \beta_{ij}, \beta_{ij}' \in \mathsf{R}\}$ is a submodule of R^k. This set is denoted as $\langle S \rangle$ and S is called its generating set.

Now similar to the case of modules over commutative polynomial rings, being Noetherian is inherited by R^k from R.

Theorem 3.4.2
Let R be a Noetherian ring. Then every submodule in R^k is also finitely generated.

[11] Here the term *basis* is used in the meaning of being a linearly independent set of generating vectors.

Proof :
Let $\mathcal{S}$ be a submodule of R^k. We show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact an ideal in R and hence by our hypothesis must be finitely generated. For $k > 1$ let us look at the set $\mathfrak{i} = \{\beta_1 \mid (\beta_1, \ldots, \beta_k) \in \mathcal{S}\}$ which is again an ideal in R and hence finitely generated by some set $\{\gamma_1, \ldots, \gamma_s \mid \gamma_i \in \mathsf{R}\}$. Choose[12] $H = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \subseteq \mathcal{S}$ such that the first coordinate of $\mathbf{c}_i$ is γ_i. Similarly the set $\mathcal{M} = \{(\beta_2, \ldots, \beta_k) \mid (0, \beta_2, \ldots, \beta_k) \in \mathcal{S}\}$ is a submodule in R^{k-1} and therefore finitely generated by our induction hypothesis. Let $\{(\delta^i_2, \ldots, \delta^i_k) \mid 1 \leq i \leq w\}$ be such a finite generating set. Then $\mathbf{d}_i = (0, \delta^i_2, \ldots, \delta^i_k) \in \mathcal{S}$, $1 \leq i \leq w$ and the set $G = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \cup \{\mathbf{d}_i \mid 1 \leq i \leq w\}$ is a finite generating set for $\mathcal{S}$. To see this assume $\mathbf{t} = (\tau_1, \ldots, \tau_k) \in \mathcal{S}$. Then $\tau_1 = \sum_{i=1}^{s} \sum_{j=1}^{n_i} \zeta_{ij} \cdot \gamma_i \cdot {\zeta_{ij}}'$ for some $\zeta_{ij}, {\zeta_{ij}}' \in \mathsf{R}$ and $\mathbf{t}' = \mathbf{t} - \sum_{i=1}^{s} \sum_{j=1}^{n_i} \zeta_{ij} * \mathbf{c}_i * {\zeta_{ij}}' \in \mathcal{S}$ with first coordinate 0. Hence $\mathbf{t}' = \sum_{i=1}^{w} \sum_{j=1}^{m_i} \eta_{ij} * \mathbf{d}_i * {\eta_{ij}}'$ for some $\eta_{ij}, {\eta_{ij}}' \in \mathsf{R}$ giving rise to

$$\mathbf{t} = \mathbf{t}' + \sum_{i=1}^{s} \sum_{j=1}^{n_i} \zeta_{ij} * \mathbf{c}_i * {\zeta_{ij}}' = \sum_{i=1}^{w} \sum_{j=1}^{m_i} \eta_{ij} * \mathbf{d}_i * {\eta_{ij}}' + \sum_{i=1}^{s} \sum_{j=1}^{n_i} \zeta_{ij} * \mathbf{c}_i * {\zeta_{ij}}'.$$

q.e.d.

We will now study submodules of modules using reduction relations. Let $\Longrightarrow$ be a reduction relation on R fulfilling (A1) – (A3). A natural reduction relation on R^k can be defined using the representations as polynomials with respect to the basis of unit vectors as follows:

Definition 3.4.3
Let $\mathbf{a} = \sum_{i=1}^{k} \alpha_i * \mathbf{e}_i$, $\mathbf{b} = \sum_{i=1}^{k} \beta_i * \mathbf{e}_i \in \mathsf{R}^k$. We say that **b reduces a** to **c** at $\alpha_s * \mathbf{e}_s$ in one step, denoted by $\mathbf{a} \longrightarrow_{\mathbf{b}} \mathbf{c}$, if

(a) $\beta_j = 0$ for $1 \leq j < s$,

(b) $\alpha_s \Longrightarrow_{\beta_s} \gamma_s$ with $\alpha_s = \gamma_s + \sum_{i=1}^{n} \delta_i \cdot \beta_s \cdot {\delta_i}'$, $\delta_i, {\delta_i}' \in \mathsf{R}$, and

(c) $\mathbf{c} = \mathbf{a} - \sum_{i=1}^{n} \delta_i * \mathbf{b} * {\delta_i}' = (\alpha_1, \ldots, \alpha_{s-1}, \gamma_s, \alpha_{s+1} - \sum_{i=1}^{n} \delta_i \cdot \beta_{s+1} \cdot {\delta_i}', \ldots, \alpha_k - \sum_{i=1}^{n} \delta_i \cdot \beta_k \cdot {\delta_i}')$. $\diamond$

The Axioms (A1) – (A3) hold for this reduction relation on R^k: $\longrightarrow_B = \bigcup_{\mathbf{b} \in B} \longrightarrow_{\mathbf{b}}$ is terminating for finite $B \subseteq \mathsf{R}^k$ since this property is inherited from the termination of the respective reduction relation $\Longrightarrow$ in R. Hence (A1) holds. (A2) is satisfied now of course in the context of submodules since $\mathbf{a} \longrightarrow_{\mathbf{b}} \mathbf{c}$ implies $\mathbf{a} - \mathbf{c} \in \langle \{\mathbf{b}\} \rangle$. (A3) is true as $\mathbf{a} \longrightarrow_{\mathbf{a}} \mathbf{0}$ holds for all $\mathbf{a} \in \mathsf{R}^k \backslash \{\mathbf{0}\}$. Moreover, it is easy to see that if condition (A4) holds for $\Longrightarrow$ then this is inherited by $\longrightarrow$ as defined in Definition 3.4.3 for R^k. First we show how the existence of weak Gröbner bases carries over for Noetherian R.

[12] In this step we need the Axiom of Choice and hence the construction is not constructive.

Definition 3.4.4
A subset B of R^k is called a **weak Gröbner basis** of the submodule $\mathcal{S} = \langle B \rangle$, if $\longrightarrow_B$ is terminating and $\mathbf{a} \xrightarrow{*}_B \mathbf{0}$ for all $\mathbf{a} \in \mathcal{S}$. ◇

Theorem 3.4.5
Let R *be a Noetherian ring with reduction relation* $\Longrightarrow$ *fulfilling (A1) – (A3). If in* R *every ideal has a finite weak Gröbner basis, then the same holds for submodules in* $(\mathsf{R}^k, \longrightarrow)$.

Proof :
Let $\mathcal{S}$ be a submodule of R^k. We show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact an ideal[13] in R and hence by our hypothesis must have a finite weak Gröbner basis. For $k > 1$ let us look at the set $\mathfrak{i} = \{\beta_1 \mid (\beta_1, \ldots, \beta_k) \in \mathcal{S}\}$ which is again an ideal[14]. Hence $\mathfrak{i}$ must have a finite weak Gröbner basis $\{\gamma_1, \ldots, \gamma_s \mid \gamma_i \in \mathsf{R}\}$. Choose $H = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \subseteq \mathcal{S}$ such that the first coordinate of $\mathbf{c}_i$ is γ_i. Similarly the set $\mathcal{M} = \{(\beta_2, \ldots, \beta_k) \mid (0, \beta_2, \ldots, \beta_k) \in \mathcal{S}\}$ is a submodule[15] in R^{k-1} which by our induction hypothesis must have a finite weak Gröbner basis $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$. Then the set $G = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \cup \{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ is a weak Gröbner basis for $\mathcal{S}$.
That G is a generating set for $\mathcal{S}$ follows as in the proof of Theorem 3.4.2. It remains to show that G is in fact a weak Gröbner basis, i.e., for every $\mathbf{t} = (\tau_1, \ldots, \tau_k) \in \mathcal{S}$ we have $\mathbf{t} \xrightarrow{*}_G \mathbf{0}$. Since $\tau_1 \stackrel{*}{\Longrightarrow}_{\{\gamma_1, \ldots, \gamma_s\}} 0$ with $\tau_1 = \sum_{i=1}^{s} \sum_{j=1}^{n_i} \zeta_{ij} \cdot \gamma_i \cdot \zeta_{ij}{}'$, by the definition of G we get $\mathbf{t} \xrightarrow{*}_{\{\mathbf{c}_1, \ldots, \mathbf{c}_s\}} \mathbf{t} - \sum_{i=1}^{s} \sum_{j=1}^{n_i} \zeta_{ij} * \mathbf{c}_i * \zeta_{ij}{}' = \mathbf{t}'$ where $\mathbf{t}' = (0, \tau_2{}', \ldots, \tau_k{}') \in \mathcal{M}$. Hence, as $(\tau_2{}', \ldots, \tau_k{}') \xrightarrow{*}_{\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}} \mathbf{0}$, we get $\mathbf{t} \xrightarrow{*}_G \mathbf{0}$ and are done.

q.e.d.

Now we turn our attention to Gröbner bases of submodules in R^k.

Definition 3.4.6
A subset B of R^k is called a **Gröbner basis** of the submodule $\mathcal{S} = \langle B \rangle$, if $\xleftrightarrow{*}_B = \equiv_{\mathcal{S}}$ and $\longrightarrow_B$ is complete. ◇

[13] At this point we could also proceed with a much weaker hypothesis, namely instead of requiring R to be Noetherian assuming that $\mathcal{S}$ is finitely generated. Then still the fact that R is supposed to be a weak reduction ring would imply the existence of a finite weak Gröbner basis for $\mathcal{S}$.

[14] Here it still would be sufficient to require that $\mathcal{S}$ is finitely generated as the first coordinates of a finite generating set for $\mathcal{S}$ then would generate $\mathfrak{i}$ hence implying that the ideal is finitely generated as well.

[15] *Now* we really need that R^{k-1} is Noetherian. Assuming that $\mathcal{S}$ is finitely generated would *not* help to deduce that $\mathcal{M}$ is finitely generated.

Theorem 3.4.7
Let R *be a Noetherian ring with reduction relation* $\Longrightarrow$ *fulfilling (A1) – (A3). If in* R *every ideal has a finite Gröbner basis, then the same holds for submodules in* $(\mathsf{R}^k, \longrightarrow)$.

Proof :
The candidate for the Gröbner basis can be built similar to the set G in the proof of Theorem 3.4.5 now of course using Gröbner bases in the construction instead of weak Gröbner bases: Let $\mathcal{S}$ be a submodule of R^k. We show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact an ideal in R and hence by our hypothesis must have a finite Gröbner basis. For $k > 1$ let us look at the set $\mathfrak{i} = \{\beta_1 \mid (\beta_1, \ldots, \beta_k) \in \mathcal{S}\}$ which is again an ideal in R. Hence $\mathfrak{i}$ must have a finite Gröbner basis $\{\gamma_1, \ldots, \gamma_s \mid \gamma_i \in \mathsf{R}\}$ by our assumption. Choose $H = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \subseteq \mathcal{S}$ such that the first coordinate of $\mathbf{c}_i$ is γ_i. Similarly the set $\mathcal{M} = \{(\beta_2, \ldots, \beta_k) \mid (0, \beta_2, \ldots, \beta_k) \in \mathcal{S}\}$ is a submodule in R^{k-1} finitely generated as R^{k-1} is Noetherian. Hence by our induction hypothesis $\mathcal{M}$ then must have a finite Gröbner basis $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$. Let $G = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \cup \{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$. Since G generates $\mathcal{S}$ (see the proof of Theorem 3.4.5) it remains to show that it is a Gröbner basis.
By the definition of the reduction relation in R^k we immediately find $\stackrel{*}{\longleftrightarrow}_G \subseteq \equiv_{\mathcal{S}}$. To see the converse let $\mathbf{r} = (\rho_1, \ldots, \rho_k) \equiv_{\mathcal{S}} \mathbf{s} = (\sigma_1, \ldots, \sigma_k)$. Then as $\rho_1 \equiv_{\{\beta_1 \mid \mathbf{b} = (\beta_1, \ldots, \beta_k) \in \mathcal{S}\}} \sigma_1$ by the definition of G we get $\rho_1 \stackrel{*}{\Longleftrightarrow}_{\{\gamma_1, \ldots, \gamma_s\}} \sigma_1$. But this gives us $\mathbf{r} \stackrel{*}{\longleftrightarrow}_H \mathbf{r} + \sum_{i=1}^{s} \sum_{j=1}^{m_i} \chi_{ij} * \mathbf{c}_i * \chi_{ij}{}' = \mathbf{r}' = (\sigma_1, \rho_2{}', \ldots, \rho_k{}')$ and we get $(\sigma_1, \rho_2{}', \ldots, \rho_k{}') \equiv_{\mathcal{S}} (\sigma_1, \ldots, \sigma_k)$. Hence $(\sigma_1, \rho_2{}', \ldots, \rho_k{}') - (\sigma_1, \ldots, \sigma_k) = (0, \rho_2{}' - \sigma_2, \ldots, \rho_k{}' - \sigma_k) \in \mathcal{S}$, implying $(\rho_2{}' - \sigma_2, \ldots, \rho_k{}' - \sigma_k) \in \mathcal{M}$. Now we have to be more careful since we cannot conclude that $(\rho_2{}', \ldots, \rho_k{}'), (\sigma_2, \ldots, \sigma_k) \in \mathcal{M}$. But we know $(\sigma_1, \rho_2{}', \ldots, \rho_k{}') = (\sigma_1, \ldots, \sigma_k) + (0, \rho_2{}' - \sigma_2, \ldots, \rho_k{}' - \sigma_k) = (\sigma_1, \ldots, \sigma_k) + \sum_{i=1}^{w} \sum_{j=1}^{n_i} \eta_{ij} * \mathbf{d}_i * \eta_{ij}{}'$ where $(0, \rho_2{}' - \sigma_2, \ldots, \rho_k{}' - \sigma_k) = \sum_{i=1}^{w} \sum_{j=1}^{n_i} \eta_{ij} * \mathbf{d}_i * \eta_{ij}{}'$ for $\eta_{ij}, \eta_{ij}{}' \in \mathsf{R}$, i.e., $(\sigma_1, \rho_2{}', \ldots, \rho_k{}') \equiv_{\langle \mathbf{d}_1, \ldots, \mathbf{d}_w \rangle} (\sigma_1, \ldots, \sigma_k)$. Hence, as $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ is a Gröbner basis of $\mathcal{M}$ both vectors $(\sigma_1, \rho_2{}', \ldots, \rho_k{}')$ and $(\sigma_1, \ldots, \sigma_k)$ must have a common normal form using $\{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ for reduction[16] and we are done.
The same argument applies to show local confluence. Let us assume there are $\mathbf{r}$, $\mathbf{s}_1$, $\mathbf{s}_2 \in \mathsf{R}^k$ such that $\mathbf{r} \longrightarrow_G \mathbf{s}_1$ and $\mathbf{r} \longrightarrow_G \mathbf{s}_2$. Then by the definition of G, the first coordinates σ_1^1 and σ_1^2 of $\mathbf{s}_1$ respectively $\mathbf{s}_2$ are joinable by $\{\gamma_1, \ldots, \gamma_s\}$ to some element, say σ, giving rise to the elements $\mathbf{r}_1 = \mathbf{s}_1 + \sum_{i=1}^{s} \sum_{j=1}^{n_i} \chi_{ij} * \mathbf{c}_i * \chi_{ij}{}'$ and $\mathbf{r}_2 = \mathbf{s}_2 + \sum_{i=1}^{s} \sum_{j=1}^{m_i} \psi_{ij} * \mathbf{c}_i * \psi_{ij}{}'$ with first coordinate σ. Again we know $(\sigma, \rho_2^1, \ldots, \rho_k^1) = (\sigma, \rho_2^2, \ldots, \rho_k^2) + (0, \rho_2^1 - \rho_2^2, \ldots, \rho_k^1 - \rho_k^2)$ with $(\rho_2^1 - \rho_2^2, \ldots, \rho_k^1 - \rho_k^2) \in \mathcal{M}$. Hence $(\sigma, \rho_2^1, \ldots, \rho_k^1) = (\sigma, \rho_2^2, \ldots, \rho_k^2) + \sum_{i=1}^{w} \sum_{j=1}^{n_i} \eta_{ij} * \mathbf{d}_i * \eta_{ij}{}'$ for $\eta_{ij}, \eta_{ij}{}' \in \mathsf{R}$, i.e., $(\sigma_1, \rho_2{}', \ldots, \rho_k{}') \equiv_{\langle \mathbf{d}_1, \ldots, \mathbf{d}_w \rangle} (\sigma_1, \ldots, \sigma_k)$. As again $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ is

[16] The elements in this set cannot influence the first coordinate which is σ_1 for both vectors.

a Gröbner basis of $\mathcal{M}$ both vectors must have a common normal with respect to reduction using $\{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$.

q.e.d.

Let us close this section with a remark on why the additional property of being Noetherian is so important. In the proofs of Theorem 3.4.5 and 3.4.7 in the induction step the "projection" of $\mathcal{S}$ on R^{k-1} plays an essential role. If this projection is defined as $\mathcal{M} = \{(\beta_2, \ldots, \beta_k) \mid (0, \beta_2, \ldots, \beta_k) \in \mathcal{S}\}$ we have to show that this module is again finitely generated. In assuming Noetherian for R this then follows as $\mathcal{M}$ is a submodule of R^{k-1} which is again Noetherian. Assuming that $\mathcal{S}$ is finitely generated by some set $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ does not improve the situation as in general we cannot extract a finite generating set for $\mathcal{M}$ from this set[17]. The situation improves if we look at one-sided reduction rings R and demand that in R all (left respectively right) syzygy modules have finite bases.

R^k is a right R-module with scalar multiplication $(\alpha_1, \ldots, \alpha_k) * \alpha = (\alpha_1 \cdot \alpha, \ldots, \alpha_k \cdot \alpha)$. Provided a finite subset $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathsf{R}$ the set of solutions of the equation $\alpha_1 \cdot X_1 + \ldots + \alpha_n \cdot X_n = 0$ is a submodule of the right R-module R^n. It is called the (first) module of syzygies of $\{\alpha_1, \ldots, \alpha_n\}$ in the literature. We will see that these special modules can be used to characterize Gröbner bases of submodules in R^k.

A reduction relation can be defined similarly to Definition 3.4.3.

Definition 3.4.8
Let $\mathbf{a} = \sum_{i=1}^k \mathbf{e}_i * \alpha_i$, $\mathbf{b} = \sum_{i=1}^k \mathbf{e}_i * \beta_i \in \mathsf{R}^k$. We say that **b right reduces a** to **c** at the monomial $\mathbf{e}_s * \alpha_s$ in one step, denoted by $\mathbf{a} \longrightarrow^{\mathrm{r}}_{\mathbf{b}} \mathbf{c}$, if

(a) $\beta_j = 0$ for $1 \leq j < s$,

(b) $\alpha_s \Longrightarrow_{\beta_s} \gamma_s$ with $\alpha_s = \gamma_s + \beta_s \cdot \delta$, $\delta \in \mathsf{R}$, and

(c) $\mathbf{c} = \mathbf{a} - \mathbf{b} * \delta = (\alpha_1, \ldots, \alpha_{s-1}, \gamma_s, \alpha_{s+1} - \beta_{s+1} \cdot \delta, \ldots, \alpha_k - \beta_k \cdot \delta)$. $\diamond$

Theorem 3.4.9
Let R be a ring with a right reduction relation $\Longrightarrow$ fulfilling (A1) – (A3). Additionally let every right module of syzygies in R have a finite basis. If every

[17] Another idea might be to look at an other projection of $\mathcal{S}$: $\mathcal{M}' = \{(\beta_2, \ldots, \beta_k) \mid$ there exists $\beta_1 \in \mathsf{R}$ such that $(\beta_1, \beta_2, \ldots, \beta_k) \in \mathcal{S}\}$. $\mathcal{M}'$ then is again a module now finitely generated by $(\alpha_2^1, \ldots, \alpha_k^1), \ldots, (\alpha_2^n, \ldots, \alpha_k^n)$. Unfortunately in this case having a Gröbner basis for this module is of no use as we can no longer lift this special basis to R^k. The trick with adding 0 as the first coordinate will no longer work as for some $(\gamma_2, \ldots, \gamma_k) \in \mathcal{M}'$ we only know that there exists some $\gamma \in \mathsf{R}$ such that $(\gamma, \gamma_2, \ldots, \gamma_k) \in \mathcal{S}$ and we cannot enforce that $\gamma = 0$. However, if we lift the set by adding appropriate elements $\gamma \in \mathsf{R}$ as first coordinates, then the resulting set does not lift the Gröbner basis properties for the reduction relation. Especially in the induction step the first coordinate of the vector being modified can no longer be expected to be left unchanged which is the case when using vectors with first coordinate 0 for reduction.

finitely generated right ideal in R *has a finite Gröbner basis, then the same holds for every finitely generated right submodule in* $(\mathsf{R}^k, \longrightarrow)$.

Proof :
Again the candidate for the right Gröbner basis can be built similar to the set G in the proofs of Theorem 3.4.5 and 3.4.7: Let $\mathcal{S}$ be a right submodule of R^k which is finitely generated by a set $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$. We show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact a finitely generated right ideal in R and hence by our hypothesis must have a finite right Gröbner basis. For $k > 1$ let us look at the set $\mathfrak{i} = \{\beta_1 \mid (\beta_1, \ldots, \beta_k) \in \mathcal{S}\}$ which is again a right ideal in R finitely generated by $\{\alpha_1^1, \ldots, \alpha_1^n\}$ where $\mathbf{a}_i = (\alpha_1^i, \ldots, \alpha_k^i)$. Hence $\mathfrak{i}$ must have a finite right Gröbner basis $\{\gamma_1, \ldots, \gamma_s \mid \gamma_i \in \mathsf{R}\}$ by our assumption. Choose $H = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \subseteq \mathcal{S}$ such that the first coordinate of $\mathbf{c}_i$ is γ_i. On the other hand the right syzygy module $\{(\psi_1, \ldots, \psi_n) \mid \sum_{i=1}^n \alpha_1^i \cdot \psi_i = 0, \psi_i \in \mathsf{R}\}$ has a finite basis $B = \{(\beta_1^j, \ldots, \beta_n^j) \mid 1 \leq j \leq m\} \subseteq \mathsf{R}^n$. Then the set $\{\sum_{i=1}^n \mathbf{a}_i * \beta_i^j \mid 1 \leq j \leq m\} \cup \{\mathbf{a}_i \mid \alpha_1^i = 0, 1 \leq i \leq n\}$ is a finite generating set for the submodule $\mathcal{M} = \{(\beta_2, \ldots, \beta_k) \mid (0, \beta_2, \ldots, \beta_k) \in \mathcal{S}\}$ of R^{k-1}. To see this let $(0, \beta_2, \ldots, \beta_k) \in \mathcal{S}$. Then $(0, \beta_2, \ldots, \beta_k) = \sum_{i=1}^n \mathbf{a}_i * \zeta_i$, $\zeta_i \in \mathsf{R}$ implies $\sum_{i=1}^n \alpha_1^i \cdot \zeta_i = 0$ and hence $(\zeta_1, \ldots, \zeta_n)$ lies in the right syzygy module and we are done. Hence by our induction hypothesis $\mathcal{M}$ then must have a finite right Gröbner basis $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$. Let $G = \{\mathbf{c}_1, \ldots, \mathbf{c}_s\} \cup \{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$. Since G generates $\mathcal{S}$ it remains to show that it is a right Gröbner basis. By the definition of the reduction relation in R^k we immediately find $\stackrel{*}{\longleftrightarrow}_G \subseteq \equiv_{\mathcal{S}}$. To see the converse let $\mathbf{r} = (\rho_1, \ldots, \rho_k) \equiv_{\mathcal{S}} \mathbf{s} = (\sigma_1, \ldots, \sigma_k)$. Then as $\rho_1 \equiv_{\{\alpha_1 \mid \mathbf{a} = (\alpha_1, \ldots, \alpha_k) \in \mathcal{S}\}} \sigma_1$ by the definition of G we get $\rho_1 \stackrel{*}{\longleftrightarrow}_{\{\gamma_1, \ldots, \gamma_s\}} \sigma_1$. But this gives us $\mathbf{r} \stackrel{*}{\Longleftrightarrow}_H \mathbf{r} + \sum_{i=1}^s \mathbf{c}_i * \chi_i = \mathbf{r}' = (\sigma_1, {\rho_2}', \ldots, {\rho_k}')$, $\chi_i \in \mathsf{R}$, and we get $(\sigma_1, {\rho_2}', \ldots, {\rho_k}') \equiv_{\mathcal{S}} (\sigma_1, \ldots, \sigma_k)$. Hence $(\sigma_1, {\rho_2}', \ldots, {\rho_k}') - (\sigma_1, \ldots, \sigma_k) = (0, {\rho_2}' - \sigma_2, \ldots, {\rho_k}' - \sigma_k) \in \mathcal{S}$ implying $({\rho_2}' - \sigma_2, \ldots, {\rho_k}' - \sigma_k) \in \mathcal{M}$. Now we have to be more careful since we cannot conclude that $({\rho_2}', \ldots, {\rho_k}'), (\sigma_2, \ldots, \sigma_k) \in \mathcal{M}$. But we know $(\sigma_1, {\rho_2}', \ldots, {\rho_k}') = (\sigma_1, \ldots, \sigma_k) + (0, {\rho_2}' - \sigma_2, \ldots, {\rho_k}' - \sigma_k) = (\sigma_1, \ldots, \sigma_k) + \sum_{i=1}^w \mathbf{d}_i * \eta_i$ where $(0, {\rho_2}' - \sigma_2, \ldots, {\rho_k}' - \sigma_k) = \sum_{i=1}^w \mathbf{d}_i * \eta_i$ for $\eta_i \in \mathsf{R}$, i.e., $(\sigma_1, {\rho_2}', \ldots, {\rho_k}') \equiv_{\langle \mathbf{d}_1, \ldots, \mathbf{d}_w \rangle} (\sigma_1, \ldots, \sigma_k)$. Hence, as $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ is a right Gröbner basis of $\mathcal{M}$ both vectors $(\sigma_1, {\rho_2}', \ldots, {\rho_k}')$ and $(\sigma_1, \ldots, \sigma_k)$ must have a common normal form using $\{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ for reduction[18] and we are done.
The same argument applies to show local confluence. Let us assume there are $\mathbf{r}$, $\mathbf{s}_1$, $\mathbf{s}_2 \in \mathsf{R}^k$ such that $\mathbf{r} \longrightarrow_G \mathbf{s}_1$ and $\mathbf{r} \longrightarrow_G \mathbf{s}_2$. Then by the definition of G the first coordinates σ_1^1 and σ_1^2 of $\mathbf{s}_1$ respectively $\mathbf{s}_2$ are joinable by $\{\gamma_1, \ldots, \gamma_s\}$ to some element say σ giving rise to elements $\mathbf{r}_1 = \mathbf{s}_1 + \sum_{i=1}^s \mathbf{c}_i * \chi_i$ and $\mathbf{r}_2 = \mathbf{s}_2 + \sum_{i=1}^s \mathbf{c}_i *$

[18]The elements in this set cannot influence the first coordinate which is σ_1 for both vectors.

ψ_i with first coordinate σ. Again we know $(\sigma, \rho_2^1, \ldots, \rho_k^1) = (\sigma, \rho_2^2, \ldots, \rho_k^2) + (0, \rho_2^1 - \rho_2^2, \ldots, \rho_k^1 - \rho_k^2)$ with $(\rho_2^1 - \rho_2^2, \ldots, \rho_k^1 - \rho_k^2) \in \mathcal{M}$. Hence $(\sigma, \rho_2^1, \ldots, \rho_k^1) = (\sigma, \rho_2^2, \ldots, \rho_k^2) + \sum_{i=1}^{w} \mathbf{d}_i * \eta_i$ for $\eta_i \in \mathsf{R}$, i.e., $(\sigma_1, \rho_2', \ldots, \rho_k') \equiv_{\langle \mathbf{d}_1, \ldots, \mathbf{d}_w \rangle} (\sigma_1, \ldots, \sigma_k)$. As again $\{(\delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$ is a right Gröbner basis of $\mathcal{M}$ both vectors must have a common normal with respect to reduction using $\{\mathbf{d}_i = (0, \delta_2^i, \ldots, \delta_k^i) \mid 1 \leq i \leq w\}$.

q.e.d.

The task of describing two-sided syzygy modules is much more complicated. We follow the ideas given by Apel in his habilitation [Ape98].

Let $\mathcal{R}$ be the free Abelian group with basis elements $\alpha \otimes \beta$ where $\alpha, \beta \in \mathsf{R}$. We define a new vector space $\mathcal{S}$ with formal sums as elements $\sum_{i=1}^{n} \gamma_i \cdot \alpha_i \otimes \beta_i \cdot \delta_i$ where $\gamma_i, \delta_i \in \mathsf{R}$ and $\alpha_i \otimes \beta_i \in \mathcal{R}$. Let $\mathcal{U}$ be the subspace of $\mathcal{S}$ generated by the vectors

$$\alpha \otimes (\beta_1 + \beta_2) - \alpha \otimes \beta_1 - \alpha \otimes \beta_2$$

$$(\alpha_1 + \alpha_2) \otimes \beta - \alpha_1 \otimes \beta - \alpha_2 \otimes \beta$$

$$\alpha \otimes (\gamma \cdot \beta) - \gamma \cdot (\alpha \otimes \beta)$$

$$(\gamma \cdot \alpha) \otimes \beta - \gamma \cdot (\alpha \otimes \beta)$$

$$\alpha \otimes (\beta \cdot \gamma) - (\alpha \otimes \beta) \cdot \gamma$$

$$(\alpha \cdot \gamma) \otimes \beta - (\alpha \otimes \beta) \cdot \gamma$$

where $\alpha, \alpha_i, \beta, \beta_i, \gamma \in \mathsf{R}$. Then the quotient $\mathcal{S}/\mathcal{U}$ is called the **tensor product** denoted by $\mathsf{R} \otimes \mathsf{R}$.

The sets we are interested in can be defined as follows: Let R be some subset of R. Syzygies of R are solutions of the equations $\sum_{i=1}^{n} \sum_{j=1}^{n_i} \alpha_{i,j} \cdot \rho_i \cdot \beta_{i,j} = 0, \alpha_{i,j}, \beta_{i,j} \in \mathsf{R}, \rho_i \in R$. The set containing all such solutions is called the syzygy module of R. We can now describe these sets using objects of the "polynomial" structure $\mathcal{S}[\mathsf{R}]$ which contains formal sums of the form $\sum_{i=1}^{n} \sum_{j=1}^{n_i} (\alpha_{i,j} \otimes \beta_{i,j}) \cdot \gamma_i$, $\alpha_i, \beta_i, \gamma_i \in \mathsf{R}$. We can associate a mapping $\phi : \mathcal{S}[\mathsf{R}] \longrightarrow \mathsf{R}$ by $\sum_{i=1}^{n} \sum_{j=1}^{n_i} (\alpha_{i,j} \otimes \beta_{i,j}) \cdot \gamma_i \mapsto \sum_{i=1}^{n} \sum_{j=1}^{n_i} \alpha_{i,j} \cdot \gamma_i \cdot \beta_{i,j}$. Then for the set R we are interested in, the set of "solutions" is $\bigcup_{\rho_1, \ldots, \rho_k \in R, k \in \mathbb{N}} S_{\rho_1, \ldots, \rho_k}$ with ordered lists of not necessarily different elements from R such that $S_{\rho_1, \ldots, \rho_k} = \{(\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j}) \mid \phi(\sum_{i=1}^{k} \sum_{j=1}^{n_i} (\alpha_{i,j} \otimes \beta_{i,j}) \cdot \rho_i) = 0, \alpha_{i,j}, \beta_{i,j} \in \mathsf{R}\}$. Then these sets $S_{\rho_1, \ldots, \rho_k}$ are in fact modules

1. $S_{\rho_1, \ldots, \rho_k}$ is closed under scalar multiplication, i.e., $(\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j}) \in S_{\rho_1, \ldots, \rho_k}$ and $\gamma \in \mathsf{R}$ implies $\gamma \cdot (\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j}) = (\gamma \cdot (\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}), \ldots, \gamma \cdot (\sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j})) \in S_{\rho_1, \ldots, \rho_k}$:
   $\phi(\sum_{i=1}^{k} \sum_{j=1}^{n_i} (\alpha_{i,j} \otimes \beta_{i,j}) \cdot \rho_i) = 0$ implies $\phi(\gamma \cdot (\sum_{i=1}^{k} \sum_{j=1}^{n_i} (\alpha_{i,j} \otimes \beta_{i,j}) \cdot \rho_i)) = 0$ as $\gamma \cdot (\alpha_{i,j} \otimes \beta_{i,j}) = (\gamma \cdot \alpha_{i,j}) \otimes \beta_{i,j}$ and hence $\phi(\gamma \cdot (\sum_{i=1}^{k} \sum_{j=1}^{n_i} (\alpha_{i,j} \otimes \beta_{i,j}) \cdot \rho_i)) =$

$\sum_{i=1}^{k} \sum_{j=1}^{n_i} \gamma \cdot \alpha_{i,j} \cdot \rho_i \cdot \beta_{i,j} = 0$. Multiplication from the right can be treated similarly.

2. $S_{\rho_1,\ldots,\rho_k}$ is closed under addition, i.e., $(\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j})$, $(\sum_{j=1}^{\tilde{n_1}} \tilde{\alpha}_{1,j} \otimes \tilde{\beta}_{1,j}, \ldots, \sum_{j=1}^{\tilde{n_k}} \tilde{\alpha}_{k,j} \otimes \tilde{\beta}_{k,j}) \in S_{\rho_1,\ldots,\rho_k}$ implies $(\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j} + \sum_{j=1}^{\tilde{n_1}} \tilde{\alpha}_{1,j} \otimes \tilde{\beta}_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j} + \sum_{j=1}^{\tilde{n_k}} \tilde{\alpha}_{k,j} \otimes \tilde{\beta}_{k,j}) \in S_{\rho_1,\ldots,\rho_k}$.

The question arises when such modules have useful bases for characterizing syzygy modules in non-commutative reduction rings. This would mean the existence of sets $B_{\rho_1,\ldots,\rho_k} = \{B_i \in (\mathsf{R} \otimes \mathsf{R})^k \mid i \in I\}$ such that for each $(\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j}) \in S_{\rho_1,\ldots,\rho_k}$ there exist $\gamma_{ij}, \delta_{ij} \in \mathsf{R}$ with $(\sum_{j=1}^{n_1} \alpha_{1,j} \otimes \beta_{1,j}, \ldots, \sum_{j=1}^{n_k} \alpha_{k,j} \otimes \beta_{k,j}) = \sum_{i \in I} \sum_{j=1}^{n_i} \gamma_{ij} \cdot B_i \cdot \delta_{ij}$. But even if this is possible it still remains the problem that we have to handle infinitely many sets of solutions associated to ordered subsets of a set admitting elements to occur more than once. This problem arises from the fact that in contrary to one-sided syzygy modules or syzygy modules in commutative structures the summands in the representations cannot be "collected" and "combined" in such a way that for a set R the sums can be written as a $\sum_{\rho \in R} \alpha_\rho \cdot \rho \cdot \beta_\rho$.

Let us close this section by illustrating the situation with two examples.

Example 3.4.10
Let $\Sigma = \{a, b\}$ and Σ^* the free monoid on the alphabet Σ. Further let $\mathsf{R} = \mathbb{Q}[\Sigma^*]$ the monoid ring over Σ^* and $\mathbb{Q}$. Let us look at the syzygy module of the set $\{a, b\} \subset \mathsf{R}$, i.e. the set of solutions of the equations $\sum_{j=1}^{n_1} \alpha_{1,j} \cdot a \cdot \beta_{1,j} + \sum_{j=1}^{n_2} \alpha_{2,j} \cdot b \cdot \beta_{2,j} = 0, \alpha_{i,j}, \beta_{i,j} \in \mathsf{R}$. Then we find $\{(-1 \otimes b, a \otimes 1), (-b \otimes 1, 1 \otimes a)\} \subseteq S_{a,b}$ and this set is a finite basis for $S_{a,b}$. $\diamond$

Example 3.4.11
Let $\mathcal{M}$ be the monoid presented by $(\{a, b, c\}; \{ab = a, ac = a, bc = b\})$ and $\mathsf{R} = \mathbb{Q}[\mathcal{M}]$ the monoid ring over $\mathcal{M}$ and $\mathbb{Q}$. Let us look at the syzygy module of the set $\{a, b\} \subset \mathsf{R}$. Then we find $\{(1 \otimes 1, -a \otimes c^i b^j) \mid i, j \in \mathbb{N}\} \subseteq S_{a,b}$ and hence $S_{a,b}$ has no finite basis. $\diamond$

Hence the task of two-sided syzygies is much more complicated than the one-sided case. This was also observed by Apel for graded structures where we have more structural information [Ape98].

3.5 Polynomial Rings over Reduction Rings

For a ring R with a reduction relation $\Longrightarrow$ fulfilling (A1) – (A3) we adopt the usual notations in $\mathsf{R}[X]$ the polynomial ring in one variable X where multiplication is denoted by $\star$. Notice that for scalar multiplication with $\alpha \in \mathsf{R}$ we assume

$\alpha \cdot X = X \cdot \alpha$ (see [Pes97] for other possibilities). We specify an ordering on the set of terms 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[19]. Note that for any two terms t and s such that t divides s we have $C(t, \mathfrak{i}) \subseteq C(s, \mathfrak{i})$. This follows, as for $s = t \star u$, $u \in \{X^i \mid i \in \mathbb{N}\}$, we find that $\mathsf{HC}(f) \in C(t, \mathfrak{i})$ implies $\mathsf{HC}(f \star u) = \mathsf{HC}(f) \in C(s, \mathfrak{i})$ since $f \in \mathfrak{i}$ implies $f \star u \in \mathfrak{i}$.

We additionally 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 $\alpha \stackrel{+}{\Longrightarrow}_B \beta$. 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 this ordering in general is neither total nor Noetherian on $\mathsf{R}[X]$.

Definition 3.5.1
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 one step, denoted by $p \longrightarrow_f q$, if

(a) $\mathsf{HT}(f)$ divides X^i, i.e. $\mathsf{HT}(f) \star X^j = X^i$ 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) $q = p - \sum_{i=1}^{k} (\gamma_i \cdot f \cdot \delta_i) \star X^j$. $\diamond$

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. Hence termination of this reduction cannot be shown by arguments involving terms only as in the case of polynomial rings over fields. But when using a *finite* set of polynomials for 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 the reduction relation as defined in Definition 3.5.1 is Noetherian when using *finite* sets of polynomials. Therefore it fulfills Axiom (A1). It is easy to see that (A2) and (A3) are also true and if the reduction relation $\Longrightarrow$ satisfies (A4) this is inherited by the reduction relation $\longrightarrow$ in $\mathsf{R}[X]$.

[19] We run into similar problems as in the module case in Section 3.4 as we cannot conclude that the ideal $C(t, \mathfrak{i})$ is finitely generated from the fact that $\mathfrak{i}$ is.

Theorem 3.5.2
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 as R is Noetherian. We only have to prove that every 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 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 $C(X^0, \mathfrak{i})$ in R, which must exist since R is supposed to be Noetherian and a reduction ring. 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 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 $\mathfrak{i}$ in G_i such that $\mathsf{HM}(p) = \alpha \cdot X^i$. Notice that in this construction we use the axiom of choice, when choosing the p_α from the infinite set $\mathfrak{i}$, and hence the construction 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. Hence G is at least a wesk Gröbner basis.
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 hence 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 $\mathfrak{i}$.

q.e.d.

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

Corollary 3.5.3
If $(\mathsf{R}, \Longrightarrow)$ *is a Noetherian reduction ring, then* $\mathsf{R}[X_1, \ldots, X_n]$ *is a Noetherian reduction ring with the respective extended reduction relation.*

Notice that other definitions of reduction relations in $\mathsf{R}[X_1, \ldots, X_n]$ 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 3.5.2 can be generalized for these cases.

Moreover, these results also hold for weak reduction rings.

Corollary 3.5.4
If $(\mathsf{R}, \Longrightarrow)$ *is a Noetherian weak reduction ring, then* $\mathsf{R}[X_1, \ldots, X_n]$ *is a Noetherian weak reduction ring with the respective extended reduction relation.*

Proof :
This follows immediately by using weak Gröbner bases G_i for the definition of G in the proof of Theorem 3.5.2. As before the property that for all $p \in \mathfrak{i}$ we have $p \overset{*}{\longrightarrow}_G 0$ and G generates $\mathfrak{i}$ follows immediately from the construction of G. Hence the result holds for $\mathsf{R}[X_1]$ and can be extended to $\mathsf{R}[X_1, \ldots, X_n]$.

q.e.d.

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 3.5.1 are computable operations. However, the proof of Theorem 3.5.2 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 is needed.

In order to provide completion procedures to compute 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. [KN85, KRK84, Mor89]). A general approach to characterize commutative reduction rings allowing the computation of Gröbner bases using Buchberger's approach was presented by Stifter in [Sti87].

Let us 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 $\sum_{i=1}^{n} g_i \star f_i \star h_i$, $g_i, h_i \in \mathsf{R}[X]$, $f_i \in F$ such that the head terms $\mathsf{HT}(g_i \star f_i \star h_i)$ are all the same within the representation. Then on one hand the respective coefficients $\mathsf{HC}(g_i \star f_i \star h_i)$ can add up to zero which in the commutative case means that the sum of the head coefficients is in an appropriate module generated by the coefficients $\mathsf{HC}(f_i)$ — m(odule)-polynomials are related to these situations. If the result is not zero the sum of the coefficients $\mathsf{HC}(g_i \star f_i \star h_i)$ as in the commutative case can be described in terms of a Gröbner basis of the coefficients $\mathsf{HC}(f_i)$ — g(röbner)-polynomials are related to these situations. Zero divisors in the reduction ring occur as a special instance of m-polynomials where $F = \{f\}$ and $\alpha \star f \star \beta$, $\alpha, \beta \in \mathsf{R}$ 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.

Let us become more precise and look into the definitions of m- and g-polynomials for the special case of rings with *right* reduction relations.

Definition 3.5.5
Let $P = \{p_1, \ldots, p_k\}$ be a finite set of polynomials in $\mathsf{R}[X]$, $u_1, \ldots, u_k$ terms in $\{X^j \mid j \in \mathbb{N}\}$ such that for the term $t = \max\{\mathsf{HT}(p_i) \mid 1 \leq i \leq k\}$ we have $t = \mathsf{HT}(p_i) \star u_i$ and $\gamma_i = \mathsf{HC}(p_i)$ for $1 \leq i \leq k$.
Let G be a right Gröbner basis of the right ideal generated by $\{\gamma_i \mid 1 \leq i \leq k\}$ in R and

$$\alpha = \sum_{i=1}^{k} \gamma_i \cdot \beta_i^{\alpha}$$

for $\alpha \in G$, $\beta_i^{\alpha} \in \mathsf{R}$. Then we define the **g-polynomials (Gröbner polynomials)** corresponding to P and t by setting

$$g_{\alpha} = \sum_{i=1}^{k} p_i \star u_i \cdot \beta_i^{\alpha}$$

where $\mathsf{HT}(p_i) \star u_i = t$. Notice that $\mathsf{HM}(g_{\alpha}) = \alpha \cdot t$.
For the right module $M = \{(\delta_1, \ldots, \delta_k) \mid \sum_{i=1}^{k} \gamma_i \cdot \delta_i = 0\}$, let the set $\{B_j \mid j \in I_M\}$

be a basis with $B_j = (\beta_{j,1}, \ldots, \beta_{j,k})$ for $\beta_{j,l} \in \mathsf{R}$ and $1 \leq l \leq k$. We define the **m-polynomials (module polynomials)** corresponding to P and t by setting

$$h_j = \sum_{i=1}^{k} p_i \star u_i \cdot \beta_{j,i} \text{ for each } j \in I_M$$

where $\mathsf{HT}(p_i) \star u_i = t$. Notice that $\mathsf{HT}(h_j) \prec t$ for each $j \in I_M$. $\diamond$

Given a set of polynomials F the corresponding m- and g-polynomials are those resulting for every subset $P \subseteq F$ according to this definition.

In case we want effectiveness, we have to require that the bases in this definition are computable. Of course for commutative reduction rings the definition extends to characterize two-sided ideals. However, the whole situation 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. Moreover the set of m-polynomials is a much more complicated structure. 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 [KRW90]. But the general case is much more involved, see Definition 3.5.6 below.

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

Using m- and g-polynomials, right Gröbner bases can be characterized similar to the characterizations in terms of syzygies (a direct generalization of the approaches by Kapur and Narendran in [KN85] respectively Möller in [Mor89]): In case for the respective subsets $P \subseteq F$ the respective terms $t = \max\{\mathsf{HT}(p) \mid p \in P\}$ only give rise to finitely many m- and g-polynomials, these situations can be localized to finitely many terms. One can provide a completion procedure based on this characterization which will indeed compute a finite right Gröbner basis if R is Noetherian. In principal ideal rings, where the function gcd (greatest common divisor) is defined it is sufficient to consider subsets $P \subseteq F$ of size 2 (compare [KN85]).

Now let us look at two-sided ideals and two-sided reduction relations.

Definition 3.5.6
Let $P = \{p_1, \ldots, p_k\}$ be a finite set of polynomials in $\mathsf{R}[X]$, $u_1, \ldots, u_k$ terms in $\{X^j \mid j \in \mathbb{N}\}$ such that for the term $t = \max\{\mathsf{HT}(p_i) \mid 1 \leq i \leq k\}$ we have $t = \mathsf{HT}(p_i) \star u_i$ and $\gamma_i = \mathsf{HC}(p_i)$ for $1 \leq i \leq k$.
Let G be a Gröbner basis of the ideal generated by $\{\gamma_i \mid 1 \leq i \leq k\}$ in R and

$$\alpha = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j}^{\alpha} \cdot \gamma_i \cdot \delta_{i,j}^{\alpha}$$

for $\alpha \in G$, $\beta^{\alpha}_{i,j}, \delta^{\alpha}_{i,j} \in \mathsf{R}$, $1 \leq i \leq k$,$1 \leq j \leq n_i$. Then we define the **g-polynomials (Gröbner polynomials)** corresponding to P and t by setting

$$g_\alpha = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta^{\alpha}_{i,j} \cdot p_i \star u_i \cdot \delta^{\alpha}_{i,j}$$

where $\mathsf{HT}(p_i) \star u_i = t$. Notice that $\mathsf{HM}(g_\alpha) = \alpha \cdot t$.
We define the **m-polynomials (module polynomials)** corresponding to P and t as

$$h = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j} \cdot p_i \star u_i \cdot \delta_{i,j}$$

where $\sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j} \cdot \gamma_i \cdot \delta_{i,j} = 0$. Notice that $\mathsf{HT}(h) \prec t$. $\diamond$

Given a set of polynomials F, the set of corresponding g- and m-polynomials contains those which are specified by Definition 3.5.6 for each subset $P \subseteq F$ fulfilling the respective conditions. For a set consisting of one polynomial the corresponding m-polynomials also 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. Notice that given a finite set of polynomials the corresponding sets of g- and m-polynomials in general can be infinite.

We can use g- and m-polynomials to characterize finite weak Gröbner bases. Notice that this characterization does not require R to be Noetherian. In order to characterize Gröbner bases in this fashion the Translation Lemma must hold for the reduction ring.

Theorem 3.5.7
Let F be a finite set of polynomials in $\mathsf{R}[X]\backslash\{0\}$. Then F is a weak Gröbner basis of the ideal it generates if and only if all g-polynomials and all m-polynomials corresponding to F as specified in Definition 3.5.6 reduce to zero.

Proof :
First let F be a weak Gröbner basis. By Definition 3.5.6 the g- and m-polynomials are elements of the ideal generated by F and hence reduce to zero using F.
It remains to show that every $g \in \mathsf{ideal}(F)\backslash\{0\}$ reduces to zero by F. Remember that for $g \in \mathsf{ideal}(F)$, $g \longrightarrow_F g'$ implies $g' \in \mathsf{ideal}(F)$. As $\longrightarrow_F$ is Noetherian[20], thus it suffices to show that every $g \in \mathsf{ideal}(F)\backslash\{0\}$ is $\longrightarrow_F$-reducible. Let $g = \sum_{i=1}^{m} \alpha_i \cdot f_i \star u_i \cdot \beta_i$ be an arbitrary representation of g with $\alpha_i, \beta_i \in \mathsf{R}$, $u_i \in \{X^j \mid j \in \mathbb{N}\}$, and $f_i \in F$ (not necessarily different polynomials). Depending on this representation of g and the degree ordering $\succeq$ on $\{X^j \mid j \in \mathbb{N}\}$ we define the maximal occurring term of this representation of g to be $t = \max\{\mathsf{HT}(f_i \star u_i) \mid$

[20]To achieve this we have demanded that F is finite.

$1 \leq i \leq m\}$ and K is the number of polynomials $f_i \star u_i$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$. We will show that G is reducible by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[21]. Without loss of generality let the first K multiples occurring in our representation of g be those with head term t, i.e., for $\sum_{i=1}^{K} \alpha_i \cdot f_i \star u_i \cdot \beta_i$ we have $\mathsf{HT}(f_i \star u_i) = t$ for $1 \leq i \leq K$, and $\mathsf{HT}(\alpha_i \cdot f_i \star u_i \cdot \beta_i) \prec t$ for $K < i \leq m$. In case $t \succ \mathsf{HT}(g)$ there is an m-polynomial corresponding to the set of polynomials $P = \{f_1, \ldots, f_K\}$ and by our assumption this polynomial is reducible to zero using F hence yielding the existence of a representation $\sum_{i=1}^{n} \gamma_i \cdot f_i \star v_i \cdot \delta_i$ with $t \succ \tilde{t} = \max\{\mathsf{HT}(f_i \star v_i) \mid i \in \{1, \ldots n\}\}$. We can then change the original representation of g by substituting this sum for $\sum_{i=1}^{K} \alpha_i \cdot f_i \star u_i \cdot \beta_i$ yielding a new representation with smaller maximal term than t.

On the other hand, if $t = \mathsf{HT}(g)$ then again we can assume that the first K multiples have head term t. In this case there exists a g-polynomial corresponding to the set of polynomials $P = \{f_1, \ldots, f_K\}$ and by our assumption this polynomial is reducible to zero using F. Now as the head monomial of the g-polynomial and the head monomial of g are equal, then g must be reducible by F as well.

q.e.d.

In order to characterize infinite sets F as weak Gröbner bases we have to be more careful since we can no longer assume that $\longrightarrow_F$ is terminating[22]. But inspecting the proof of the previous theorem closely we see that this is not necessary. Under the stronger assumption that the g-polynomial reduces to zero using reduction at head monomials only, i.e., we have a terminating reduction sequence using finitely many polynomials in F only, we can conclude that the polynomials used to extinguish the term t in the g-polynomial can equally be applied to extinguish the head monomial of g. Since there cannot be an infinite sequence of decreasing terms t one can show that g reduces to zero by iterating arguments involving g- and m-polynomials.

Corollary 3.5.8

Let F be a set of polynomials in $\mathsf{R}[X]\backslash\{0\}$. Then F is a weak Gröbner basis of the ideal it generates if and only if all g-polynomials and all m-polynomials corresponding to F as specified in Definition 3.5.6 reduce to zero using reduction at head monomials only.

Corollary 3.5.9

Let F be a set of polynomials in $\mathsf{R}[X]\backslash\{0\}$. Additionally let the Translation Lemma hold in R. Then F is a Gröbner basis of the ideal it generates if and

[21] Note that this ordering is well-founded since $\succ$ is well-founded on $\{X^j \mid j \in \mathbb{N}\}$ and $K \in \mathbb{N}$.

[22] This can of course be achieved by requiring the stronger axiom (A1') to hold for the reduction relation.

only if all g-polynomials and all m-polynomials corresponding to F as specified in Definition 3.5.6 reduce to zero using reduction at head monomials only.

Still the problem remains that the set of m-polynomials does not have a nice characterization as an algebraic structure. Remember that in the one-sided case or the case of commutative reduction rings the m-polynomials for a finite set of polynomials P correspond to submodules of $\mathsf{R}^{|P|}$, as they correspond to solutions of linear equations. When attempting to describe the setting for two-sided ideals in non-commutative reduction rings one runs into the same problems as in the previous section on modules.

Chapter 4

Function Rings

In the literature Gröbner bases and reduction relations have been introduced to various algebraic structures such as the classical commutative polynomial rings over fields, non-commutative polynomial rings over fields, commutative polynomial rings over reduction rings, skew polynomial rings, Lie algebras, monoid and group rings and many more. This chapter is intended to give a generalized setting subsuming these approaches and outlining a framework for introducing reduction relations and Gröbner bases to other structures fitting the appropriate requirements. An additional aim was to work out what conditions are necessary at what point in order to give more insight into the ideas behind algebraic characterizations such as specialized standard representations for ideal elements as well as into the idea of using rewriting techniques for achieving confluent reduction relations describing the ideal congruence.

This chapter is organized as follows: Section 4.1 introduces the general structure we are looking into called function rings. Section 4.2 gives the algebraic characterization for the case of right ideals in form of right standard representations. To work out the difficulties involved by our notion of terms and coefficients separately, Section 4.2.1 first treats the easier case of function rings over fields while Section 4.2.2 then goes into the details when taking a reduction ring as introduced in Chapter 3 as coefficient domain. Since for function rings over general reduction rings only a feasible characterization of weak Gröbner bases is possible, we show that this situation can be improved when looking at the special case of function rings over the integers in Section 4.2.3. Section 4.3 is dedicated to the study of a generalization of the concept of right ideals – right modules. The remaining Sections 4.4 – 4.5 then treat the same concepts and problems now in the more complex setting of two-sided ideals.

4.1 The General Setting

Let $\mathcal{T}$ be a set and let $\mathsf{R} = (\mathsf{R}, +, \cdot, 0, 1)$ be an associative ring with 1. By $\mathcal{F}_{\mathsf{R}}^{\mathcal{T}}$ we will denote the set of all functions $f : \mathcal{T} \longrightarrow \mathsf{R}$ with finite **support** $\mathsf{supp}(f) = \{t \mid t \in \mathcal{T}, f(t) \neq 0\}$. We will simply write $\mathcal{F}$ if the context is clear. By o we will denote the function with empty support, i.e., $\mathsf{supp}(o) = \emptyset$. This function will be called the **zero function**. Two elements of $\mathcal{F}$ are equal if they are equal as functions, i.e., they have the same support and coincide in their respective values. We require the set $\mathcal{T}$ to be independent in the sense that a function f has unique support.

$\mathcal{F}$ can be viewed as a group with respect to a binary operation

$$\oplus : \mathcal{F} \times \mathcal{F} \longrightarrow \mathcal{F}$$

called **addition** by associating to f, g in $\mathcal{F}$ the function in $\mathcal{F}$, denoted by $f \oplus g$, which has support $\mathsf{supp}(f \oplus g) \subseteq \mathsf{supp}(f) \cup \mathsf{supp}(g)$ and values $(f \oplus g)(t) = f(t) + g(t)$ for $t \in \mathsf{supp}(f) \cup \mathsf{supp}(g)$. The zero function o fulfills $o \oplus f = f \oplus o = f$, hence is neutral with respect to $\oplus$. For an element $f \in \mathcal{F}$ we define the element $-f$ with $\mathsf{supp}(-f) = \mathsf{supp}(f)$ and for all $t \in \mathsf{supp}(f)$ the value of $(-f)(t)$ is the inverse of the element $f(t)$ with respect to $+$ in R denoted by $-f(t)$. Notice that since in R every element has such an inverse the inverse of an element in $\mathcal{F} \backslash \{o\}$ is always defined. Then $-f$ is the (left and right) inverse of f, since $f \oplus (-f)$ as well as $(-f) \oplus f$ equals o, i.e., has empty support. This follows as for all $t \in \mathsf{supp}(f)$ we have $(f \oplus (-f))(t) = f(t) + (-f)(t) = f(t) - f(t) = 0 = -f(t) + f(t) = (-f)(t) + f(t) = ((-f) \oplus f)(t)$. We will write $f - g$ to abbreviate $f \oplus (-g)$ for f, g in $\mathcal{F}$. If the context is clear we will also write $f + g$ instead of $f \oplus g$. Notice that $(\mathcal{F}, \oplus, o)$ is an Abelian group since $(\mathsf{R}, +, 0)$ is Abelian. Sums of functions $f_1, \ldots, f_m$ will be abbreviated by $f_1 \oplus \ldots \oplus f_m = \sum_{i=1}^{m} f_i$ as usual. Now if R is a computable ring[1], then $(\mathcal{F}, \oplus)$ is a computable group.

In the next lemma we provide a syntactical representation for elements of the function ring.

Lemma 4.1.1
Every $f \in \mathcal{F} \backslash \{o\}$ has a finite representation of the form

$$f = \sum_{t \in \mathsf{supp}(f)} m_t$$

where $m_t \in \mathcal{F}$ such that $\mathsf{supp}(m_t) = \{t\}$ and $f(t) = m_t(t)$. The representation of o is the empty sum.

Proof :
This can be shown by induction on $n = |\mathsf{supp}(f)|$. For $n = 0$ we have the empty

[1] A ring R is called computable, if the ring operations $+$ and $\cdot$ are computable, i.e. for $\alpha, \beta \in \mathsf{R}$ we can compute $\alpha + \beta$ and $\alpha \cdot \beta$.

sum which is the zero function o and are done. Hence let $\mathsf{supp}(f) = \{t_1, \ldots, t_n\}$ and $n > 0$. Furthermore let $f(t_1) = \alpha \in \mathsf{R}$ and $m \in \mathcal{F}$ be the unique function with $\mathsf{supp}(m) = \{t_1\}$ and $m(t_1) = \alpha$. Then there exists an inverse function $-m$ and a function $(-m) \oplus f \in \mathcal{F}$ such that

$$f = (m \oplus (-m)) \oplus f = m \oplus ((-m) \oplus f)$$

and $\mathsf{supp}((-m) \oplus f) = \{t_2, \ldots t_n\}$. Hence by our induction hypothesis $\mathsf{supp}((-m) \oplus f)$ has a representation $\sum_{t \in \{t_2, \ldots t_n\}} m_t$ yielding

$$f = m \oplus ((-m) \oplus f) = m \oplus \sum_{t \in \{t_2, \ldots t_n\}} m_t = \sum_{t \in \mathsf{supp}(f)} m_t$$

with $m_{t_1} = m$.

q.e.d.

This presentation is unique up to permutations. We will call such a representation of an element as a formal sum of special functions a **polynomial representation** or a **polynomial** to stress the similarity with the objects known as polynomials in other fields of mathematics. Polynomial representations in terms of these functions are unique up to permutations of the respective elements of their support. Since these special functions are of interest we define the following subsets of $\mathcal{F}$:

$$\mathsf{M}(\mathcal{F}) = \{f \in \mathcal{F} \mid |\mathsf{supp}(f)| = 1\}$$

will be called the set of **monomial functions** or **monomials** in $\mathcal{F}$. Monomials will often be denoted by m_t where the suffix t is the element of the support, i.e., $\mathsf{supp}(m_t) = \{t\}$. A subset of this set, namely

$$\mathsf{T}(\mathcal{F}) = \{m_t \in \mathsf{M}(\mathcal{F}) \mid m_t(t) = 1\}$$

where 1 denotes the unit in R will be called the set of **term functions** or **terms** of $\mathcal{F}$. Notice that this set can be viewed as an embedding of $\mathcal{T}$ in $\mathcal{F}$ via the mapping $t \longmapsto f$ with $\mathsf{supp}(f) = \{t\}$ and $f(t) = 1$.

Further we assume the existence of a second binary operation called **multiplication**

$$\star : \mathcal{F} \times \mathcal{F} \longrightarrow \mathcal{F}$$

such that $(\mathcal{F}, \oplus, \star, o)$ is a ring. In particular we have $o \star f = f \star o = o$ for all f in $\mathcal{F}$. This ring is called a **function ring**[2]. In case $\star$ is a computable operation, $\mathcal{F}$ is a computable function ring.

[2]Notice that in the literature the term function ring is usually restricted to those rings where the multiplication is defined pointwise as in Example 4.1.3. Here we want to allow more interpretations for $\star$.

Definition 4.1.2
An element $\mathbf{1}^r_{\mathcal{F}} \in \mathcal{F}$ is called a **right unit** of $\mathcal{F}$ if for all $f \in \mathcal{F}$ we have $f \star \mathbf{1}^r_{\mathcal{F}} = f$. Similarly $\mathbf{1}^\ell_{\mathcal{F}} \in \mathcal{F}$ is called a **left unit** of $\mathcal{F}$ if for all $f \in \mathcal{F}$ we have $\mathbf{1}^\ell_{\mathcal{F}} \star f = f$. An element $\mathbf{1}_{\mathcal{F}} \in \mathcal{F}$ is called a **unit** if for all $f \in \mathcal{F}$ we have $\mathbf{1}_{\mathcal{F}} \star f = f \star \mathbf{1}_{\mathcal{F}} = f$.
$\diamond$

In general $\mathcal{F}$ need not have a left or right unit. If $\mathcal{F}$ does not have a unit this can be achieved by enlarging the set $\mathcal{T}$ by a new element, say Λ, and associating to Λ a function f_Λ with support $\{\Lambda\}$ and $f_\Lambda(\Lambda) = 1$. The definition of $\star$ must be extended such that for all $f \in \mathcal{F}$ we have $f \star f_\Lambda = f_\Lambda \star f = f$. Similarly we could add a left or right unit by requiring $f \star f^r_\Lambda = f$ respectively $f^\ell_\Lambda \star f = f$. When adding a new element f_Λ as a unit to $\mathcal{F}$ we have $f_\Lambda \in \mathsf{T}(\mathcal{F}) \subseteq \mathsf{M}(\mathcal{F})$.

We will not specify our ring multiplication $\star$ further at the moment except for giving some examples.

Our first example outlines the situation for multiplying two elements by multiplying the respective values of the support. This is the definition of multiplication normally associated to function rings in the mathematical literature.

Example 4.1.3
Let us specify our multiplication $\star$ by associating to f, g in $\mathcal{F}$ the function in $\mathcal{F}$, denoted by $f \star g$, which has support $\mathsf{supp}(f \star g) \subseteq \mathsf{supp}(f) \cap \mathsf{supp}(g)$ and values $(f \star g)(t) := f(t) \cdot g(t)$ for $t \in \mathsf{supp}(f) \cap \mathsf{supp}(g)$. Notice that in this case $\mathcal{F}$ can only contain a (right, left) unit if $\mathcal{T}$ is finite, since otherwise a unit function would have infinite support and hence be no element of $\mathcal{F}$. But the set of special functions $u_S = \sum_{t \in S} u_t$ where $S \subseteq \mathcal{T}$ finite, $\mathsf{supp}(u_t) = \{t\}$ and $u_t(t) = 1$ is an approximation of a unit, since for every function f in $\mathcal{F}$ and all functions u_S with $\mathsf{supp}(f) \subseteq S$ we have $f \star u_S = u_S \star f = f$. However, if we want a real unit, adding a new symbol Λ to $\mathcal{T}$ and f_Λ with $f_\Lambda(\Lambda) = 1$ to $\mathcal{F}$ together with an extension of the definition of $\star$ by $f_\Lambda \star f = f \star f_\Lambda = f$ for all $f \in \mathcal{F}$ will do the trick. $\diamond$

Remember that by Lemma 4.1.1 polynomials have representations of the form $f = \sum_{t \in \mathsf{supp}(f)} m_t$ and $g = \sum_{s \in \mathsf{supp}(g)} n_s$ yielding

$$f \star g = (\sum_{t \in \mathsf{supp}(f)} m_t) \star (\sum_{s \in \mathsf{supp}(g)} n_s) = \sum_{t \in \mathsf{supp}(f), s \in \mathsf{supp}(g)} m_t \star n_s$$

since the multiplication $\star$ must satisfy the distributivity law of the ring axioms. Hence knowing the behaviour of the multiplication for monomials, i.e. $\star : \mathsf{M}(\mathcal{F}) \times \mathsf{M}(\mathcal{F}) \longrightarrow \mathcal{F}$, is enough to characterize the multiplication $\star$.

For all examples from the literature mentioned in this work, we can even state that the multiplication can be defined by specifying $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}$, and then lifting it to $\mathsf{M}(\mathcal{F})$ and $\mathcal{F}$. This is done by defining $m_t \star n_s = (m_t(t) \cdot n_s(s)) \cdot (t \star s)$ and extending this to the formal sums of monomials[3].

[3]Notice that this lifting requires that when writing a monomial m_t as $m_t(t) \cdot t$ we have $m_t(t) \cdot t = t \cdot m_t(t)$.

A well-known example for the special instance $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ are the polynomial rings from Section 2.3.

Example 4.1.4
For a set of variables $X_1, \ldots, X_n$ let us define the set of commutative terms $\mathcal{T} = \{X_1^{i_1} \ldots X_n^{i_n} \mid i_1, \ldots i_n \in \mathbb{N}\}$ and let $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ be the set of all functions $f : \mathcal{T} \longrightarrow \mathbb{Q}$ with finite support, where $\mathbb{Q}$ are the rational numbers. Multiplication $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ is specified as $X_1^{i_1} \ldots X_n^{i_n} \star X_1^{j_1} \ldots X_n^{j_n} = X_1^{i_1+j_1} \ldots X_n^{i_n+j_n}$. Hence here we have an example where the set $\mathcal{T}$ is a monoid with unit element $X_1^0 \ldots X_n^0$. Then $\mathcal{F}$ can be interpreted as the ordinary polynomial ring $\mathbb{Q}[X_1, \ldots, X_n]$ with the usual multiplication $(\alpha \cdot t) \star (\beta \cdot s) = (\alpha \cdot \beta) \cdot (t \star s)$ where $\alpha, \beta \in \mathbb{Q}, s, t \in \mathcal{T}$. $\diamond$

Notice that in this example the unit element is an element of the set $\mathcal{T}$ embedded in $\mathcal{F}$. This does not have to be the case as the next example shows.

Example 4.1.5
Let us fix a finite set $\mathcal{T} = \{e_{11}, e_{12}, e_{21}, e_{22}\}$ and let $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ be the set of all functions $f : \mathcal{T} \longrightarrow \mathbb{Q}$, where $\mathbb{Q}$ are the rational numbers. We specify the multiplication $\star$ on $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ by the action on $\mathcal{T}$ as follows: $e_{ij} \star e_{kl} = o$ in case $j \neq k$ and $e_{ij} \star e_{jl} = e_{il}$ for $i, j, l, k \in \{1, 2\}$. Then multiplication is not Abelian since $e_{11} \star e_{12} = e_{12}$ whereas $e_{12} \star e_{11} = o$. $(\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}, \oplus, \star, o)$ is a ring, in fact isomorphic to the ring of 2×2 rational matrices[4] It contains a unit element, namely $e_{11} + e_{22}$. $\diamond$

Notice that in this example the unit element is *not* an element of the set $\mathcal{T}$ embedded in $\mathcal{F}$. Moreover, the multiplication here arises from the situation $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T} \cup \{o\}$. The next example even allows multiplications of terms to result in polynomials, i.e., $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}$.

Example 4.1.6
For a set of variables X_1, X_2, X_3 let us define the set of commutative terms $\mathcal{T} = \{X_1^{i_1} X_2^{i_2} X_3^{i_3} \mid i_1, i_2, i_3 \in \mathbb{N}\}$ and let $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ be the set of all functions $f : \mathcal{T} \longrightarrow \mathbb{Q}$ with finite support, where $\mathbb{Q}$ are the rational numbers. Multiplication $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}$ is lifted from the following multiplication of the variables: $X_2 \star X_1 = X_2 + X_3$, $X_3 \star X_1 = X_1 X_3$, $X_3 \star X_2 = X_2 X_3$ and $X_i \star X_j = X_i X_j$ for $i < j$. Then $\mathcal{F}$ can be interpreted as a skew-polynomial ring $\mathbb{Q}[X_1, X_2, X_3]$ with unit element $X_1^0 X_2^0 X_3^0 \in \mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$. $\diamond$

Finally, many examples for function rings will be taken from monoid rings and hence we close this subsection by giving an example of a monoid ring.

[4] This interpretation can be extended to arbitrary rings of $n \times n$ matrices over a field $\mathbb{K}$ by setting $\mathcal{T} = \{e_{ij} \mid 1 \leq i, j \leq n\}$, $e_{ij} \star e_{kl} = o$ in case $j \neq k$ and $e_{ij} \star e_{jl} = e_{il}$ else. The unit element then is $e_{11} + \ldots + e_{nn}$.

Example 4.1.7
Let $\mathcal{T} = \{a^i, b^i, 1 \mid i \in \mathbb{N}^+\}$, where 1 is the empty word in $\{a,b\}^*$, and let the multiplication $\star$ be defined by the following multiplication table:

	1	a^j	b^j
1	1	a^j	b^j
a^i	a^i	a^{i+j}	$a^{i \text{ monus } j} b^{j \text{ monus } i}$
b^i	b^i	$a^{j \text{ monus } i} b^{i \text{ monus } j}$	b^{i+j}

where $i, j \in \mathbb{N}^+$ and $i \text{ monus } j = i - j$ if $i \geq j$ and 0 else. In fact $\mathcal{T}$ is the free group on one generator which can be presented as a monoid by $(\{a,b\}; \{ab = ba = 1\})$. Let $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ be the set of all functions $f : \mathcal{T} \longrightarrow \mathbb{Q}$ with finite support. Then $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ is a ring and is known as a special case of the free group ring. Its unit element is $1 \in \mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$. ◇

For the special case that we have $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$, and some subring $\mathsf{R}' \subseteq \mathsf{R}$ we get that the function ring $\mathcal{F}_{\mathsf{R}'}^{\mathcal{T}}$ is a subring of $\mathcal{F}_{\mathsf{R}}^{\mathcal{T}}$. This follows directly as then for $f, g \in \mathcal{F}_{\mathsf{R}'}^{\mathcal{T}}$ we have $f + (-g), f \star g \in \mathcal{F}_{\mathsf{R}'}^{\mathcal{T}}$. This is no longer true if $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}_{\mathsf{R}}^{\mathcal{T}}$. Let $\mathsf{R} = \mathbb{Q}$, $\mathsf{R}' = \mathbb{Z}$ and $\mathcal{T} = \{X_1^i X_2^j \mid i, j \in \mathbb{N}\}$ with $\star$ induced by $X_2 \star X_1 = \frac{1}{2} \cdot X_1 X_2$, $X_1 \star X_2 = X_1 X_2$. Then for $X_2, X_1 \in \mathcal{F}_{\mathbb{Z}}^{\mathcal{T}}$ we get $X_2 \star X_1 = \frac{1}{2} \cdot X_1 X_2 \in \mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$.

Similarly, if we have $\mathcal{T}' \subseteq \mathcal{T}$ and $\star : \mathcal{T}' \times \mathcal{T}' \longrightarrow \mathcal{F}_{\mathsf{R}}^{\mathcal{T}'}$, then $\mathcal{F}_{\mathsf{R}}^{\mathcal{T}'}$ is a subring of $\mathcal{F}_{\mathsf{R}}^{\mathcal{T}}$. Again this follows as for $f, g \in \mathcal{F}_{\mathsf{R}}^{\mathcal{T}'}$ we have $f + (-g), f \star g \in \mathcal{F}_{\mathsf{R}}^{\mathcal{T}'}$. Let us review Example 4.1.6: There we have $\mathcal{T} = \{X_1^{i_1} X_2^{i_2} X_3^{i_3} \mid i_1, i_2, i_3 \in \mathbb{N}\}$ and the multiplication $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$ is lifted from the following multiplication of the variables: $X_2 \star X_1 = X_2 + X_3$, $X_3 \star X_1 = X_1 X_3$, $X_3 \star X_2 = X_2 X_3$ and $X_i \star X_j = X_i X_j$ for $i < j$. Then for $\mathcal{T}' = \{X_2^{i_2} X_3^{i_3} \mid i_2, i_3 \in \mathbb{N}\}$ we have $\star : \mathcal{T}' \times \mathcal{T}' \longrightarrow \mathcal{F}_{\mathbb{Q}}^{\mathcal{T}'}$ and hence $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}'}$ is a subring of $\mathcal{F}_{\mathbb{Q}}^{\mathcal{T}}$.

4.2 Right Ideals and Right Standard Representations

Since $\mathcal{F}$ is a ring, we can define right, left or two-sided ideals. In this section in a first step we will restrict our attention to one-sided ideals, in particular to right ideals since left ideals in general can be treated in a symmetrical manner.

A subset $\mathfrak{i} \subseteq \mathcal{F}$ is called a **right ideal**, if

1. $o \in \mathfrak{i}$,

2. for $f, g \in \mathfrak{i}$ we have $f \oplus g \in \mathfrak{i}$, and
3. for $f \in \mathfrak{i}$, $g \in \mathcal{F}$ we have $f \star g \in \mathfrak{i}$.

Right ideals can also be specified in terms of generating sets. For $F \subseteq \mathcal{F} \backslash \{o\}$ let $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{n} f_i \star g_i \mid f_i \in F, g_i \in \mathcal{F}, n \in \mathbb{N}\} = \{\sum_{i=1}^{n} f_i \star m_i \mid f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}\}$. These generated sets are subsets of $\mathcal{F}$ since for $f, g \in \mathcal{F}$ $f \star g$ as well as $f \oplus g$ are again elements of $\mathcal{F}$, and it is easily checked that they are in fact right ideals:

1. $o \in \mathsf{ideal}_r(F)$ since o can be written as the empty sum.
2. For two elements $\sum_{i=1}^{n} f_i \star g_i$ and $\sum_{j=1}^{m} f_j \star h_j$ in $\mathsf{ideal}_r(F)$, the resulting sum $\sum_{i=1}^{n} f_i \star g_i \oplus \sum_{j=1}^{m} f_j \star h_j$ is again an element in $\mathsf{ideal}_r(F)$.
3. For an element $\sum_{i=1}^{n} f_i \star g_i$ in $\mathsf{ideal}_r(F)$ and a polynomial h in $\mathcal{F}$, the product $(\sum_{i=1}^{n} f_i \star g_i) \star h = \sum_{i=1}^{n} f_i \star (g_i \star h)$ is again an element in $\mathsf{ideal}_r(F)$.

Given a right ideal $\mathfrak{i} \subseteq \mathcal{F}$ we call a set $F \subseteq \mathcal{F} \backslash \{o\}$ a **basis** or a **generating set** of $\mathfrak{i}$ if $\mathfrak{i} = \mathsf{ideal}_r(F)$. Then every element $g \in \mathsf{ideal}_r(F) \backslash \{o\}$ has different representations of the form

$$g = \sum_{i=1}^{n} f_i \star h_i, f_i \in F, h_i \in \mathcal{F}, n \in \mathbb{N}.$$

Of course the distributivity law in $\mathcal{F}$ then allows to convert any such representation into one of the form

$$g = \sum_{j=1}^{m} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), m \in \mathbb{N}.$$

As we have seen in Section 1.3, it is not obvious whether some polynomial belongs to an ideal. Let again $f_1 = X_1^2 + X_2$ and $f_2 = X_1^2 + X_3$ be two polynomials in the polynomial ring $\mathbb{Q}[X_1, X_2, X_3]$ and $\mathfrak{i} = \{f_1 * g_1 + f_2 * g_2 \mid g_1, g_2 \in \mathbb{Q}[X_1, X_2, X_3]\}$ the (right) ideal generated by them. It is not hard to see that the polynomial $X_2 - X_3$ belongs to $\mathfrak{i}$ since $X_2 - X_3 = f_1 - f_2$ is a representation of $X_2 - X_3$ in terms of f_1 and f_2. The same is true for the polynomial $X_2^2 - X_2X_3$ where now we have to use multiples of f_1 and f_2, namely $X_2^2 - X_2X_3 = f_1 \star X_2 - f_2 \star X_2$. However, when looking at the polynomial $X_3^3 + X_1 + X_3$ we find that there is no obvious algorithm to find such appropriate multiples. The problem is that for an arbitrary generating set for an ideal we have to look at arbitrary polynomial multiples with no boundary. One first improvement for the situation can be achieved if we can represent ideal elements by special representations in terms of the given generating set. In polynomial rings such representations are studied as variations of the term **standard representations** in the literature (see also Section 2.3). They will also be introduced in this setting. Since standard representations are in general distinguished by conditions involving an ordering on the set of polynomials, we will start by introducing the notion of an ordering to $\mathcal{F}$.

Let $\succeq$ be a total well-founded ordering on the set $\mathcal{T}$. This enables us to make our polynomial representations of functions unique by using the ordering $\succeq$ to arrange the elements of the support:

$$f = \sum_{i=1}^{k} m_{t_i}, \text{ where } \mathsf{supp}(f) = \{t_1, \ldots, t_k\}, t_1 \succ \ldots \succ t_k.$$

Using the ordering $\succeq$ on $\mathcal{T}$ we are now able to give some notions for polynomials which are essential in introducing standard representations, standard bases and Gröbner bases in the classical approach. We call the monomial with the largest term according to $\succeq$ the **head monomial** of f denoted by $\mathsf{HM}(f)$, consisting of the **head term** denoted by $\mathsf{HT}(f)$ and the **head coefficient** denoted by $\mathsf{HC}(f) = f(\mathsf{HT}(f))$. $f - \mathsf{HM}(f)$ is called the **reductum** of f denoted by $\mathsf{RED}(f)$. Note that $\mathsf{HM}(f) \in \mathsf{M}(\mathcal{F})$, $\mathsf{HT}(f) \in \mathcal{T}$ and $\mathsf{HC}(f) \in \mathsf{R}$. These notions can be extended to sets of functions $F \subseteq \mathcal{F}\backslash\{o\}$ by setting $\mathsf{HM}(F) = \{\mathsf{HM}(f) \mid f \in F\}$, $\mathsf{HT}(F) = \{\mathsf{HT}(f) \mid f \in F\}$ and $\mathsf{HC}(F) = \{\mathsf{HC}(f) \mid f \in F\}$.

Notice that for some polynomial $f = \sum_{i=1}^{k} m_{t_i} \in \mathcal{F}$, and some term $t \in \mathcal{T}$ we cannot conclude that for the terms occurring in the multiple $f \star t = \sum_{i=1}^{k} m_{t_i} \star t$ we have $t_1 \star t \succ \ldots \succ t_k \star t$ (in case the multiplication of terms again results in terms) or $\mathsf{HT}(t_1 \star t) \succ \ldots \succ \mathsf{HT}(t_k \star t)$ as the ordering need not be compatible with multiplication in $\mathcal{F}$.

Example 4.2.1
Let $\mathcal{T} = \{x, 1\}$ and $\star$ induced by the following multiplication on $\mathcal{T}$: $x \star x = 1 \star 1 = 1$, $x \star 1 = 1 \star x = x$. Then assuming $x \succ 1$, after multiplying both sides of the equation with x, we get $x \star x = 1 \prec 1 \star x = x$. On the other hand, assuming the precedence $1 \succ x$ similarly we get $x = 1 \star x \prec 1 = x \star x$. Hence the ordering is not compatible with multiplication using elements in $\mathcal{T}$. ◇

We will later on see that this lack of compatibility leads to additional requirements when defining standard representations, standard bases and Gröbner bases. Since the elements of $\mathcal{T}$ can be identified with the terms in $\mathsf{T}(\mathcal{F})$, the ordering $\succeq$ can be extended as a total well-founded[5] ordering on $\mathsf{T}(\mathcal{F})$. Additionally we can provide orderings on $\mathsf{M}(\mathcal{F})$ and $\mathcal{F}$ as follows.

Definition 4.2.2
Let $\succeq$ be a total well-founded ordering on $\mathcal{T}$. Let $>_{\mathsf{R}}$ be a (not necessarily total)

[5] An ordering $\succeq$ on a set $\mathcal{M}$ will be called well-founded if its strict part $\succ$ is well-founded, i.e., does not allow infinite descending chains of the form $m_1 \succ m_2 \succ \ldots$.

well-founded ordering on R. We define an ordering on $\mathsf{M}(\mathcal{F})$ by $m_{t_1} \succ m_{t_2}$ if $t_1 \succ t_2$ or ($t_1 = t_2$ and $m_{t_1}(t_1) >_{\mathsf{R}} m_{t_2}(t_2)$).
For two elements f, g in $\mathcal{F}$ we define $f \succ g$ iff $\mathsf{HM}(f) \succ \mathsf{HM}(g)$ or ($\mathsf{HM}(f) = \mathsf{HM}(g)$ and $\mathsf{RED}(f) \succ \mathsf{RED}(g)$). We further define $f \succ o$ for all $f \in \mathcal{F}\backslash\{o\}$. $\diamond$

Notice that the total well-founded ordering on $\mathsf{T}(\mathcal{F})$ extends to a well-founded ordering on $\mathsf{M}(\mathcal{F})$.

For a field $\mathbb{K}$ we have the trivial ordering $>_{\mathbb{K}}$ where $\alpha >_{\mathbb{K}} 0$ for all $\alpha \in \mathbb{K}\backslash\{0\}$ and no other elements are comparable. Then the resulting ordering on the respective function ring corresponds to the one given in Definition 2.3.3 for polynomial rings over fields.

Lemma 4.2.3
The ordering $\succ$ on $\mathcal{F}$ is well-founded.

Proof :
The proof of this lemma will use a method known as Cantor's second diagonal argument (compare e.g. [BW92] Chapter 4). Let us assume that $\succ$ is not well-founded on $\mathcal{F}$. We will show that this gives us a contradiction to the fact that the ordering $\succeq$ on $\mathsf{M}(\mathcal{F})$ inducing $\succ$ is well-founded. Hence, let us suppose $f_0 \succ f_1 \succ \ldots \succ f_k \succ \ldots$, $k \in \mathbb{N}$ is a strictly descending chain in $\mathcal{F}$. Then we can construct a sequence of sets of pairs $\{\{(m_{t_k}, g_{kn}) \mid n \in \mathbb{N}\} \mid k \in \mathbb{N}\}$ recursively as follows: For $k = 0$ let $m_{t_0} = \min_{\succeq}\{\mathsf{HM}(f_i) \mid i \in \mathbb{N}\}$ which is well-defined since $\succeq$ is well-founded on $\mathsf{M}(\mathcal{F})$. Now let $j \in \mathbb{N}$ be the least index such that we have $m_{t_0} = \mathsf{HM}(f_j)$. Then $m_{t_0} = \mathsf{HM}(f_{j+n})$ holds for all $n \in \mathbb{N}$ and we can set $g_{0n} = f_{j+n} - \mathsf{HM}(f_{j+n})$, i.e., $m_{t_0} \succ \mathsf{HM}(g_{0n})$ for all $n \in \mathbb{N}$. For $k+1$ we let $m_{t_{k+1}} = \min_{\succeq}\{\mathsf{HM}(g_{ki}) \mid i \in \mathbb{N}\}$ and again let $j \in \mathbb{N}$ be the least index such that $m_{t_{k+1}} = \mathsf{HM}(g_{kj})$ holds, i.e., $m_{t_{k+1}} = \mathsf{HM}(g_{k(j+n)})$ for all $n \in \mathbb{N}$. Again we set $g_{(k+1)n} = g_{k(j+n)} - \mathsf{HM}(g_{k(j+n)})$.
Then the following statements hold for every $k \in \mathbb{N}$:

1. For all monomials m occuring in the polynomials g_{kn}, $n \in \mathbb{N}$, we have $m_{t_k} \succ m$.
2. $g_{k0} \succ g_{k1} \succ \ldots$ is a strictly descending chain in $\mathcal{F}$.

Hence we get that $m_{t_0} \succ m_{t_1} \succ \ldots$ is a strictly descending chain in $\mathsf{M}(\mathcal{F})$ contradicting the fact that $\succeq$ is supposed to be well-founded on this set.

q.e.d.

Characterizations of ideal bases in terms of special standard representations they allow are mainly provided for polynomial rings over *fields* in the literature (compare [BW92] and Section 2.3). Hence we will first take a closer look at possible generalizations of these concepts to function rings over fields.

4.2.1 The Special Case of Function Rings over Fields

Let $\mathcal{F}_{\mathbb{K}}$ be a function ring over a field $\mathbb{K}$. Remember that for a set F of polynomials in $\mathcal{F}_{\mathbb{K}}$ every polynomial $g \in \mathsf{ideal}_r(F)$ has a representation of the form $g = \sum_{i=1}^{n} f_i \star h_i, f_i \in F, h_i \in \mathcal{F}_{\mathbb{K}}, n \in \mathbb{N}$. However, such an arbitrary representation can contain monomials larger than $\mathsf{HM}(g)$ which are cancelled in the sum. A first idea of standard representations in the literature now is to represent g as a sum of polynomial multiples $f_i \star h_i$ such that no cancellation of monomials larger than $\mathsf{HM}(g)$ takes place, i.e. $\mathsf{HM}(g) \succeq \mathsf{HM}(f_i \star h_i)$. Hence in a first step we look at the following analogon of a definition of standard representations (compare [BW92], page 218):

Definition 4.2.4
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and g a non-zero polynomial in $\mathsf{ideal}_r(F)$. A representation of the form

$$g = \sum_{i=1}^{n} f_i \star h_i, f_i \in F, h_i \in \mathcal{F}_{\mathbb{K}}, n \in \mathbb{N} \tag{4.1}$$

where additionally $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i \star h_i)$ holds for $1 \leq i \leq n$ is called a **(general) right standard representation** of g in terms of F. If every $g \in \mathsf{ideal}_r(F)\backslash\{o\}$ has such a representation in terms of F, then F is called a **(general) right standard basis** of $\mathsf{ideal}_r(F)$. ◇

What distinguishes an arbitrary representation from a (general) right standard representation is the fact that the former may contain polynomial multiples $f_i \star h_i$ with head terms $\mathsf{HT}(f_i \star h_i)$ larger than the head term of the represented polynomial g. Therefore, in order to change an arbitrary representation into one fulfilling our additional condition (4.1) we have to deal with special sums of polynomials.

Definition 4.2.5
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and t an element in $\mathcal{T}$. Then we define the **critical set** $\mathcal{C}_{gr}(t, F)$ to contain all tuples of the form $(t, f_1, \ldots, f_k, h_1, \ldots, h_k)$, $k \in \mathbb{N}$, $f_1, \ldots, f_k \in F$[6], $h_1, \ldots, h_k \in \mathcal{F}_{\mathbb{K}}$ such that

1. $\mathsf{HT}(f_i \star h_i) = t$, $1 \leq i \leq k$, and
2. $\sum_{i=1}^{k} \mathsf{HM}(f_i \star h_i) = o$.

We set $\mathcal{C}_{gr}(F) = \bigcup_{t \in \mathcal{T}} \mathcal{C}_{gr}(t, F)$. ◇

[6] As in the case of commutative polynomials, $f_1, \ldots, f_k$ are not necessarily different polynomials from F.

Notice that for the sums of polynomial multiples in this definition we get $\mathsf{HT}(\sum_{i=1}^{k} f_i \star h_i) \prec t$. This definition is motivated by the definition of syzygies of polynomials in commutative polynomial rings over rings. However, it differs from the original definition insofar as we need not have $\mathsf{HT}(f \star h) = \mathsf{HT}(\mathsf{HT}(f) \star \mathsf{HT}(h))$, i.e., we cannot localize the definition to the head monomials of the polynomials in F. Still we can characterize (general) right standard bases using this concept.

Theorem 4.2.6
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a (general) right standard basis of $\mathsf{ideal}_r(F)$ if and only if for every tuple $(t, f_1, \ldots, f_k, h_1, \ldots, h_k)$ in $\mathcal{C}_{gr}(F)$ the polynomial $\sum_{i=1}^{k} f_i \star h_i$ (i.e., the element in $\mathcal{F}_{\mathbb{K}}$ corresponding to this sum) has a (general) right standard representation with respect to F.

Proof :
In case F is a (general) right standard basis, since these polynomials are all elements of $\mathsf{ideal}_r(F)$, they must have (general) right standard representations with respect to F.
To prove the converse, it remains to show that every element in $\mathsf{ideal}_r(F)$ has a (general) right standard representation with respect to F. Hence, let $g = \sum_{j=1}^{m} f_j \star h_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}_r(F)$ such that $f_j \in F$, $h_j \in \mathcal{F}_{\mathbb{K}}$, $m \in \mathbb{N}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star h_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star h_j$ with head term t. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that this representation is already a (general) right standard one. Else we proceed by induction on t. Without loss of generality let $f_1, \ldots, f_K$ be the polynomials in the corresponding representation such that $t = \mathsf{HT}(f_i \star h_i)$, $1 \leq i \leq K$. Then the tuple $(t, f_1, \ldots, f_K, h_1, \ldots, h_K)$ is in $\mathcal{C}_{gr}(F)$ and let $h = \sum_{i=1}^{K} f_i \star h_i$. We will now change our representation of g in such a way that for the new representation of g we have a smaller maximal term. Let us assume h is not o[7]. By our assumption, h has a (general) right standard representation with respect to F, say $\sum_{j=1}^{n} p_j \star q_j$, where $p_j \in F$, $q_j \in \mathcal{F}_{\mathbb{K}}$, $n \in \mathbb{N}$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$ as $\sum_{i=1}^{K} \mathsf{HM}(f_i \star h_i) = o$. This gives us:

$$\begin{aligned} g &= \sum_{i=1}^{K} f_i \star h_i + \sum_{i=K+1}^{m} f_i \star h_i \\ &= \sum_{j=1}^{n} p_j \star q_j + \sum_{i=K+1}^{m} f_i \star h_i \end{aligned}$$

[7]In case $h = o$, just substitute the empty sum for the representation of h in the equations below.

which is a representation of g where the maximal term of the involved polynomial multiples is smaller than t.

q.e.d.

Remember that by the distributivity law in $\mathcal{F}_{\mathbb{K}}$ any representation of a polynomial g of the form $g = \sum_{i=1}^{n} f_i \star h_i, f_i \in F, h_i \in \mathcal{F}_{\mathbb{K}}, n \in \mathbb{N}$ can be converted into one of the form $g = \sum_{j=1}^{m} f_j \star m_j, f_j \in F, m_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), m \in \mathbb{N}$. Now for polynomial rings the conversion of a (general right) standard representation from a sum of polynomial multiples into a sum of monomial multiples again results in a standard representation. This is due to the fact that the orderings used for the polynomial rings are compatible with multiplication. Now let us look at a second analogon to this kind of standard representations in our setting.

Definition 4.2.7
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and g a non-zero polynomial in $\mathsf{ideal}_r(F)$. A representation of the form

$$g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N} \tag{4.2}$$

where additionally $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i \star m_i)$ holds for $1 \leq i \leq n$ is called a **right standard representation** of g in terms of F. If every $g \in \mathsf{ideal}_r(F) \backslash \{o\}$ has such a representation in terms of F, then F is called a **right standard basis** of $\mathsf{ideal}_r(F)$. $\diamond$

If our ordering $\succ$ on $\mathcal{F}_{\mathbb{K}}$ is compatible with $\star$ we can conclude that the conversion of a general right standard representation into a sum involving only monomial multiples again results in a right standard representation as defined in Definition 4.2.7. But since in general the ordering and the multiplication are not compatible (review Example 4.2.1) a polynomial multiple $f \star h$ can contain monomials $m, m' \in \mathsf{M}(f \star m_j)$ where $h = \sum_{j=1}^{n} m_j$ such that m and m' are larger than $\mathsf{HM}(f \star h)$ and $m = m'$. Hence just applying the distributivity to a sum of polynomial multiples no longer changes a standard representation as defined in Definition 4.2.4 into one as defined in Definition 4.2.7. Remember that this was true for polynomial rings over fields where both definitions are equivalent. Let us look at the monoid ring $\mathbb{Q}[\mathcal{M}]$ where $\mathcal{M}$ is the monoid presented by $(\{a, b, c\}; ab = a)$. Moreover, let $\succ$ be the length-lexicographical ordering induced by the precedence $c \succ b \succ a$. Then for the polynomials $f = ca + 1$, $h = b^2 - b \in \mathbb{Q}[\mathcal{M}]$ we get $\mathsf{HT}(f \star b^2) = \mathsf{HT}(ca + b^2) = ca$ and $\mathsf{HT}(f \star b) = \mathsf{HT}(ca + b) = ca$. On the other hand $\mathsf{HT}(f \star h) = \mathsf{HT}(ca + b^2 - ca - b) = \mathsf{HT}(b^2 - b) = b^2$. Hence for the polynomial $g = b^2 - b$ the polynomial multiple $f \star h$ is a general right standard representation as defined in Definition 4.2.4 while the sum of monomial multiples $f \star b^2 - f \star b$ is no right standard representation as defined in Definition 4.2.7. We can even state that g has no right standard representation in terms of the polynomial f.

Now as our aim is to link standard representations of polynomials to reduction relations, a closer inspection of the concept of general right standard representations shows that a reduction relation related to them has to involve polynomial multiples for defining the reduction steps. Right standard representations can also be linked to special instances of such reduction relations but are traditionally linked to reduction relations involving monomial multiples. There is no example known from the literature where reduction relations involving polynomial multiples gain real advantages over reduction relations involving monomial multiples only[8]. Therefore we will restrict our attention to right standard representations as presented in Definition 4.2.7.

Again, in order to change an arbitrary representation into one fulfilling our additional condition (4.2) of Definition 4.2.7 we have to deal with special sums of polynomials.

Definition 4.2.8
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and t an element in $\mathcal{T}$. Then we define the **critical set** $\mathcal{C}_r(t, F)$ to contain all tuples of the form $(t, f_1, \ldots, f_k, m_1, \ldots, m_k)$, $k \in \mathbb{N}$, $f_1, \ldots, f_k \in F$[9], $m_1, \ldots, m_k \in \mathsf{M}(\mathcal{F})$ such that

1. $\mathsf{HT}(f_i \star m_i) = t$, $1 \leq i \leq k$, and
2. $\sum_{i=1}^{k} \mathsf{HM}(f_i \star m_i) = o$.

We set $\mathcal{C}_r(F) = \bigcup_{t \in \mathcal{T}} \mathcal{C}_r(t, F)$. $\diamond$

As before, we can characterize right standard bases using this concept.

Theorem 4.2.9
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a right standard basis of $\mathsf{ideal}_r(F)$ if and only if for every tuple $(t, f_1, \ldots, f_k, m_1, \ldots, m_k)$ in $\mathcal{C}_r(F)$ the polynomial $\sum_{i=1}^{k} f_i \star m_i$ (i.e., the element in $\mathcal{F}$ corresponding to this sum) has a right standard representation with respect to F.

Proof :
In case F is a right standard basis, since these polynomials are all elements of $\mathsf{ideal}_r(F)$, they must have right standard representations with respect to F.
To prove the converse, it remains to show that every element in $\mathsf{ideal}_r(F)$ has a right standard representation with respect to F. Hence, let $g = \sum_{j=1}^{m} f_j \star m_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}_r(F)$ such that

[8]Examples where reduction relations involving polynomial multiples are studied for the original case of Gröbner bases in commutative polynomial rings can be found in [Tri78, Zac78].

[9]As in the case of commutative polynomials, $f_1, \ldots, f_k$ are not necessarily different polynomials from F.

$f_j \in F$, $m_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$, $m \in \mathbb{N}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star m_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star m_j$ with head term t. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that this representation is already a right standard one. Else we proceed by induction on t. Without loss of generality let $f_1, \ldots, f_K$ be the polynomials in the corresponding representation such that $t = \mathsf{HT}(f_i \star m_i)$, $1 \leq i \leq K$. Then the tuple $(t, f_1, \ldots, f_K, m_1, \ldots, m_K)$ is in $\mathcal{C}_r(F)$ and let $h = \sum_{i=1}^{K} f_i \star m_i$. We will now change our representation of g in such a way that for the new representation of g we have a smaller maximal term. Let us assume h is not o[10]. By our assumption, h has a right standard representation with respect to F, say $\sum_{j=1}^{n} h_j \star l_j$, where $h_j \in F$, $l_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$, $n \in \mathbb{N}$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$ as $\sum_{i=1}^{K} \mathsf{HM}(f_i \star m_i) = o$. This gives us:

$$\begin{aligned} g &= \sum_{i=1}^{K} f_i \star m_i + \sum_{i=K+1}^{m} f_i \star m_i \\ &= \sum_{j=1}^{n} h_j \star l_j + \sum_{i=K+1}^{m} f_i \star m_i \end{aligned}$$

which is a representation of g where the maximal term of the involved monomial multiples is smaller than t.

q.e.d.

For commutative polynomial rings over fields standard bases are in fact Gröbner bases. Remember that in algebraic terms a set F is a Gröbner basis of the ideal $\mathsf{ideal}(F)$ it generates if and only if $\mathsf{HT}(\mathsf{ideal}(F)) = \{t \star w \mid t \in \mathsf{HT}(F), w \text{ a term}\}$ (compare Definition 2.3.12). The localization to the set of head terms only is possible as the ordering and multiplication are compatible, i.e. $\mathsf{HT}(f \star w) = \mathsf{HT}(f) \star w$ for any $f \in F$ and any term w. Then of course if every $g \in \mathsf{ideal}(F)$ has a standard representation in terms of F we immediately get that $\mathsf{HT}(g) = \mathsf{HT}(f \star w) = \mathsf{HT}(f) \star w$ for some $f \in F$ and some term w. Moreover, for any reduction relation based on divisibility of terms we get that g is reducible at its head monomial by this polynomial f. This of course corresponds to the second definition of Gröbner bases in rewriting terms – a set F is a Gröbner basis of the ideal it generates if and only if the reduction relation $\longrightarrow^{\mathrm{b}}_{F}$ associated to the polynomials in F is confluent[11] (compare Definition 2.3.8). Central in both definitions of Gröbner bases is the idea of "dividing" terms. Important in this context is the fact that divisors are smaller than the terms they divide with respect to term orderings and moreover the ordering on the terms is stable

[10] In case $h = o$, just substitute the empty sum for the representation of h in the equations below.

[11] The additional properties of capturing the ideal congruence and being terminating required by Definition 3.1.4 trivially hold for polynomial rings over fields.

under multiplication with monomials. The algebraic definition states that every head term of a polynomial in $\mathsf{ideal}(G)$ has a head term of a polynomial in G as a divisor[12]. Similarly the reduction relation is based on divisibility of terms (compare Definition 2.3.7). The stability of the ordering under multiplication is important for the correctness of these characterizations of Gröbner bases since it allows finite localizations for the test sets to s-polynomials (Lemma 2.3.9 is central in this context).

In our context now the ordering $\succ$ and the multiplication $\star$ on $\mathcal{F}_{\mathbb{K}}$ in general are not compatible. Hence, a possible algebraic definition of Gröbner bases and a definition of a reduction relation related to right standard representations must involve the whole polynomials and not only their head terms.

Definition 4.2.10
A subset F of $\mathcal{F}_{\mathbb{K}}\backslash\{o\}$ is called a **weak right Gröbner basis** of $\mathsf{ideal}_r(F)$ if $\mathsf{HT}(\mathsf{ideal}_r(F)\backslash\{o\}) = \mathsf{HT}(\{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\}\backslash\{o\})$. $\diamond$

Instead of considering multiples of head terms of the generating set F we look at head terms of monomial multiples of polynomials in F.

In the setting of function rings over fields, in order to localize the definitions of standard representations and weak Gröbner bases to head terms instead of head monomials and show their equivalence we have to view $\mathcal{F}$ as a vector space with scalars from $\mathbb{K}$. We define a natural left **scalar multiplication** $\cdot : \mathbb{K} \times \mathcal{F} \longrightarrow \mathcal{F}$ by associating to $\alpha \in \mathbb{K}$ and $f \in \mathcal{F}$ the function in $\mathcal{F}$, denoted by $\alpha \cdot f$, which has support $\mathsf{supp}(\alpha \cdot f) \subseteq \mathsf{supp}(f)$ and values $(\alpha \cdot f)(t) = \alpha \cdot f(t)$ for $t \in \mathsf{supp}(f)$. Notice that if $\alpha \neq 0$ we have $\mathsf{supp}(\alpha \cdot f) = \mathsf{supp}(f)$. Similarly, we can define a natural right scalar multiplication $\cdot : \mathcal{F} \times \mathbb{K} \longrightarrow \mathcal{F}$ by associating to $\alpha \in \mathbb{K}$ and $f \in \mathcal{F}$ the function in $\mathcal{F}$, denoted by $f \cdot \alpha$, which has support $\mathsf{supp}(f \cdot \alpha) \subseteq \mathsf{supp}(f)$ and values $(f \cdot \alpha)(t) = f(t) \cdot \alpha$ for $t \in \mathsf{supp}(f)$. Since $\mathbb{K}$ is associative we have

$$\begin{aligned}
((\alpha \cdot f) \cdot \beta)(t) &= (\alpha \cdot f)(t) \cdot \beta \\
&= (\alpha \cdot f(t)) \cdot \beta \\
&= \alpha \cdot (f(t) \cdot \beta) \\
&= \alpha \cdot ((f \cdot \beta)(t)) \\
&= (\alpha \cdot (f \cdot \beta))(t)
\end{aligned}$$

and we will write $\alpha \cdot f \cdot \beta$. Monomials can be represented as $m = \alpha \cdot t$ where $\mathsf{supp}(m) = \{t\}$ and $m(t) = \alpha$.

[12] When generalizing this definition to our setting of function rings we have to be very careful as in reality this implies that every polynomial in the ideal is reducible to zero which is the definition of a weak Gröbner basis (compare Definition 3.1.2). Gröbner bases and weak Gröbner bases coincide in polynomial rings over fields due to the Translation Lemma (compare Lemma 2.3.9 (2)).

Additionally we have to state how scalar multiplication and ring multiplication are compatible. Remember that we have introduced the elements of our function rings as formal sums of monomials. We want to treat these objects similar to those occurring in the examples known from the literature. In particular we want to achieve that multiplication in $\mathcal{F}_{\mathbb{K}}$ can be specified by defining a multiplication on the terms and lifting it to the monomials. Hence we require the following equations $(\alpha \cdot f) \star g = \alpha \cdot (f \star g)$ and $f \star (g \cdot \alpha) = (f \star g) \cdot \alpha$ to hold[13]. These equations are valid in the examples from the literature studied here. The condition of course then implies that multiplication in $\mathcal{F}_{\mathbb{K}}$ can be specified by knowing $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}_{\mathbb{K}}$. This follows as for $\alpha, \beta \in \mathbb{K}$ and $t, s \in \mathcal{T}$ we have

$$\begin{aligned}
(\alpha \cdot t) \star (\beta \cdot s) &= \alpha \cdot (t \star (\beta \cdot s)) \\
&= \alpha \cdot (t \star (s \cdot \beta)) \\
&= \alpha \cdot (t \star s) \cdot \beta \\
&= (\alpha \cdot \beta) \cdot (t \star s).
\end{aligned}$$

If $\mathcal{F}$ contains a unit element $\mathbf{1}$ the field can be embedded into $\mathcal{F}$ by $\alpha \longmapsto \alpha \cdot \mathbf{1}$. Then for $\alpha \in \mathbb{K}$ and $f \in \mathcal{F}_{\mathbb{K}}$ the equations $\alpha \cdot f = (\alpha \cdot \mathbf{1}) \star f$ and $f \cdot \alpha = f \star (\alpha \cdot \mathbf{1})$ hold. Moreover, as $\mathbb{K}$ is Abelian $\alpha \cdot f \cdot \beta = \alpha \cdot \beta \cdot f$ for any $\alpha, \beta \in \mathbb{K}$, $f \in \mathcal{F}_{\mathbb{K}}$.

In the next lemma we show that in fact both characterizations of special bases, right standard bases and weak Gröbner bases, coincide as in the case of polynomial rings over fields.

Lemma 4.2.11
Let F be a subset of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a right standard basis if and only if it is a weak right Gröbner basis.

Proof :
Let us first assume that F is a right standard basis, i.e., every polynomial g in $\mathsf{ideal}_r(F)$ has a right standard representation with respect to F. In case $g \neq o$ this implies the existence of a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(g) = \mathsf{HT}(f \star m)$. Hence $\mathsf{HT}(g) \in \mathsf{HT}(\{f \star m \mid m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F\} \backslash \{o\})$. As the converse, namely $\mathsf{HT}(\{f \star m \mid m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F\} \backslash \{o\}) \subseteq \mathsf{HT}(\mathsf{ideal}_r(F) \backslash \{o\})$ trivially holds, F then is a weak right Gröbner basis.
Now suppose that F is a weak right Gröbner basis and again let $g \in \mathsf{ideal}_r(F)$. We have to show that g has a right standard representation with respect to F. This will be done by induction on $\mathsf{HT}(g)$. In case $g = o$ the empty sum is our required right standard representation. Hence let us assume $g \neq o$. Since then $\mathsf{HT}(g) \in \mathsf{HT}(\mathsf{ideal}_r(F) \backslash \{o\})$ by the definition of weak right Gröbner bases we know there exists a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such

[13] Then of course since $\mathbb{K}$ is Abelian we have $(\alpha \cdot f) \star g = \alpha \cdot (f \star g) = f \star (\alpha \cdot g) = f \star (g \cdot \alpha) = (f \star g) \cdot \alpha$.

that $\mathsf{HT}(g) = \mathsf{HT}(f \star m)$. Then there exists a monomial $\tilde{m} \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HM}(g) = \mathsf{HM}(f \star \tilde{m})$, namely[14] $\tilde{m} = (\mathsf{HC}(g) \cdot \mathsf{HC}(f \star m)^{-1}) \cdot m)$. Let $g_1 = g - f \star \tilde{m}$. Then $\mathsf{HT}(g) \succ \mathsf{HT}(g_1)$ implies the existence of a right standard representation for g_1 which can be added to the multiple $f \star \tilde{m}$ to give the desired right standard representation of g.

q.e.d.

Inspecting this proof closer we get the following corollary.

Corollary 4.2.12
Let a subset F of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$ be a weak right Gröbner basis. Then every $g \in \mathsf{ideal}_r(F)$ has a right standard representation in terms of F of the form $g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$ such that $\mathsf{HM}(g) = \mathsf{HM}(f_1 \star m_1)$ and $\mathsf{HT}(f_1 \star m_1) \succ \mathsf{HT}(f_2 \star m_2) \succ \ldots \succ \mathsf{HT}(f_n \star m_n)$.

Notice that we hence get stronger representations as specified in Definition 4.2.7 for the case that the set F is a weak right Gröbner basis or a right standard basis.

In the literature Gröbner bases are linked to reduction relations. These reduction relations in general then correspond to the respective standard representations as follows: if $g \xrightarrow{*}_F o$, then the monomial multiples involved in the respective reduction steps add up to a standard representation of g in terms of F. One possible reduction relation related to right standard representations as defined in Definition 4.2.7 is called **strong reduction**[15] where a monomial m_1 is reducible by some polynomial f, if there exists some monomial m_2 such that $m_1 = \mathsf{HM}(f \star m_2)$. Notice that such a reduction step eliminates the occurence of the term $\mathsf{HT}(m_1)$ in the resulting reductum $m_1 - f \star m_2$. When generalizing this reduction relation to function rings we can no longer localize the reduction step to checking whether $\mathsf{HM}(f)$ divides m_1, as now the whole polynomial is involved in the reduction step. We can no longer conclude that $\mathsf{HM}(f)$ divides m_1 but only that $m_1 = \mathsf{HM}(f \star m_2)$.

Our definition of weak right Gröbner bases using the condition $\mathsf{HT}(\mathsf{ideal}_r(F) \backslash \{o\}) = \mathsf{HT}(\{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\} \backslash \{o\})$ in Definition 4.2.10 corresponds to this problem that in many cases orderings on $\mathcal{T}$ are not compatible with the multiplication $\star$. Let us review Example 4.2.1 where the ordering $\succeq$ induced by $x \succ 1$ on terms respectively monomials is well-founded but in general not compatible with multiplication, due to the algebraic structure of $\mathcal{T}$. There for the polynomial $f = x+1$ and the term x we get $\mathsf{HM}(f \star x) = x$ while $\mathsf{HM}(f) \star x = 1$.

[14]Notice that this step requires that we can view $\mathcal{F}_{\mathbb{K}}$ as a vector space. In order to get a similar result without introducing vector spaces we would have to use a different definition of weak right Gröbner bases. E.g. requiring that $\mathsf{HM}(\mathsf{ideal}_r(F) \backslash \{o\}) = \mathsf{HM}(\{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\} \backslash \{o\})$ would be a possibility. However, then no localization of critical situations to head terms is possible, which is *the* advantage of having a field as coefficient domain.

[15]Strong reduction has been studied extensively for monoid rings in [Rei95].

Behind this phenomenon lies the fact that the definition of "divisors" arising from the algebraic characterization of weak Gröbner bases in the context of function rings does not have the same properties as divisors in polynomial rings. One such important property is that divisors are smaller with respect to the ordering on terms and that this ordering is transitive. Hence if t_1 is a divisor of t_2 and t_2 is a divisor of t_3 then t_1 is also a divisor of t_3. This is the basis of localizations when checking for the Gröbner basis property in polynomial rings over fields (compare Lemma 2.3.9). Unfortunately this is no longer true for function rings in general. Now $m_1 \in \mathsf{HM}(\mathsf{ideal}_r(G))$ implies the existence of $m_2 \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HM}(f \star m_2) = m_1$. Reviewing the previous example we see that for $f = x + 1$, $m_2 = x$ and $m_1 = \mathsf{HM}(f) = x$ we get $\mathsf{HM}(f \star m_2) = \mathsf{HM}((x + 1) \star x) = x$, i.e. $\mathsf{HM}(f \star m_2)$ divides m_1. On the other hand $m_1 = x$ divides 1 as $x \star x = 1$. But $\mathsf{HM}(\mathsf{HM}(f \star m_2) \star x) = 1$ while $\mathsf{HM}(f \star m_2 \star x) = x$, i.e. the head monomial of the multiple involving the polynomial $f \star m_2$ does not divide 1.

Notice that even if we restrict the concept of right divisors to monomials only we do not get transitivity. We are interested when for some monomials $m_1, m_2, m_3 \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ the facts that m_1 divides m_2 and m_2 divides m_3 imply that m_1 divides m_3. Let $m, m' \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HM}(m_1 \star m) = m_2$ and $\mathsf{HM}(m_2 \star m') = m_3$. Then $m_3 = \mathsf{HM}(m_2 \star m') = \mathsf{HM}(\mathsf{HM}(m_1 \star m) \star m')$. When does this equal $\mathsf{HM}(m_1 \star m \star m')$ or even $\mathsf{HM}(m_1 \star \mathsf{HM}(m \star m'))$? Obviously if we have $\star : \mathsf{M}(\mathcal{F}_{\mathbb{K}}) \times \mathsf{M}(\mathcal{F}_{\mathbb{K}}) \mapsto \mathsf{M}(\mathcal{F}_{\mathbb{K}})$, which is true for the Examples 4.1.3, 4.1.4 and 4.1.5, this is true. However if multiplication of monomials results in polynomials we are in trouble. Let us look at the skew-polynomial ring $\mathbb{Q}[X_1, X_2, X_3]$, $X_1 \succ X_2 \succ X_3$, defined in Example 4.1.6, i.e. $X_2 \star X_1 = X_2 + X_3$,$X_3 \star X_1 = X_1X_3$, $X_3 \star X_2 = X_2X_3$ and $X_i \star X_j = X_iX_j$ for $i < j$. Then from the fact that X_2 divides X_2 we get $\mathsf{HM}(X_2 \star X_1) = X_2$ and since again X_2 divides X_2, $\mathsf{HM}(\mathsf{HM}(X_2 \star X_1) \star X_1) = \mathsf{HM}(X_2 \star X_1) = X_2$. But $\mathsf{HM}(X_2 \star X_1 \star X_1) = \mathsf{HM}(X_1X_3 + X_2 + X_3) = X_1X_3$. Next we will show how using a restricted set of divisors only will enable some sort of transitivity.

To establish a certain kind of compatibility for the ordering $\succeq$ and the multiplication $\star$, additional requirements can be added. One way to do this is by giving an additional ordering on $\mathcal{T}$ which is in some sense weaker than $\succeq$ but adds more information on compatibility with right multiplication. Examples from the literature, where this technique is successfully applied, include special monoid and group rings (see e.g. [Rei95, MR98a, MR98d]). There restrictions of the respective orderings on the monoid or group elements are of syntactical nature involving the presentation of the monoid or group (e.g. prefix orderings of various kinds for commutative monoids and groups, free groups and polycyclic groups).

Definition 4.2.13
We will call an ordering $\geq$ on $\mathcal{T}$ a **right reductive restriction** of the ordering $\succeq$ or simply **right reductive**, if the following hold:

1. $t \geq s$ implies $t \succeq s$ for $t, s \in \mathcal{T}$.

2. $\geq$ is a partial ordering on $\mathcal{T}$ which is compatible with multiplication $\star$ from the right in the following sense: if for $t, t_1, t_2, w \in \mathcal{T}$, $t_2 \geq t_1$, $t_1 \succ t$ and $t_2 = \mathsf{HT}(t_1 \star w)$ hold, then $t_2 \succ t \star w$. $\diamond$

Notice that if $\succeq$ is a partial well-founded ordering on $\mathcal{T}$ so is $\geq$.

We can now distinguish special "divisors" of monomials: For $m_1, m_2 \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we call m_1 a **stable left divisor** of m_2 if and only if $\mathsf{HT}(m_2) \geq \mathsf{HT}(m_1)$ and there exists $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $m_2 = \mathsf{HM}(m_1 \star m)$. Then m is called a **stable right multiplier** of m_1.

If $\mathcal{T}$ contains a unit element[16] $\mathbf{1}$ and $\mathbf{1} \preceq t$ for all terms $t \in \mathcal{T}$ this immediately[17] implies $\mathbf{1} \leq t$ and hence $\mathbf{1}$ is a stable divisor of any monomial m. It remains to show that stable division is also transitive. For three monomials $m_1, m_2, m_3 \in \mathsf{M}(\mathcal{F})$ let m_1 be a stable divisor of m_2 and m_2 a stable divisor of m_3. Then there exist monomials $m, m' \in \mathsf{M}(\mathcal{F})$ such that $m_2 = \mathsf{HM}(m_1 \star m)$ with $\mathsf{HT}(m_2) \geq \mathsf{HT}(m_1)$ and $m_3 = \mathsf{HM}(m_2 \star m')$ with $\mathsf{HT}(m_3) \geq \mathsf{HT}(m_2)$. Let us have a look at the monomial $\mathsf{HM}(\mathsf{HM}(m_1 \star m) \star m')$. Remember how on page 78 we have seen that the case $m_1 \star m \in \mathsf{M}(\mathcal{F})$ is not critical as then we immediately have that this monomial equals $\mathsf{HM}(m_1 \star m \star m') = \mathsf{HM}(m_1 \star \mathsf{HM}(m \star m'))$. Hence let us assume that $m_1 \star m \notin \mathsf{M}(\mathcal{F})$. Then for all terms $s \in \mathsf{T}(m_1 \star m) \backslash \mathsf{HT}(m_1 \star m)$ we know $s \prec \mathsf{HT}(m_1 \star m) = \mathsf{HT}(m_2)$. Moreover $\mathsf{HT}(m_3) \geq \mathsf{HT}(m_2)$ and $\mathsf{HT}(m_3) = \mathsf{HT}(\mathsf{HT}(m_2) \star \mathsf{HT}(m'))$ then implies $\mathsf{HT}(m_3) \succ \mathsf{HT}(s \star \mathsf{HT}(m'))$ and hence $\mathsf{HM}(\mathsf{HM}(m_1 \star m) \star m') = \mathsf{HM}(m_1 \star m \star m')$. In both cases now $\mathsf{HT}(m_3) \geq \mathsf{HT}(m_1)$. However, we cannot conclude that $\mathsf{HM}(m_1 \star m \star m') = \mathsf{HM}(m_1 \star \mathsf{HM}(m \star m'))$. Still m_1 is a stable right divisor of m_3 as in case $m \star m'$ is a polynomial there exists some monomial $\tilde{m}$ in this polynomial such that $\mathsf{HM}(m_1 \star m \star m') = \mathsf{HM}(m_1 \star \tilde{m})$.

The intention of restricting the ordering is that now, if $\mathsf{HT}(m_2) \geq \mathsf{HT}(m_1)$ and $m_2 = m_1 \star m$, then for all terms t with $\mathsf{HT}(m_1) \succ t$ we then can conclude $\mathsf{HT}(m_2) \succ \mathsf{HT}(t \star m)$, which will be used to localize the multiple $\mathsf{HT}(m_1 \star m)$ to $\mathsf{HT}(m_1)$ achieving an equivalent to the properties of "divisors" in the case of commutative polynomial rings. Under certain conditions reduction relations based on this divisibility property for terms will have the stability properties we desire. On the other hand, restricting the choice of divisors in this way will lead to reduction relations which in general no longer capture the respective right ideal congruences[18].

Example 4.2.14
In Example 4.1.4 of a commutative polynomial ring we can state a reductive restriction of any term ordering by $t \geq s$ for two terms t and s if and only if

[16] I.e. $\mathbf{1} \star t = t \star \mathbf{1} = t$ for all $t \in \mathcal{T}$.

[17] As there are no terms smaller than $\mathbf{1}$ the second condition of Definition 4.2.13 trivially holds.

[18] Prefix reduction for monoid rings is an example where the right ideal congruence is lost. See e.g. [MR98d] for more on this topic.

s divides t as a term, i.e. for $t = X_1^{i_1} \dots X_n^{i_n}$, $s = X_1^{j_1} \dots X_n^{j_n}$ we have $j_l \leq i_l$, $1 \leq l \leq n$. The same is true for skew-polynomial rings as defined by Kredel in his PhD thesis [Kre93]. The situation changes if for the defining equations of skew-polynomial rings, $X_j \star X_i = c_{ij} \cdot X_i X_j + p_{ij}$ where $i < j$, $p_{ij} \prec X_i X_j$, we allow $c_{ij} = 0$. Then other restrictions of the ordinary term orderings have to be considered due to the possible vanishing of head terms. Let $X_2 \star X_1 = X_1, X_3 \star X_1 = X_1 X_3, X_3 \star X_2 = X_2 X_3$ and $\succ$ a term ordering with precedence $X_3 \succ X_2 \succ X_1$. Then, although $X_2 \succ X_1$, as $X_2 \star (X_1 X_2) = X_1 X_2$ and $X_1 \star (X_1 X_2) = X_1^2 X_2 \succ X_1 X_2$, we get $X_2 \star (X_1 X_2) \prec X_1 \star (X_1 X_2)$. Hence, since X_2 is a divisor of $X_1 X_2$ as a term, the classical restriction for polynomial rings no longer holds as X_2 is no stable divisor of $X_1 X_2$. For these cases the restriction to $u < v$ if and only if u is a prefix of v as a word will work. Then we know that for the respective term w with $u \star w = v$ multiplication is just concatenation of u and w as words and hence for all $t \prec u$ the result of $t \star w$ is again smaller than $u \star w$. ◇

Let us continue with algebraic consequences related to the right reductive restriction of our ordering by distinguishing special standard representations. Notice that for standard representations in commutative polynomial rings we already have that $\mathsf{HT}(g) = \mathsf{HT}(f_i \star m_i)$ implies $\mathsf{HT}(g) = \mathsf{HT}(f_i) \star \mathsf{HT}(m_i)$ and for all $t \prec \mathsf{HT}(f_i)$ we have $t \star w \prec \mathsf{HT}(f_i) \star w$ for any term w. In the setting of function rings an analogon to the latter property now can be achieved by restricting the monomial multiples in the representation to stable ones. Herefore we have different possibilities to incorporate these restrictions into the condition $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i \star m_i)$ of Definition 2.3.4 and Definition 4.2.7. The most general one is to require $\mathsf{HT}(g) = \mathsf{HT}(f_1 \star m_1) = \mathsf{HT}(\mathsf{HT}(f_1) \star m_1) \geq \mathsf{HT}(f_1)$ and $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i \star m_i)$ for all $2 \leq i \leq n$. Then a representation of g can contain further monomial multiples $f_j \star m_j$, $2 \leq j \leq n$ with $\mathsf{HT}(g) = \mathsf{HT}(f_j \star m_j)$ not fullfilling the restriction on the first multiple of f_1. Hence when defining critical situations we have to look at the same set as in Definition 4.2.8. Another generalization is to demand $\mathsf{HT}(g) = \mathsf{HT}(f_1 \star m_1) = \mathsf{HT}(\mathsf{HT}(f_1) \star m_1) \geq \mathsf{HT}(f_1)$ and $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \geq \mathsf{HT}(f_i)$ for all $2 \leq i \leq n$. Then critical situations can be localized to stable multiplers. But we can also give a weaker analogon as follows:

Definition 4.2.15
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and g a non-zero polynomial in $\mathsf{ideal}_r(F)$. A representation of the form

$$g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \geq \mathsf{HT}(f_i)$ for $1 \leq i \leq k$, for some $k \geq 1$, and $\mathsf{HT}(g) \succ \mathsf{HT}(f_i \star m_i)$ for $k < i \leq n$ is called a **right reductive standard representation** in terms of F. ◇

Notice that we restrict the possible multipliers to stable ones if the monomial multiple has the same head term as g, i.e. contributes to the head term of g. For definitions sake we will let the empty sum be the right reductive standard representation of o. The idea behind right reductive standard representations is that for an appropriate definition of a reduction relation based now on stable divisors such representations will again allow a reduction step to take place at the head monomial.

In case we have $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ we can rephrase the condition in Definition 4.2.15 to $\mathsf{HT}(g) = \mathsf{HT}(f_i \star m_i) = \mathsf{HT}(f_i) \star \mathsf{HT}(m_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$.

Definition 4.2.16
A set $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ is called a **right reductive standard basis** (with respect to the reductive ordering $\geq$) of $\mathsf{ideal}_r(F)$ if every polynomial $f \in \mathsf{ideal}_r(F)$ has a right reductive standard representation in terms of F. ⋄

Again, in order to change an arbitrary representation into one fulfilling our additional condition of Definition 4.2.15 we have to deal with special sums of polynomials.

Definition 4.2.17
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and t an element in $\mathcal{T}$. Then we define the **critical set** $\mathcal{C}_{rr}(t, F)$ to contain all tuples of the form $(t, f_1, \ldots, f_k, m_1, \ldots, m_k)$, $k \in \mathbb{N}$, $f_1, \ldots, f_k \in F$[19], $m_1, \ldots, m_k \in \mathsf{M}(\mathcal{F})$ such that

1. $\mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) = t$, $1 \leq i \leq k$,
2. $\mathsf{HT}(f_i \star m_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$, and
3. $\sum_{i=1}^{k} \mathsf{HM}(f_i \star m_i) = o$.

We set $\mathcal{C}_{rr}(F) = \bigcup_{t \in \mathcal{T}} \mathcal{C}_{rr}(t, F)$. ⋄

Unfortunately, in contrary to the characterization of right standard bases in Theorem 4.2.9 these critical situations will not be sufficient to characterize right reductive standard bases. To see this let us consider the following example:

Example 4.2.18
Let us recall the description of the free group ring in Example 4.1.7 with $\mathcal{T} = \{a^i, b^i, 1 \mid i \in \mathbb{N}^+\}$ and let $\succeq$ be the ordering induced by the length-lexicographical odering on $\mathcal{T}$ resulting from the precedence $a \succ b$.
Then the set consisting of the polynomial $a + 1$ does not give rise to non-trivial critical situations, but still is no right reductive standard basis as the polynomial $b+1 \in \mathsf{ideal}_r(\{a+1\})$ has no right reductive standard representation with respect to $a + 1$. ⋄

[19] As in the case of commutative polynomials, $f_1, \ldots, f_k$ are not necessarily different polynomials from F.

However, the failing situation $b+1=(a+1)\star b$ described in Example 4.2.18 describes the only kind of additional critical situations which have to be resolved in order to characterize right reductive standard bases.

Theorem 4.2.19
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{o\}$. Then F is a right reductive standard basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for every $f \in F$ and every $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ the multiple $f \star m$ has a right reductive standard representation in terms of F,*
2. *for every tuple $(t, f_1, \ldots, f_k, m_1, \ldots, m_k)$ in $\mathcal{C}_{rr}(F)$ the polynomial $\sum_{i=1}^{k} f_i \star m_i$ (i.e., the element in $\mathcal{F}$ corresponding to this sum) has a right reductive standard representation with respect to F.*

Proof :
In case F is a right reductive standard basis, since these polynomials are all elements of $\mathsf{ideal}_r(F)$, they must have right reductive standard representations with respect to F.
To prove the converse, it remains to show that every element in $\mathsf{ideal}_r(F)$ has a right reductive standard representation with respect to F. Hence, let $g = \sum_{j=1}^{m} f_j \star m_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}_r(F)$ such that $f_j \in F$, and $m_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. By our first statement every such monomial multiple $f_j \star m_j$ has a right reductive standard representation in terms of F and we can assume that all multiples are replaced by them. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star m_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star m_j$ with head term t. Then for each multiple $f_j \star m_j$ with $\mathsf{HT}(f_j \star m_j) = t$ we know that $\mathsf{HT}(f_j \star m_j) = \mathsf{HT}(\mathsf{HT}(f_j) \star m_j) \geq \mathsf{HT}(f_j)$ holds. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that this representation is already a right reductive standard one. Else we proceed by induction on t. Without loss of generality let $f_1, \ldots, f_K$ be the polynomials in the corresponding representation such that $t = \mathsf{HT}(f_i \star m_i)$, $1 \leq i \leq K$. Then the tuple $(t, f_1, \ldots, f_K, m_1, \ldots, m_K)$ is in $\mathcal{C}_{rr}(F)$ and let $h = \sum_{i=1}^{K} f_i \star m_i$. We will now change our representation of g in such a way that for the new representation of g we have a smaller maximal term. Let us assume h is not o[20]. By our assumption, h has a right reductive standard representation with respect to F, say $\sum_{j=1}^{n} h_j \star l_j$, where $h_j \in F$, and $l_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$ as

[20] In case $h = o$, just substitute the empty sum for the representation of h in the equations below.

$\sum_{i=1}^{K} \mathsf{HM}(f_i \star m_i) = o$. This gives us:

$$\begin{aligned} g &= \sum_{i=1}^{K} f_i \star m_i + \sum_{i=K+1}^{m} f_i \star m_i \\ &= \sum_{j=1}^{n} h_j \star l_j + \sum_{i=K+1}^{m} f_i \star m_i \end{aligned}$$

which is a representation of g where the maximal term is smaller than t.

q.e.d.

We can similarly refine Definition 4.2.10 with respect to a reductive restriction $\geq$ of the ordering $\succeq$.

Definition 4.2.20

A set $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ is called a **weak right reductive Gröbner basis** (with respect to the reductive ordering $\geq$) of $\mathsf{ideal}_r(F)$ if $\mathsf{HT}(\mathsf{ideal}_r(F) \backslash \{o\}) = \mathsf{HT}(\{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), \mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)\} \backslash \{o\})$. $\diamond$

This definition now localizes the characterization of the Gröbner basis to the head terms of the generating set of polynomials.

The next lemma states that in fact both characterizations of special bases, right reductive standard bases and weak right reductive Gröbner bases, coincide as in the case of polynomial rings over fields.

Lemma 4.2.21

Let F be a subset of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a right reductive standard basis if and only if it is a weak right reductive Gröbner basis.

Proof :

Let us first assume that F is a right reductive standard basis, i.e., every polynomial g in $\mathsf{ideal}_r(F)$ has a right reductive standard representation with respect to F. In case $g \neq o$ this implies the existence of a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(g) = \mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)$. Hence $\mathsf{HT}(g) \in \mathsf{HT}(\{f \star m \mid m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F, \mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)\} \backslash \{o\})$. As the converse, namely $\mathsf{HT}(\{f \star m \mid m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F, \mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)\} \backslash \{o\}) \subseteq \mathsf{HT}(\mathsf{ideal}_r(F) \backslash \{o\})$ trivially holds, F is then a weak right reductive Gröbner basis.

Now suppose that F is a weak right reductive Gröbner basis and again let $g \in \mathsf{ideal}_r(F)$. We have to show that g has a right reductive standard representation with respect to F. This will be done by induction on $\mathsf{HT}(g)$. In case $g = o$ the empty sum is our required right reductive standard representation. Hence let us assume $g \neq o$. Since then $\mathsf{HT}(g) \in \mathsf{HT}(\mathsf{ideal}_r(F) \backslash \{o\})$ by the definition of weak right reductive Gröbner bases we know there exists a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(g) = \mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)$. Then there exists a monomial $\tilde{m} \in \mathsf{M}(\mathcal{F})$ such that $\mathsf{HM}(g) = \mathsf{HM}(f \star \tilde{m})$, namely[21] $\tilde{m} = (\mathsf{HC}(g) \cdot \mathsf{HC}(f \star m)^{-1}) \cdot m)$. Let $g_1 = g - f \star \tilde{m}$. Then $\mathsf{HT}(g) \succ \mathsf{HT}(g_1)$ implies the existence of a right reductive standard representation for g_1 which can be added to the multiple $f \star \tilde{m}$ to give the desired right reductive standard representation of g.

q.e.d.

An inspection of the proof shows that in fact we can require a stronger condition for the head terms of the monomial multiples involved in right reductive standard representations in terms of right reductive Gröbner bases.

Corollary 4.2.22
Let a subset F of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$ be a weak right reductive Gröbner basis. Then every $g \in \mathsf{ideal}_r(F)$ has a right reductive standard representation in terms of F of the form $g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$ such that $\mathsf{HT}(g) = \mathsf{HT}(f_1 \star m_1) \succ \mathsf{HT}(f_2 \star m_2) \succ \ldots \succ \mathsf{HT}(f_n \star m_n)$, and $\mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \geq \mathsf{HT}(f_i)$ for all $1 \leq i \leq n$.

The importance of Gröbner bases in commutative polynomial rings stems from the fact that they can be characterized by special polynomials, the so-called s-polynomials, and that only finitely many such polynomials have to be checked in order to decide whether a set is a Gröbner basis. This test can be combined with adding ideal elements to the generating set leading to an algorithm which computes finite Gröbner bases by means of completion. These finite sets then can be used to solve many problems related to the ideals they generate.

Given a field as coefficient domain the critical situations for function rings now lead to s-polynomials as in the original case and can be identified by studying term multiples of polynomials. Let p and q be two non-zero polynomials in $\mathcal{F}_{\mathbb{K}}$. We are interested in terms t, u_1, u_2 such that $\mathsf{HT}(p \star u_1) = \mathsf{HT}(\mathsf{HT}(p) \star u_1) = t = \mathsf{HT}(q \star u_2) = \mathsf{HT}(\mathsf{HT}(q) \star u_2)$ and $\mathsf{HT}(p) \leq t$, $\mathsf{HT}(q) \leq t$. Let $\mathcal{C}_s(p,q)$ (this is a specialization of Definition 4.2.17) be the critical set containing all such tuples (t, u_1, u_2) (as a short hand for (t, p, q, u_1, u_2)). We call the polynomial $\mathsf{HC}(p \star u_1)^{-1} \cdot p \star u_1 - \mathsf{HC}(q \star u_2)^{-1} \cdot q \star u_2 = \mathsf{spol}_r(p, q, t, u_1, u_2)$ the **s-polynomial** of p and q related to the tuple (t, u_1, u_2).

Theorem 4.2.23
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a weak right reductive Gröbner basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for all f in F and for $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ the multiple $f \star m$ has a right reductive standard representation in terms of F, and*

[21] Notice that this step again requires that we can view $\mathcal{F}$ as a vector space.

2. *for all p and q in F and every tuple (t, u_1, u_2) in $\mathcal{C}_s(p, q)$ the respective s-polynomial $\mathsf{spol}_r(p, q, t, u_1, u_2)$ has a right reductive standard representation in terms of F.*

Proof :
In case F is a weak right reductive Gröbner basis it is also a right reductive standard basis, and since all multiples $f \star m$ and s-polynomials $\mathsf{spol}_r(p, q, t, u_1, u_2)$ stated above are elements of $\mathsf{ideal}_r(F)$, they must have right reductive standard representations in terms of F.
The converse will be proven by showing that every element in $\mathsf{ideal}_r(F)$ has a right reductive standard representation in terms of F. Now, let $g = \sum_{j=1}^{m} f_j \star m_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}_r(F)$ such that $f_j \in F$, $m_j \in \mathsf{M}(\mathcal{F})$, $m \in \mathbb{N}$. By our first assumption every multiple $f_j \star m_j$ in this sum has a right reductive representation. Hence without loss of generaltity we can assume that $\mathsf{HT}(\mathsf{HT}(f_j) \star m_j) = \mathsf{HT}(f_j \star m_j) \geq \mathsf{HT}(f_j)$ holds.
Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star m_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star m_j$ with head term t. Without loss of generality we can assume that the multiples with head term t are just $f_1 \star m_1, \ldots, f_K \star m_K$. We proceed by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[22].
Obviously, $t \succeq \mathsf{HT}(g)$ holds. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and by our assumptions our representation is already of the required form. Hence let us assume $K > 1$, then there are two not necessarily different polynomials f_1, f_2 and corresponding monomials $m_1 = \alpha_1 \cdot w_1$, $m_2 = \alpha_2 \cdot w_2$ with $\alpha_1, \alpha_2 \in \mathbb{K}$, $w_1, w_2 \in \mathcal{T}$ in the corresponding representation such that $t = \mathsf{HT}(\mathsf{HT}(f_1) \star w_1) = \mathsf{HT}(f_1 \star w_1) = \mathsf{HT}(f_2 \star w_2) = \mathsf{HT}(\mathsf{HT}(f_2) \star w_2)$ and $t \geq \mathsf{HT}(f_1)$, $t \geq \mathsf{HT}(f_2)$. Then the tuple (t, w_1, w_2) is in $\mathcal{C}_s(f_1, f_2)$ and we have an s-polynomial $h = \mathsf{HC}(f_1 \star w_1)^{-1} \cdot f_1 \star w_1 - \mathsf{HC}(f_2 \star w_2)^{-1} \cdot f_2 \star w_2$ corresponding to this tuple. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume the s-polynomial is not o[23]. By our assumption, h has a right reductive standard representation in terms of F, say $\sum_{i=1}^{n} h_i \star l_i$, where $h_i \in F$, and $l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$. This gives us:

$$f_1 \star m_1 + f_2 \star m_2$$

[22]Note that this ordering is well-founded since $\succ$ is well-founded on $\mathcal{T}$ and $K \in \mathbb{N}$.
[23]In case $h = o$, just substitute the empty sum for the right reductive representation of h in the equations below.

$$
\begin{aligned}
&= \alpha_1 \cdot f_1 \star w_1 + \alpha_2 \cdot f_2 \star w_2 \\
&= \alpha_1 \cdot f_1 \star w_1 + \underbrace{\alpha_2' \cdot \beta_1 \cdot f_1 \star w_1 - \alpha_2' \cdot \beta_1 \cdot f_1 \star w_1}_{=0} + \underbrace{\alpha_2' \cdot \beta_2}_{=\alpha_2} \cdot f_2 \star w_2 \\
&= (\alpha_1 + \alpha_2' \cdot \beta_1) \cdot f_1 \star w_1 - \alpha_2' \cdot \underbrace{(\beta_1 \cdot f_1 \star w_1 - \beta_2 \cdot f_2 \star w_2)}_{=h} \\
&= (\alpha_1 + \alpha_2' \cdot \beta_1) \cdot f_1 \star w_1 - \alpha_2' \cdot (\sum_{i=1}^{n} h_i \star l_i) \qquad (4.3)
\end{aligned}
$$

where $\beta_1 = \mathsf{HC}(f_1 \star w_1)^{-1}$, $\beta_2 = \mathsf{HC}(f_2 \star w_2)^{-1}$ and $\alpha_2' \cdot \beta_2 = \alpha_2$. By substituting (4.3) in our representation of g it becomes smaller.

q.e.d.

Notice that both test sets in this characterization in general are not finite.

Remember that in commutative polynomial rings over fields we can restrict these critical situations to one s-polynomial arising from the least common multiple of the head terms $\mathsf{HT}(p)$ and $\mathsf{HT}(q)$. Here we can introduce a similar concept of least common multiples, but now two terms can have no, one, finitely many and even infinitely many such multiples.

Given two non-zero polynomials p and q in $\mathcal{F}_{\mathbb{K}}$ let $S(p,q) = \{t \mid$ there exist $u_1, u_2 \in \mathcal{T}$ such that $\mathsf{HT}(p \star u_1) = \mathsf{HT}(\mathsf{HT}(p) \star u_1) = t = \mathsf{HT}(q \star u_2) = \mathsf{HT}(\mathsf{HT}(q) \star u_2)$ and $\mathsf{HT}(p) \leq t, \mathsf{HT}(q) \leq t\}$. A subset $LCM(p,q)$ of $S(p,q)$ is called a set of least common multiples for p and q if for any $t \in S(p,q)$ there exists $t' \in LCM(p,q)$ such that $t' \leq t$ and all other $s \in LCM(p,q)$ are not comparable with t' with respect to the reductive ordering $\leq$.

For polynomial rings over fields a term t is smaller than another term s with respect to the reductive ordering if t is a divisor of s and $LCM(p,q)$ consists of the least common multiple of the head terms $\mathsf{HT}(p)$ and $\mathsf{HT}(q)$. But for function rings in general other situations are possible. Two polynomials do not have to give rise to any s-polynomial. Just take $\mathcal{T}$ to be the free monoid on $\{a,b\}$ and $\mathbb{K} = \mathbb{Q}$. Then for the two polynomials $p = a+1$ and $q = b+1$ we have $S(p,q) = \emptyset$ as there are no terms u_1, u_2 in $\mathcal{T}$ such that $a \star u_1 = b \star u_2$.

Next we give an example where the set $LCM(p,q)$ is finite but larger that one element.

Example 4.2.24
Let our set of terms $\mathcal{T}$ be presented as a monoid by $(\{a,b,c,d_1,d_2,x_1,x_2\}; \{ax_i = cx_i, bx_i = cx_i, d_jx_i = x_id_j \mid i,j \in \{1,2\}\})$, $\succeq$ is the length-lexicographical ordering induced by the precedence $x_2 \succ x_1 \succ a \succ b \succ c \succ d_1 \succ d_2$ and the reductive

ordering $\geq$ is the prefix ordering. Then for the two polynomials $p = a + d_1$ and $q = b + d_2$ we get the respective sets $S(p,q) = \{cx_1w, cx_2w \mid w \in \mathcal{T}\}$ and $LCM(p,q) = \{cx_1, cx_2\}$ with resulting s-polynomials $\mathsf{spol}_r(p,q,cx_1,x_1,x_1) = x_1d_1 - x_1d_2$ and $\mathsf{spol}_r(p,q,cx_2,x_2,x_2) = x_2d_1 - x_2d_2$. ◇

It is also possible to have infinitely many least common multiples.

Example 4.2.25
Let our set of terms $\mathcal{T}$ be presented as a monoid by $(\{a,b,c,d_1,d_2,x_i \mid i \in \mathbb{N}\}; \{ax_i = cx_i, bx_i = cx_i, d_jx_i = x_id_j \mid i \in \mathbb{N}, j \in \{1,2\}\})$, $\succeq$ is the length-lexicographical ordering induced by the precedence $\ldots \succ x_n \succ \ldots \succ x_1 \succ a \succ b \succ c \succ d_1 \succ d_2$ and the reductive ordering $\geq$ is the prefix ordering. Then for the two polynomials $p = a + d_1$ and $q = b + d_2$ we get the respective set $S(p,q) = \{cx_iw \mid i \in \mathbb{N}, w \in \mathcal{T}\}$ and the infinite set $LCM(p,q) = \{cx_i \mid i \in \mathbb{N}\}$ with infinitely many resulting s-polynomials $\mathsf{spol}_r(p,q,cx_i,x_i,x_i) = x_id_1 - x_id_2$. ◇

However, we have to show that we can restrict the set $\mathcal{C}_s(p,q)$ to those tuples corresponding to terms in $LCM(p,q)$.

Remember that one problem which is related to the fact that the ordering $\succeq$ and the multiplication $\star$ in general are not compatible is that an important property fulfilled for representations of polynomials in commutative polynomial rings over fields no longer holds. This property in fact underlies Lemma 2.3.9 (4), which is essential in Buchberger's characterization of Gröbner bases in polynomial rings: $p \xrightarrow{*}^{\mathrm{b}}_F 0$ implies $p \star m \xrightarrow{*}^{\mathrm{b}}_F 0$ for any monomial m. Notice that $p \xrightarrow{*}^{\mathrm{b}}_F 0$ implies that p has a standard representation with respect to F, say $\sum_{i=1}^n f_i \star m_i$, and it is easy to see that then $\sum_{i=1}^n f_i \star m_i \star m$ is a standard representation of $p \star m$ with respect to F. This lemma is central in localizing *all* the critical situations related to two polynomials to the *one* s-polynomial resulting from the least common multiple of the respective head terms.

Unfortunately, neither the lemma nor its implication for the existence of the respective standard representations holds in our more general setting. There, if $g \in \mathsf{ideal}_r(F)$ has a right reductive standard representation $g = \sum_{i=1}^n f_i \star m_i$, then the sum $\sum_{i=1}^n f_i \star m_i \star m$ in general is *no* right reductive standard representation not even a right standard representation of the multiple $g \star m$ for $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. Even while $g \in \mathsf{ideal}_r(\{g\})$ has the trivial right reductive standard representation $g = g$, the multiple $g \star m$ is in general *no* right reductive standard representation of the function $g \star m$ for $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. Recall the example on page 77 where for $g = x+1$ we have $\mathsf{HM}(g \star x) = x$ while $\mathsf{HM}(g) \star x = 1$ as $x \star x = 1$. Similarly, while $g \longrightarrow_g 0$ must hold for any reduction relation, this no longer will imply $g \star m \xrightarrow{*}_g 0$. To see this let us review Example 4.2.18: For $g = a + 1$ and $m = b$ we get the multiple $g \star m = (a+1) \star b = 1 + b$, but $\mathsf{HT}(g \star m) = b \neq 1 = \mathsf{HT}(\mathsf{HT}(g) \star m)$. Moreover, $b+1$ is not reducible by $a+1$ for any reduction relation based on head monomial divisibility.

In order to give localizations of the test sets from Theorem 4.2.23 it is important to study under which conditions the stability of right reductive standard representations with respect to multiplication by monomials can be restored. The next lemma provides a sufficient condition.

Lemma 4.2.26
Let $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ and p a non-zero polynomial in $\mathcal{F}_{\mathbb{K}}$. Moreover, we assume that p has a right reductive standard representation in terms of F and m is a monomial such that $\mathsf{HT}(p \star m) = \mathsf{HT}(\mathsf{HT}(p) \star m) \geq \mathsf{HT}(p)$. Then $p \star m$ again has a right reductive standard representation in terms of F.

Proof :
Let $p = \sum_{i=1}^{n} f_i \star m_i$ with $n \in \mathbb{N}$, $f_i \in F$, $m_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ be a right reductive standard representation of p in terms of F, i.e., $\mathsf{HT}(p) = \mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$ and $\mathsf{HT}(p) \succ \mathsf{HT}(f_i \star m_i)$ for all $k+1 \leq i \leq n$.
Let us first analyze $f_j \star m_j \star m$ for $1 \leq j \leq k$:
Let $\mathsf{T}(f_j \star m_j) = \{s_1, \ldots, s_l\}$ with $s_1 \succ s_i$, $2 \leq i \leq l$, i.e. $s_1 = \mathsf{HT}(f_j \star m_j) = \mathsf{HT}(\mathsf{HT}(f_j) \star m_j) = \mathsf{HT}(p)$. Hence $\mathsf{HT}(\mathsf{HT}(p) \star m) = \mathsf{HT}(s_1 \star m) \geq \mathsf{HT}(p) = s_1$ and as $s_1 \succ s_i$, $2 \leq i \leq l$, by Definition 4.2.13 we can conclude $\mathsf{HT}(\mathsf{HT}(p) \star m) = \mathsf{HT}(s_1 \star m) \succ s_i \star m \succeq \mathsf{HT}(s_i \star m)$ for $2 \leq i \leq l$. This implies $\mathsf{HT}(\mathsf{HT}(f_j \star m_j) \star m) = \mathsf{HT}(f_j \star m_j \star m)$. Hence we get

$$\begin{aligned} \mathsf{HT}(p \star m) &= \mathsf{HT}(\mathsf{HT}(p) \star m) \\ &= \mathsf{HT}(\mathsf{HT}(f_j \star m_j) \star m), \text{ as } \mathsf{HT}(p) = \mathsf{HT}(f_j \star m_j) \\ &= \mathsf{HT}(f_j \star m_j \star m) \end{aligned}$$

and since $\mathsf{HT}(p \star m) \geq \mathsf{HT}(p) \geq \mathsf{HT}(f_j)$ we can conclude $\mathsf{HT}(f_j \star m_j \star m) \geq \mathsf{HT}(f_j)$.
It remains to show that $f_j \star m_j \star m$ has a right reductive standard representation in terms of F. First we show that $\mathsf{HT}(\mathsf{HT}(f_j) \star m_j \star m) \geq \mathsf{HT}(f_j)$: We know $\mathsf{HT}(f_j) \star m_j \succeq \mathsf{HT}(\mathsf{HT}(f_j) \star m_j) = \mathsf{HT}(f_j \star m_j)$ and hence $\mathsf{HT}(\mathsf{HT}(f_j) \star m_j \star m) = \mathsf{HT}(\mathsf{HT}(f_j \star m_j) \star m) = \mathsf{HT}(f_j \star m_j \star m) \geq \mathsf{HT}(f_j)$.
Now in case $m_j \star m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we are done as then $f_j \star (m_j \star m)$ is a right reductive standard representation in terms of F.
Hence let us assume $m_j \star m = \sum_{i=1}^{k} \tilde{m}_i$, $\tilde{m}_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. Let $\mathsf{T}(f_j) = \{t_1, \ldots, t_s\}$ with $t_1 \succ t_p$, $2 \leq p \leq s$, i.e. $t_1 = \mathsf{HT}(f_j)$. As $\mathsf{HT}(\mathsf{HT}(f_j) \star m_j) \geq \mathsf{HT}(f_j) \succ t_p$,$2 \leq p \leq s$, again by Definition 4.2.13 we can conclude $\mathsf{HT}(\mathsf{HT}(f_j) \star m_j) \succ t_p \star m_j \succeq \mathsf{HT}(t_p \star m_j)$, and $\mathsf{HT}(f_j) \star m_j \succ \sum_{p=2}^{s} t_p \star m_1$. Then for each s_i, $2 \leq i \leq l$ there exists $t_p \in \mathsf{T}(f_j)$ such that $s_i \in \mathsf{supp}(t_p \star m_j)$. Since $\mathsf{HT}(p) \succ s_i$ and even[24] $\mathsf{HT}(p) \succeq t_p \star m_j$ we find that either $\mathsf{HT}(p \star m) \succeq \mathsf{HT}((t_p \star m_j) \star m) = \mathsf{HT}(t_p \star (m_j \star m))$ in case $\mathsf{HT}(t_p \star m_j) = \mathsf{HT}(f_j \star m_j)$ or $\mathsf{HT}(p \star m) \succ \mathsf{HT}((t_p \star m_j) \star m) =$

[24] $\mathsf{HT}(p) \succ t_p \star m_j$ if $\mathsf{HT}(f_j \star m_j) \notin \mathsf{supp}(t_p \star m_j)$.

$\mathsf{HT}(t_p \star (m_j \star m))$. Hence we can conclude $f_j \star \tilde{m}_i \preceq \mathsf{HT}(p \star m)$, $1 \leq i \leq l$ and for at least one $\tilde{m}_i$ we get $\mathsf{HT}(f_j \star \tilde{m}_i) = \mathsf{HT}(f_j \star m_j \star m) \geq \mathsf{HT}(f_j)$.
It remains to analyze the situation for the function $(\sum_{i=k+1}^{n} f_i \star m_i) \star m$. Again we find that for all terms s in the $f_i \star m_i$, $k+1 \leq i \leq n$, we have $\mathsf{HT}(p) \succ s$ and we get $\mathsf{HT}(p \star m) \succ \mathsf{HT}(s \star m)$. Hence all polynomial multiples of the f_i in the representation $\sum_{i=k+1}^{n} \sum_{j=1}^{k_i} f_i \star \tilde{m}_j^i$, where $m_i \star m = \sum_{j=1}^{k_i} \tilde{m}_j^i$, are bounded by $\mathsf{HT}(p \star m)$.

q.e.d.

Notice that these observations are no longer true in case we only require $\mathsf{HT}(p \star m) = \mathsf{HT}(\mathsf{HT}(p) \star m) \succeq \mathsf{HT}(p)$, as then $\mathsf{HT}(p) \succ s$ no longer implies that $\mathsf{HT}(p \star m) \succ \mathsf{HT}(s \star m)$ will hold.

Of course this lemma now implies that if for two polynomials p and q in $\mathcal{F}_{\mathbb{K}}$ all s-polynomials related to the set $LCM(p, q)$ have right reductive standard representations so have all s-polynomials related to any tuple in $\mathcal{C}_s(p, q)$.

So far we have characterized weak right reductive Gröbner bases as special right ideal bases providing right reductive standard representations for the right ideal elements. In the literature the existence of such representations is normally established by means of reduction relations. The special representations presented here can be related to a reduction relation based on the divisibility of terms as defined in the context of right reductive restrictions of our ordering following Definition 4.2.13. Let $\geq$ be such a right reductive restriction of the ordering $\succeq$.

Definition 4.2.27
Let f, p be two non-zero polynomials in $\mathcal{F}_{\mathbb{K}}$. We say f **right reduces** p **to** q **at a monomial** $\alpha \cdot t$ **in one step**, denoted by $p \longrightarrow^{\mathrm{r}}_{f} q$, if there exists $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) = t \geq \mathsf{HT}(f)$,
3. $\mathsf{HM}(f \star m) = \alpha \cdot t$, and
4. $q = p - f \star m$.

We write $p \longrightarrow^{\mathrm{r}}_{f}$ if there is a polynomial q as defined above and p is then called right reducible by f. Further, we can define $\stackrel{*}{\longrightarrow}^{\mathrm{r}}$, $\stackrel{+}{\longrightarrow}^{\mathrm{r}}$ and $\stackrel{n}{\longrightarrow}^{\mathrm{r}}$ as usual. Right reduction by a set $F \subseteq \mathcal{F}_{\mathbb{K}}$ is denoted by $p \longrightarrow^{\mathrm{r}}_{F} q$ and abbreviates $p \longrightarrow^{\mathrm{r}}_{f} q$ for some $f \in F$. $\diamond$

Notice that if f right reduces p to q at $\alpha \cdot t$ then $t \notin \mathsf{supp}(q)$. If for some $w \in \mathcal{T}$ we have $\mathsf{HT}(f \star w) = \mathsf{HT}(\mathsf{HT}(f) \star w) = t \geq \mathsf{HT}(f)$ we can always reduce $\alpha \cdot t$ in p by f using the monomial $m = (\alpha \cdot \mathsf{HC}(f \star w)^{-1}) \cdot w$. Other definitions of reduction relations are possible, e.g. substituting item 2 by the condition $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m)$ (called right reduction in the context of monoid rings in [Rei95]; such a reduction relation would be connected to standard representations as defined in Definition 4.2.7) or by the condition $\mathsf{HT}(f \star m) = t$ (called strong reduction in the context of monoid rings in [Rei95] and for function rings on page 77). We have chosen this particular reduction relation as it provides the necessary information to apply Lemma 4.2.26 to give localizations for the test sets in Theorem 4.2.23 later on. Let us continue by studying some of the properties of our reduction relation.

Lemma 4.2.28
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$.

1. *For $p, q \in \mathcal{F}_{\mathbb{K}}$, $p \longrightarrow^{\mathrm{r}}_{f \in F} q$ implies $p \succ q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.*
2. *$\longrightarrow^{\mathrm{r}}_{F}$ is Noetherian.*

Proof :

1. Assuming that the reduction step takes place at a monomial $\alpha \cdot t$, by Definition 4.2.27 we know $\mathsf{HM}(f \star m) = \alpha \cdot t$ which yields $p \succ p - f \star m$ since $\mathsf{HM}(f \star m) \succ \mathsf{RED}(f \star m)$.
2. This follows directly from 1. as the ordering $\succeq$ on $\mathcal{T}$ is well-founded (compare Theorem 4.2.3).

q.e.d.

The next lemma shows how reduction sequences and right reductive standard representations are related.

Lemma 4.2.29
Let $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ and $p \in \mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then $p \xrightarrow{*}^{\mathrm{r}}_{F} o$ implies that p has a right reductive standard representation in terms of F.

Proof :
This follows directly by adding up the polynomials used in the reduction steps occurring in the reduction sequence $p \xrightarrow{*}^{\mathrm{r}}_{F} o$, say $p \longrightarrow^{\mathrm{r}}_{f_1} p_1 \longrightarrow^{\mathrm{r}}_{f_2} \ldots \longrightarrow^{\mathrm{r}}_{f_n} o$. If the reduction steps take place at the respective head monomials only, we can additionally state that $p = \sum_{i=1}^{n} f_i \star m_i$, $\mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq n$, and even $\mathsf{HT}(f_1 \star m_1) \succ \mathsf{HT}(f_2 \star m_2) \succ \ldots \mathsf{HT}(f_n \star m_n)$.

q.e.d.

If $p \xrightarrow{*}{}^{\mathrm{r}}_{F} q$, then p has a right reductive standard representation in terms of $F \cup \{q\}$, respectively $p-q$ has a right reductive standard representation in terms of F. On the other hand, if a polynomial g has a right reductive standard representation in terms of some set F it is reducible by a polynomial in F. To see this let $g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$ be a right reductive standard representation of g in terms of F. Then $\mathsf{HT}(g) = \mathsf{HT}(f_1 \star m_1) = \mathsf{HT}(\mathsf{HT}(f_1) \star m_1) \geq \mathsf{HT}(f_1)$ and by Definition 4.2.27 this implies that $g \longrightarrow^{\mathrm{r}}_{f_1} g - \alpha \cdot f_1 \star m_1 = g'$ where $\alpha \in \mathbb{K}$ such that $\alpha \cdot \mathsf{HC}(f_1 \star m_1) = \mathsf{HC}(g)$.

So far we have given an algebraic characterization of *weak* right reductive Gröbner bases in Definition 4.2.20 and a characterization of them as right reductive standard bases in Lemma 4.2.21. Another characterization known from the literature is that for a Gröbner basis in a polynomial ring every element of the ideal it generates reduces to zero using the Gröbner basis. Reviewing Definition 3.1.2 we find that this is in fact only the definition of a weak Gröbner basis. However in polynomial rings over fields and many other structures in the literature the definitions of weak Gröbner bases and Gröbner bases coincide as the Translation Lemma holds (see Lemma 2.3.9 (2)). This is also true for function rings over fields.

The first part of the following lemma is only needed for the proof of the second part which is an analogon of the Translation Lemma for function rings over fields.

Lemma 4.2.30
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and p, q, h polynomials in $\mathcal{F}_{\mathbb{K}}$.

1. *Let $p - q \longrightarrow^{\mathrm{r}}_{F} h$. Then there exist $p', q' \in \mathcal{F}_{\mathbb{K}}$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_{F} p'$ and $q \xrightarrow{*}{}^{\mathrm{r}}_{F} q'$ and $h = p' - q'$.*
2. *Let o be a normal form of $p-q$ with respect to F. Then there exists $g \in \mathcal{F}_{\mathbb{K}}$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_{F} g$ and $q \xrightarrow{*}{}^{\mathrm{r}}_{F} g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{r}}_{F} h$ at the monomial $\alpha \cdot t$, i.e., $h = p - q - f \star m$ for some $f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) = t \geq \mathsf{HT}(f)$ and $\mathsf{HM}(f \star m) = \alpha \cdot t$, i.e., α is the coefficient of t in $p - q$. We have to distinguish three cases:
   (a) $t \in \mathsf{supp}(p)$ and $t \in \mathsf{supp}(q)$: Then we can eliminate the occurrence of t in the respective polynomials by right reduction and get $p \longrightarrow^{\mathrm{r}}_{f} p - \alpha_1 \cdot f \star m = p'$, $q \longrightarrow^{\mathrm{r}}_{f} q - \alpha_2 \cdot f \star m = q'$, where $\alpha_1 \cdot \mathsf{HC}(f \star m)$ and $\alpha_2 \cdot \mathsf{HC}(f \star m)$ are the coefficients of t in p respectively q. Moreover,

$\alpha_1 \cdot \mathsf{HC}(f \star m) - \alpha_2 \cdot \mathsf{HC}(f \star m) = \alpha$ and hence $\alpha_1 - \alpha_2 = 1$, as $\mathsf{HC}(f \star m) = \alpha$. This gives us $p' - q' = p - \alpha_1 \cdot f \star m - q + \alpha_2 \cdot f \star m = p - q - (\alpha_1 - \alpha_2) \cdot f \star m = p - q - f \star m = h$.

(b) $t \in \mathsf{supp}(p)$ and $t \notin \mathsf{supp}(q)$: Then we can eliminate the term t in the polynomial p by right reduction and get $p \longrightarrow^{\mathrm{r}}_{f} p - f \star m = p'$, $q = q'$, and, therefore, $p' - q' = p - f \star m - q = h$.

(c) $t \in \mathsf{supp}(q)$ and $t \notin \mathsf{supp}(p)$: Then we can eliminate the term t in the polynomial q by right reduction and get $q \longrightarrow^{\mathrm{r}}_{f} q + f \star m = q'$, $p = p'$, and, therefore, $p' - q' = p - (q + f \star m) = h$.

2. We show our claim by induction on k, where $p - q \overset{k}{\longrightarrow}{}^{\mathrm{r}}_{F} o$. In the base case $k = 0$ there is nothing to show as then $p = q$. Hence, let $p - q \longrightarrow^{\mathrm{r}}_{F} h \overset{k}{\longrightarrow}{}^{\mathrm{r}}_{F} o$. Then by 1. there are polynomials $p', q' \in \mathcal{F}_{\mathbb{K}}$ such that $p \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} p'$ and $q \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \overset{k}{\longrightarrow}{}^{\mathrm{r}}_{F} o$ yields the existence of a polynomial $g \in \mathcal{F}_{\mathbb{K}}$ such that $p \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} g$ and $q \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} g$.

q.e.d.

The essential part of the proof is that right reducibility is connected to stable divisors of terms. We will later see that for function rings over arbitrary reduction rings, when the coefficient is also involved in the reduction step, this lemma no longer holds.

Definition 4.2.31
A subset G of $\mathcal{F}_{\mathbb{K}}$ is called a **right Gröbner basis** (with respect to the reduction relation $\longrightarrow^{\mathrm{r}}$) of the right ideal $\mathfrak{i} = \mathsf{ideal}_r(G)$ it generates, if $\overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_{G} = \equiv_{\mathfrak{i}}$ and $\longrightarrow^{\mathrm{r}}_{G}$ is confluent.

Recall the free group ring in Example 4.2.18. There the polynomial $b + 1$ lies in the right ideal generated by the polynomial $a+1$. Unlike in the case of polynomial rings over fields where for any set of polynomials F we have $\overset{*}{\longleftrightarrow}{}^{\mathrm{b}}_{F} = \equiv_{\mathsf{ideal}(F)}$, here we have $b + 1 \equiv_{\mathsf{ideal}_r(\{a+1\})} o$ but $b + 1 \overset{*}{\not\longleftrightarrow}{}^{\mathrm{r}}_{a+1} o$. Hence the first condition of Definition 4.2.31 now becomes necessary while it can be omitted in the definition of Gröbner bases for ordinary polynomial rings.

Now by Lemma 4.2.30 and Theorem 3.1.5 weak right reductive Gröbner bases are right Gröbner bases and can be characterized as follows:

Corollary 4.2.32
Let G be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. G is a right Gröbner basis if and only if for every $g \in \mathsf{ideal}_r(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{G} o$.

Finally we can characterize right Gröbner bases similar to Theorem 2.3.11.

Theorem 4.2.33
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{o\}$. Then F is a right Gröbner basis if and only if

1. *for all f in F and for all $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we have $f \star m \xrightarrow{*}{}^{\mathrm{r}}_{F} o$, and*
2. *for all p and q in F and every tuple (t, u_1, u_2) in $\mathcal{C}_s(p,q)$ and the respective s-polynomial $\mathsf{spol}_r(p,q,t,u_1,u_2)$ we have $\mathsf{spol}_r(p,q,t,u_1,u_2) \xrightarrow{*}{}^{\mathrm{r}}_{F} o$.*

However, the importance of Gröbner bases in the classical case stems from the fact that we only have to check a finite set of s-polynomials for F in order to decide, whether F is a Gröbner basis. Hence, we are interested in localizing the test sets in Theorem 4.2.33 – if possible to finite ones.

Definition 4.2.34
A set of polynomials $F \subseteq \mathcal{F}_{\mathbb{K}}\backslash\{o\}$ is called **weakly saturated**, if for every monomial $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and every polynomial f in F we have $f \star m \xrightarrow{*}{}^{\mathrm{r}}_{F} o$. $\diamond$

Then for a weakly saturated set F and any monomial $m \in \mathsf{M}(\mathcal{F}_{\mathcal{T}})$, $f \in F$, the multiple $f \star m$ has a right reductive standard representation in terms of F. Notice that since the coefficient domain is a field and $\mathcal{F}$ a vector space we can even restrict ourselves to multiples with elements of $\mathcal{T}$. However, for reduction rings as coefficient domains, we will need monomial multiples and hence we give the more general definition. For the free group ring in Example 4.2.18 the set $\{a+1, b+1\}$ is weakly saturated.

Definition 4.2.35
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{0\}$. A set $\mathsf{SAT}(F) \subseteq \{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\}$ is called a **stable saturator** for F if for any $f \in F$, $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ there exist $s \in \mathsf{SAT}(F)$, $m' \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $f \star m = s \star m'$ and $\mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(s) \star m') \geq \mathsf{HT}(s)$.

Notice that a stable saturator need not be weakly saturated. Let $s \in \mathsf{SAT}(F) \subseteq \{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\}$ and $m' \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. For $\mathsf{SAT}(F)$ to be weakly saturated then $s \star m' \xrightarrow{*}_{\mathsf{SAT}(F)} o$ must hold. We know that $s = f \star m$ for some $f \in F, m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. In case $m \star m' \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we are done. But this is no longer true if the monomial multiple results in a polynomial. Let our set of terms consist of words on the alphabet $\{a, b, c\}$ with multiplication $\star$ deduced form the equations $a \star b = a, b \star a = b^2 - b, a \star a = o$. As ordering on $\mathcal{T}$ we take the length lexicographical ordering with precedence $a \succ b \succ c$ and as reductive restriction the prefix ordering. For the polynomial $f = ca + 1$ we get a stable saturator $\mathsf{SAT}(\{f\}) = \{ca+1, ca+b, ca+b^2, b^3+ca, a\}$. Then the polynomial multiple $(f \star b) \star a = f \star (b \star a) = f \star (b^2 - b) = ca + b^2 - (ca + b) = b^2 - b$ is not reducible by $\mathsf{SAT}(\{f\})$ while $f \star b = ca + b \in \mathsf{SAT}(\{f\})$.

Corollary 4.2.36
Let $\mathsf{SAT}(F)$ *be a stable saturator of a set* $F \subseteq \mathcal{F}_{\mathbb{K}}$*. Then for any* $f \in F$, $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ *there exists* $s \in \mathsf{SAT}(F)$ *such that* $f \star m \longrightarrow^{\mathrm{r}}_{s} o$.

Lemma 4.2.37
Let F *be a set of polynomials in* $\mathcal{F}_{\mathbb{K}} \backslash \{0\}$*. If for all* s *in a stable saturator* $\mathsf{SAT}(F)$ *we have* $s \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} o$*, then for every* m *in* $\mathsf{M}(\mathcal{F}_{\mathbb{K}})$ *and every polynomial* f *in* F *the right multiple* $f \star m$ *has a right reductive standard representation in terms of* F.

Proof :
This follows immediately from Lemma 4.2.29 and Lemma 4.2.26.

q.e.d.

Definition 4.2.38
Let p and q be two non-zero polynomials in $\mathcal{F}_{\mathbb{K}}$. Then a subset $C \subseteq \{\mathsf{spol}_r(p, q, t, u_1, u_2) \mid (t, u_1, u_2) \in \mathcal{C}_s(p, q)\}$ is called a **stable localization** for the critical situations if for every s-polynomial $\mathsf{spol}_r(p, q, t, u_1, u_2)$ related to a tuple (t, u_1, u_2) in $\mathcal{C}_s(p, q)$ there exists a polynomial $h \in C$ and a monomial $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that

1. $\mathsf{HT}(h) \leq \mathsf{HT}(\mathsf{spol}_r(p, q, t, u_1, u_2))$,
2. $\mathsf{HT}(h \star m) = \mathsf{HT}(\mathsf{HT}(h) \star m) = \mathsf{HT}(\mathsf{spol}_r(p, q, t, u_1, u_2))$,
3. $\mathsf{spol}_r(p, q, t, u_1, u_2) = h \star m$. ◇

The set $LCM(p, q)$ (see page 4.2.1) allows a stable localization as follows: $C = \{\mathsf{spol}_r(p, q, t, u_1, u_2) \mid t \in LCM(p, q), (t, u_1, u_2) \in \mathcal{C}_s(p, q)\}$.

Corollary 4.2.39
Let $C \subseteq \{\mathsf{spol}_r(p, q, t, u_1, u_2) \mid (t, u_1, u_2) \in \mathcal{C}_s(p, q)\}$ *be a stable localization for two polynomials* $p, q \in \mathcal{F}_{\mathbb{K}}$*. Then for any s-polynomial* $\mathsf{spol}_r(p, q, t, u_1, u_2)$ *there exists* $h \in C$ *such that* $\mathsf{spol}_r(p, q, t, u_1, u_2) \longrightarrow^{\mathrm{r}}_{h} o$.

Lemma 4.2.40
Let F *be a set of polynomials in* $\mathcal{F}_{\mathbb{K}} \backslash \{0\}$*. If for all* h *in a stable localization* $C \subseteq \{\mathsf{spol}_r(p, q, t, u_1, u_2) \mid (t, u_1, u_2) \in \mathcal{C}_s(p, q)\}$*, we have* $h \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} o$*, then for every* (t, u_1, u_2) *in* $\mathcal{C}_s(p, q)$ *the s-polynomial* $\mathsf{spol}_r(p, q, t, u_1, u_2)$ *has a right reductive standard representation in terms of* F.

Proof :
This follows immediately from Lemma 4.2.29 and Lemma 4.2.26.

q.e.d.

So far we have seen that basically the theory for right Gröbner bases and the refined notion of right reductive standard bases (for right ideals of course) carries over similar from the case of polynomial rings over fields. Now Lemma 4.2.26 and Lemma 4.2.29 allow a localization of the test situations from Theorem 4.2.33.

Theorem 4.2.41
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{0\}$. Then F is a right Gröbner basis if and only if

1. *for all s in a stable saturator $\mathsf{SAT}(F)$ we have $s \xrightarrow{*}{}^{\mathrm{r}}_{F} o$, and*
2. *for all p and q in F, and every polynomial h in a stable localization $C \subseteq \{\mathsf{spol}_r(p,q,t,u_1,u_2) \mid (t,u_1,u_2) \in \mathcal{C}_s(p,q)\}$, we have $h \xrightarrow{*}{}^{\mathrm{r}}_{F} o$.*

Proof :
In case F is a right Gröbner basis by Lemma 4.2.32 all elements of $\mathsf{ideal}_r(F)$ must right reduce to zero by F. Since the polynomials in question all belong to the right ideal generated by F we are done.
The converse will be proven by showing that every element in $\mathsf{ideal}_r(F)$ has a right reductive representation in terms of F. Now, let $g = \sum_{j=1}^{m} f_j \star m_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}_r(F)$ such that $f_j \in F$, and $m_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$.
By our first assumption for every multiple $f_j \star m_j$ in this sum we have some $s \in \mathsf{SAT}(F)$, $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $f_j \star m_j = s \star m$ and $\mathsf{HT}(f_j \star m_j) = \mathsf{HT}(s \star m) = \mathsf{HT}(\mathsf{HT}(s) \star m) \geq \mathsf{HT}(s)$. Since we have $s \xrightarrow{*}{}^{\mathrm{r}}_{F} o$, by Lemma 4.2.26 we can conclude that each $f_j \star m_j$ has a right reductive standard representation in terms of F. Therefore, we can assume that $\mathsf{HT}(\mathsf{HT}(f_j) \star m_j) = \mathsf{HT}(f_j \star m_j) \geq \mathsf{HT}(f_j)$ holds.
Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star m_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star m_j$ with head term t.
Without loss of generality we can assume that the polynomial multiples with head term t are just $f_1 \star m_1, \ldots, f_K \star m_K$. We proceed by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[25]. Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and by our assumption our representation is already of the required form.
Hence let us assume $K > 1$, then for the two not necessarily different polynomials

[25]Note that this ordering is well-founded since $\succ$ is well-founded on $\mathcal{T}$ and $K \in \mathbb{N}$.

f_1, f_2 and corresponding monomials $m_1 = \alpha_1 \cdot w_1$, $m_2 = \alpha_2 \cdot w_2$, $\alpha_1, \alpha_2 \in \mathbb{K}$, $w_1, w_2 \in \mathcal{T}$, in the corresponding representation we have $t = \mathsf{HT}(\mathsf{HT}(f_1) \star w_1) = \mathsf{HT}(f_1 \star w_1) = \mathsf{HT}(f_2 \star w_2) = \mathsf{HT}(\mathsf{HT}(f_2) \star w_2)$ and $t \geq \mathsf{HT}(f_1)$, $t \geq \mathsf{HT}(f_2)$. Then the tuple (t, w_1, w_2) is in $\mathcal{C}_s(f_1, f_2)$ and we have a polynomial h in a stable localization $C \subseteq \{\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) \mid (t, w_1, w_2) \in \mathcal{C}_s(f_1, f_2)\}$ and $m \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) = \mathsf{HC}(f_1 \star w_1)^{-1} \cdot f_1 \star w_1 - \mathsf{HC}(f_2 \star w_2)^{-1} \cdot f_2 \star w_2 = h \star m$ and $\mathsf{HT}(\mathsf{spol}_r(f_1, f_2, t, w_1, w_2)) = \mathsf{HT}(h \star m) = \mathsf{HT}(\mathsf{HT}(h) \star m) \geq \mathsf{HT}(h)$.
We will now change our representation of g by using the additional information on this situation in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume the s-polynomial is not o[26]. By our assumption, $h \xrightarrow{*}{}^{\mathrm{r}}_{F} o$ and by Lemma 4.2.29 h then has a right reductive standard representation in terms of F. Then by Lemma 4.2.26 the multiple $h \star m$ again has a right reductive standard representation in terms of F, say $\sum_{i=1}^{n} h_i \star l_i$, where $h_i \in F$, and $l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and all terms occurring in this sum are bounded by $t \succ \mathsf{HT}(h \star m)$. This gives us:

$$\begin{aligned}
& \alpha_1 \cdot f_1 \star w_1 + \alpha_2 \cdot f_2 \star w_2 \\
= \ & \alpha_1 \cdot f_1 \star w_1 + \underbrace{\alpha_2' \cdot \beta_1 \cdot f_1 \star w_1 - \alpha_2' \cdot \beta_1 \cdot f_1 \star w_1}_{=0} + \underbrace{\alpha_2' \cdot \beta_2}_{=\alpha_2} \cdot f_2 \star w_2 \\
= \ & (\alpha_1 + \alpha_2' \cdot \beta_1) \cdot f_1 \star w_1 - \alpha_2' \cdot \underbrace{(\beta_1 \cdot f_1 \star w_1 - \beta_2 \cdot f_2 \star w_2)}_{=h \star m} \\
= \ & (\alpha_1 + \alpha_2' \cdot \beta_1) \cdot f_1 \star w_1 - \alpha_2' \cdot (\sum_{i=1}^{n} h_i \star l_i) \qquad (4.4)
\end{aligned}$$

where $\beta_1 = \mathsf{HC}(f_1 \star w_1)^{-1}$, $\beta_2 = \mathsf{HC}(f_2 \star w_2)^{-1}$ and $\alpha_2' \cdot \beta_2 = \alpha_2$. By substituting (4.4) our representation of g becomes smaller.

q.e.d.

Obviously we now have criteria for when a set is a right Gröbner basis. As in the case of completion procedures such as the Knuth-Bendix procedure or the Buchberger algorithm, elements from these test sets which do not reduce to zero can be added to the set being tested, to gradually describe a not necessarily finite right Gröbner basis. Of course in order to get a computable completion procedure certain assumptions on the test sets have to be made, e.g. they should themselves be recursively enumerable, and normal forms with respect to finite sets have to be computable. Then provided such enumeration procedures for stable saturators and critical situations, an enumeration procedure for a respective right Gröbner basis has to ensure that all necessary candidates are enumerated and tested for

[26]In case $h = o$, just substitute the empty sum for the right reductive representation of h in the equations below.

reducibility to o. If this is not the case they are added to the right Gröbner basis, have to be added to the enumeration of the stable saturator candidates and the new arising critical situations have to be added to the respective enumeration process.

We close this subsection by outlining how different structures known to allow finite Gröbner bases can be interpreted as function rings. Using the respective interpretations the terminology can be adapted at once to the respective structures and in general the resulting characterizations of Gröbner bases coincide with the results known from literature.

Polynomial Rings

A commutative polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the set of terms $\{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{N}\}$.
- $\succ$ can be any admissible term ordering on $\mathcal{T}$. For the reductive ordering $\geq$ we have $t \geq s$ if s divides t as as term[27].
- Multiplication $\star$ is specified by the action on terms, i.e. $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ where $x_1^{i_1} \ldots x_n^{i_n} \star x_1^{j_1} \ldots x_n^{j_n} = x_1^{i_1+j_1} \ldots x_n^{i_n+j_n}$.

We do not need the concept of weak saturation. A stable localization of $\mathcal{C}_s(p, q)$ is already provided by the tuple corresponding to the least common multiple of the terms $\mathsf{HT}(p)$ and $\mathsf{HT}(q)$.

Since this structure is Abelian, one-sided and two-sided ideals coincide. Buchberger's Algorithm provides an effective procedure to compute finite Gröbner bases.

Solvable Polynomial Rings

According to [KRW90, Kre93], a solvable polynomial ring $\mathbb{K}\{x_1, \ldots, x_n; p_{ij}; c_{ij}\}$ with $1 \leq j < i \leq n$, $p_{ij} \in \mathbb{K}[x_1, \ldots, x_n]$, $c_{ij} \in \mathbb{K}^*$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the set of terms $\{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{N}\}$.
- $\succ$ can be any admissible term ordering on $\mathcal{T}$ for which $x_j x_i \succ p_{ij}$, $j < i$, must hold. For the reductive ordering $\geq$ we have $t \geq s$ if s divides t as as term.

[27] Apel has studied another possible reductive ordering $\geq$ where we have $t \geq s$ if s is a prefix of t. This ordering gives rise to Janet bases.

- Multiplication $\star$ is specified by lifting the following action on the variables: $x_i \star x_j = x_i x_j$ if $i \leq j$ and $x_i \star x_j = c_{ij} \cdot x_j x_i + p_{ij}$ if $i > j$.

We do not need the concept of weak saturation except in case we also allow $c_{ij} = 0$. Then appropriate term multiples which "delete" head terms have to be taken into account. This critical set can be described in a finitary manner. For the reductive ordering $\geq$ then we can chose $t \geq s$ if s is a prefix of t (compare Example 4.2.14).

The set $\mathcal{C}_s(p, q)$ again contains as a stable localization the tuple corresponding to the least common multiple of the terms $\mathsf{HT}(p)$ and $\mathsf{HT}(q)$.

This structure is no longer Abelian, but finite Gröbner bases can be computed for one- and two-sided ideals (see [KRW90, Kre93]).

Non-commutative Polynomial Rings

A non-commutative polynomial ring $\mathbb{K}[\{x_1, \ldots, x_n\}^*]$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the set of words on $\{x_1, \ldots, x_n\}$.
- $\succ$ can be any admissible ordering on $\mathcal{T}$. For the reductive ordering $\geq$ we can chose $t \geq s$ if s is a subword of t.
- Multiplication $\star$ is specified by the action on words which is just concatenation.

We do not need the concept of weak saturation. A stable localization of $\mathcal{C}_s(p, q)$ is already provided by the tuples corresponding to word overlaps resulting from the equations $u_1\mathsf{HT}(p)v_1 = \mathsf{HT}(q)$, $u_2\mathsf{HT}(q)v_2 = \mathsf{HT}(p)$, $u_3\mathsf{HT}(p) = \mathsf{HT}(q)v_3$ respectively $u_4\mathsf{HT}(q) = \mathsf{HT}(p)v_4$ with the restriction that $|u_3| < |\mathsf{HT}(q)|$ and $|u_4| < |\mathsf{HT}(p)|$, $u_i, v_i \in \mathcal{T}$.

This structure is not Abelian. For the case of one-sided ideals finite Gröbner bases can be computed (see e.g. [Mor94]). The case of two-sided ideals only allows an enumerating procedure. This is not surprising as the word problem for monoids can be reduced to the problem of computing the respective Gröbner bases (see e.g. [Mor87, MR98d]).

Monoid and Group Rings

A monoid or group ring $\mathbb{K}[\mathcal{M}]$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the monoid or group $\mathcal{M}$. In the cases studied by us as well as in [Ros93, Lo96], it is assumed that the elements of the monoid or group have a certain form. This presentation is essential in the approach. We will assume that the given monoid or group is presented by a convergent semi-Thue system.
- $\succ$ will be the completion ordering induced from the presentation of $\mathcal{M}$ to $\mathcal{M}$ and hence to $\mathcal{T}$. The reductive ordering $\geq$ depends on the choice of the presentation.
- Multiplication $\star$ is specified by lifting the monoid or group operation.

The concept of weak saturation and the choice of stable localizations of $\mathcal{C}_s(p,q)$ again depend on the choice of the presentation. We will close this section by listing monoids and groups which allow finite Gröbner bases for the respective monoid or group ring and pointers to the literature where the appropriate solutions can be found.

Structure	Ideals	Quote
Finite monoid	one- and two-sided	[Rei96, MR97b]
Free monoid	one-sided	[Mor94, MR97b]
Finite group	one- and two-sided	[Rei95, MR97b]
Free group	one-sided	[MR93a, Ros93, Rei95, MR97b]
Plain group	one-sided	[MR93a, Rei95, MR97b]
Context-free group	one-sided	[Rei95, MR97b]
Nilpotent group	one- and two-sided	[Rei95, MR97a]
Polycyclic group	one- and two-sided	[Lo96, Rei96]

4.2.2 Function Rings over Reduction Rings

The situation becomes more complicated for a function ring $\mathcal{F}_{\mathsf{R}}$ where R is not a field. We will abbreviate $\mathcal{F}_{\mathsf{R}}$ by $\mathcal{F}$.

Notice that similar to the previous section it is possible to study generalizations of standard representations for function rings over reduction rings with respect to the orderings $\succeq$ and $\geq$ on $\mathcal{T}$. General right standard representations as defined in Definition 4.2.4, as well as the corresponding critical situations from Definition 4.2.5 and the characterization of general right standard bases as in Theorem 4.2.6 carry over to our function ring $\mathcal{F}$. The same is true for right standard representations as defined in Definition 4.2.7, the corresponding critical situations from

Definition 4.2.8 and the characterization of right standard bases as in Theorem 4.2.6. However, these standard representations can no longer be linked to weak right Gröbner bases as defined in Definition 4.2.10. This is of course obvious as for function rings over fields we have a characterization of such Gröbner bases by head terms which is no longer possible for function rings over reduction rings. This is already the case for polynomial rings over the integers. For example take the polynomial $3 \cdot X$ in $\mathbb{Q}[X]$. Then obviously for $F_1 = \{3 \cdot X\}$ and $F_2 = \{X\}$ we get that $\mathsf{HT}(\mathsf{ideal}_r(F_1)\backslash\{0\}) = \mathsf{HT}(\{3 \cdot X \star X^i \mid i \in \mathbb{N}\}) = \mathsf{HT}(\{X \star X^i \mid i \in \mathbb{N}\}) = \mathsf{HT}(\mathsf{ideal}_r(F_2)\backslash\{0\})$ while of course F_1 is no right Gröbner basis of $\mathsf{ideal}_r(F_2)$ and F_2 is no right Gröbner basis of $\mathsf{ideal}_r(F_1)$. One possible generalizing of Definition 4.2.10 is as follows: F is a weak right Gröbner basis of $\mathsf{ideal}_r(F)$ if $\mathsf{HM}(\mathsf{ideal}_r(F)\backslash\{0\}) = \mathsf{HM}(\{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F})\})$. But this does not solve the problem as there is no equivalent to Lemma 4.2.11 to link these right Gröbner bases to the respective standard bases. The reason for this is that the definitions of standard representations as provided by Definition 4.2.4 and 4.2.7 are no longer related to reduction relations corresponding to Gröbner bases. Of course it is possible to study other generalizations of these definitions, e.g. involving the ordering on the coefficients, but we take a different approach. Our studies of standard representations for function rings over fields revealed that in fact we can identify stronger conditions for such representations in terms of weak right Gröbner bases (review e.g. Corollary 4.2.12 and 4.2.22). These special represenations arise from reduction sequences. Hence we will proceed by studying such standard representations which can be directly related to reduction relations in our function ring.

Similar to function rings over fields we need to view $\mathcal{F}$ as a vector space now over R, a reduction ring as described in Section 3.1. In general R is not Abelian and hence we have to distinguish right and left scalar multiplication as defined on page 75. However, since R is associative as in the case of fields we can write $\alpha \cdot f \cdot \beta$.

Notice that for f, g in $\mathcal{F}$ and $\alpha, \beta \in \mathsf{R}$ we have

1. $\alpha \cdot (f \oplus g) = \alpha \cdot f \oplus \alpha \cdot g$
2. $\alpha \cdot (\beta \cdot f) = (\alpha \cdot \beta) \cdot f$
3. $(\alpha + \beta) \cdot f = \alpha \cdot f \oplus \beta \cdot f$,

i.e., $\mathcal{F}$ is a left R-module. Similarly we have

1. $(f \oplus g) \cdot \alpha = f \cdot \alpha \oplus g \cdot \alpha$
2. $(f \cdot \alpha) \cdot \beta = f \cdot (\alpha \cdot \beta)$
3. $f \cdot (\alpha + \beta) = f \cdot \alpha \oplus f \cdot \beta$,

i.e., $\mathcal{F}$ is a right R-module as well. Moreover, as $(\alpha \cdot f) \cdot \beta = \alpha \cdot (f \cdot \beta)$ for all $f \in \mathcal{F}$, $\alpha, \beta \in \mathsf{R}$, $\mathcal{F}$ is an R-R bimodule.

In order to state how scalar multiplication and ring multiplication are compatible, we again require $(\alpha \cdot f) \star g = \alpha \cdot (f \star g)$ and $f \star (g \cdot \alpha) = (f \star g) \cdot \alpha$ to hold. This is true for all examples we know from the literature.

If we additionally require that for $\alpha, \beta \in \mathsf{R}$ and $t, s \in \mathcal{T}$ we have $(\alpha \cdot t) \star (\beta \cdot s) = (\alpha \cdot \beta) \cdot (t \star s)$, then the multiplication in $\mathcal{F}$ can be specified by knowing $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{F}$.

If $\mathcal{F}$ contains a unit $\mathbf{1}$, R can be embedded into $\mathcal{F}$ via the mapping $\alpha \longmapsto \alpha \cdot \mathbf{1}$. Then for $\alpha \in \mathsf{R}$ and $f \in \mathcal{F}$ the equations $\alpha \cdot f = (\alpha \cdot \mathbf{1}) \star f$ and $f \cdot \alpha = f \star (\alpha \cdot \mathbf{1})$ hold. Since for $\alpha \in \mathsf{R}$ and $t \in \mathcal{T}$ we have $\alpha \cdot t = t \cdot \alpha$ this implies $(\alpha \cdot t) \star (\beta \cdot s) = (\alpha \cdot \beta) \cdot (t \star s)$[28].

Moreover, if R is Abelian, we get $\alpha \cdot (f \star g) = f \star (\alpha \cdot g)$ and $\mathcal{F}$ is an algebra.

Remember that we want to study standard representations directly related to reduction relations on $\mathcal{F}$. Since we have a function ring over a reduction ring such a reduction relation originates from the reduction relation on the reduction ring R. Here we want to distinguish two such reduction relations on $\mathcal{F}$.

One possible generalization in the spirit of these ideas for function rings over reduction rings is as follows:

Definition 4.2.42
Let F be a set of polynomials in $\mathcal{F}$ and g a non-zero polynomial in $\mathsf{ideal}_r(F)$. A representation of the form

$$g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(\mathsf{HT}(f_1) \star m_1) = \mathsf{HT}(f_1 \star m_1) \geq \mathsf{HT}(f_1)$ and $\mathsf{HT}(g) \succ \mathsf{HT}(f_i \star m_i)$ for all $2 \leq i \leq n$ is called a **right reductive standard representation** in terms of F. A set $F \subseteq \mathcal{F} \backslash \{o\}$ is called a **right reductive standard basis** of $\mathsf{ideal}_r(F)$ if every polynomial $f \in \mathsf{ideal}_r(F)$ has a right reductive standard representation in terms of F. $\diamond$

Notice that that this definition differs from Definition 4.2.15 insofar as we demand $\mathsf{HT}(g) \succ \mathsf{HT}(f_i \star m_i)$ for all $2 \leq i \leq n$. In fact we use those special standard representations which arise in the case of function rings for $g \in \mathsf{ideal}_r(F)$ when F already is a right reductive standard basis (compare Corollary 4.2.22). This definition is directly related to the reduction relation presented in Definition 4.2.27 for $\mathcal{F}_{\mathbb{K}}$ generalized to $\mathcal{F}$. A possible definition of reduction can be given in the following fashion where we require that the reduction step eliminates the respective monomial it is applied to.

[28] $(\alpha \cdot t) \star (\beta \cdot s) = (\alpha \cdot t) \star ((\beta \cdot \mathbf{1}) \star s) = ((\alpha \cdot t) \star (\beta \cdot \mathbf{1})) \star s = (\alpha \cdot (t \star (\beta \cdot \mathbf{1})) \star s = (\alpha \cdot (t \cdot \beta)) \star s = (\alpha \cdot (\beta \cdot t)) \star s = (\alpha \cdot \beta) \cdot (t \star s)$.

Definition 4.2.43
Let f, p be two non-zero polynomials in $\mathcal{F}$. We say f **right reduces** p **to** q **eliminating the monomial** $\alpha \cdot t$ **in one step**, denoted by $p \longrightarrow^{\mathrm{r,e}}_{f} q$, if there exists $m \in \mathsf{M}(\mathcal{F})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) = t \geq \mathsf{HT}(f)$,
3. $\mathsf{HM}(f \star m) = \alpha \cdot t$, such that $\alpha \Longrightarrow_{\mathsf{HC}(f \star m)} 0$, and
4. $q = p - f \star m$.

We write $p \longrightarrow^{\mathrm{r,e}}_{f}$ if there is a polynomial q as defined above and p is then called right reducible by f. Further, we can define $\xrightarrow{*}^{\mathrm{r,e}}$, $\xrightarrow{+}^{\mathrm{r,e}}$ and $\xrightarrow{n}^{\mathrm{r,e}}$ as usual. Right reduction by a set $F \subseteq \mathcal{F}$ is denoted by $p \longrightarrow^{\mathrm{r,e}}_{F} q$ and abbreviates $p \longrightarrow^{\mathrm{r,e}}_{f} q$ for some $f \in F$. ◇

This reduction relation is related to a special instance[29] of the reduction relation $\Longrightarrow$. Notice that by Axiom (A2) $\alpha \Longrightarrow_{\mathsf{HC}(f \star m)} 0$ implies $\alpha \in \mathsf{ideal}^{\mathsf{R}}_{r}(\mathsf{HC}(f \star m))$ and hence $\alpha = \mathsf{HC}(f \star m) \cdot \beta$ for some $\beta \in \mathsf{R}$.

Notice that in contrary to $\mathcal{F}_{\mathbb{K}}$ now for $g, f \in \mathcal{F}$ and $m \in \mathsf{M}(\mathcal{F})$ the situation $\mathsf{HT}(g) = \mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)$ alone no longer implies that $\mathsf{HM}(g)$ is right reducible by f. This is due to the fact that we can no longer modify the coefficients involved in the reduction step in the appropriate manner since reduction rings in general will not contain inverse elements.

Let us continue by studying our reduction relation.

Lemma 4.2.44
Let F be a set of polynomials in $\mathcal{F} \backslash \{o\}$.

1. *For $p, q \in \mathcal{F}$ $p \longrightarrow^{\mathrm{r,e}}_{F} q$ implies $p \succ q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.*
2. *$\longrightarrow^{\mathrm{r,e}}_{F}$ is Noetherian.*

Proof :

1. Assuming that the reduction step takes place at a monomial $\alpha \cdot t$, by Definition 4.2.43 we know $\mathsf{HM}(f \star m) = \alpha \cdot t$ which yields $p \succ p - f \star m$ since $\mathsf{HM}(f \star m) \succ \mathsf{RED}(f \star m)$.
2. This follows from 1.

[29] Compare Pan's reduction relation for the integers as defined in Example 3.1.1.

q.e.d.

The Translation Lemma no longer holds for this reduction relation. This is already so for polynomial rings over the integers.

Example 4.2.45
Let $\mathbb{Z}[X]$ be the polynomial ring in one indeterminant over $\mathbb{Z}$. Moreover, let $\Longrightarrow$ be the reduction relation on $\mathbb{Z}$ where for $\alpha, \beta \in \mathbb{Z}$, $\alpha \Longrightarrow_\beta$ if and only if there exists $\gamma \in \mathbb{Z}$ such that $\alpha = \beta \cdot \gamma$ (compare Example 3.1.1). Let $p = 2 \cdot x$, $q = -3 \cdot X$ and $f = 5 \cdot X$. Then $p - q = 5 \cdot X \longrightarrow^{\mathrm{r,e}}_f 0$ while $p \not\longrightarrow^{\mathrm{r,e}}_f$ and $q \not\longrightarrow^{\mathrm{r,e}}_f$. $\diamond$

The reduction relation $\longrightarrow^{\mathrm{r,e}}$ in polynomial rings over the integers is known as Pan's reduction in the literature. The generalization of Gröbner bases then are weak Gröbner bases as by completion one can achieve that all ideal elements reduce to zero. Next we present a proper algebraic characterization of weak right Gröbner bases related to right reductive standard representations and the reduction relation defined in Definition 4.2.43. Notice that it differs from Definition 4.2.20 for function rings over fields insofar as we now have to look at the head monomials of the right ideal instead of the head terms only.

Definition 4.2.46
A set $F \subseteq \mathcal{F}\backslash\{o\}$ is called a **weak right reductive Gröbner basis** of $\mathsf{ideal}_r(F)$ if $\mathsf{HM}(\mathsf{ideal}_r(F)\backslash\{o\}) = \mathsf{HM}(\{f \star m \mid f \in F, m \in \mathsf{M}(\mathcal{F}), \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)\}\backslash\{o\})$. $\diamond$

Similar to Lemma 4.2.21 right reductive standard bases and weak right reductive Gröbner bases coincide.

Lemma 4.2.47
Let F be a subset of $\mathcal{F}\backslash\{o\}$. Then F is a right reductive standard basis if and only if it is a weak right reductive Gröbner basis.

Proof :
Let us first assume that F is a right reductive standard basis, i.e., every polynomial g in $\mathsf{ideal}_r(F)$ has a right reductive standard representation with respect to F. In case $g \neq o$ this implies the existence of a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F})$ such that $\mathsf{HT}(g) = \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)$ and $\mathsf{HM}(g) = \mathsf{HM}(f \star m)$[30]. Hence $\mathsf{HM}(g) \in \mathsf{HM}(\{f \star m \mid m \in \mathsf{M}(\mathcal{F}), f \in F, \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)\}\backslash\{o\})$. As the converse, namely $\mathsf{HM}(\{f \star m \mid m \in \mathsf{M}(\mathcal{F}), f \in F, \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)\}\backslash\{o\}) \subseteq \mathsf{HM}(\mathsf{ideal}_r(F)\backslash\{o\})$ trivially holds, F is a weak right reductive Gröbner basis.
Now suppose that F is a weak right reductive Gröbner basis and again let

[30] Notice that if we had generalized the original Definition 4.2.15 this would not holds.

$g \in \mathsf{ideal}_r(F)$. We have to show that g has a right reductive standard representation with respect to F. This will be done by induction on $\mathsf{HT}(g)$. In case $g = o$ the empty sum is our required right reductive standard representation. Hence let us assume $g \neq o$. Since then $\mathsf{HM}(g) \in \mathsf{HM}(\mathsf{ideal}_r(F) \backslash \{o\})$ by the definition of weak right reductive Gröbner bases we know there exists a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F})$ such that $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)$ and $\mathsf{HM}(g) = \mathsf{HM}(f \star m)$. Let $g_1 = g - f \star m$. Then $\mathsf{HT}(g) \succ \mathsf{HT}(g_1)$ implies the existence of a right reductive standard representation for g_1 which can be added to the multiple $f \star m$ to give the desired right reductive standard representation of g.

q.e.d.

Corollary 4.2.48
Let F a subset of $\mathcal{F} \backslash \{o\}$ be a weak right reductive Gröbner basis. Then every $g \in \mathsf{ideal}_r(F)$ has a right reductive standard representation in terms of F of the form $g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$ such that $\mathsf{HT}(g) = \mathsf{HT}(\mathsf{HT}(f_1) \star m_1) = \mathsf{HT}(f_1 \star m_1) \geq \mathsf{HT}(f_1)$ and $\mathsf{HT}(f_1 \star m_1) \succ \mathsf{HT}(f_2 \star m_2) \succ \ldots \succ \mathsf{HT}(f_n \star m_n)$.

Proof :
This follows from inspecting the proof of Lemma 4.2.47.

q.e.d.

Another consequence of Lemma 4.2.47 is the characterization of weak right reductive Gröbner bases in rewriting terms.

Lemma 4.2.49
A subset F of $\mathcal{F} \backslash \{o\}$ is a weak right reductive Gröbner basis if for all $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}^{\mathrm{r}}_{F} o$.

Now to find some analogon to s-polynomials in $\mathcal{F}$ we again study what polynomial multiples occur when changing arbitrary representations of right ideal elements into right reductive standard representations.

Given a generating set $F \subseteq \mathcal{F}$ of a right ideal in $\mathcal{F}$ the key idea in order to characterize weak right Gröbner bases is to distinguish special elements of $\mathsf{ideal}_r(F)$ which have representations $\sum_{i=1}^{n} f_i \star m_i$, $f_i \in F$, $m_i \in \mathsf{M}(\mathcal{F})$ such that the head terms $\mathsf{HT}(f_i \star m_i)$ are all the same within the representation. Then on one hand the respective coefficients $\mathsf{HC}(f_i \star m_i)$ can add up to zero which means that the sum of the head coefficients is in an appropriate module in R — m-polynomials are related to these situations (see also Definition 4.2.8). If the result is not zero the sum of the coefficients $\mathsf{HC}(f_i \star m_i)$ can be described in terms of a (weak) right Gröbner basis in R — g-polynomials are related to these situations. Zero divisors in the reduction ring eliminating the head monomial of a polynomial occur as a special instance of m-polynomials where $F = \{f\}$ and $f \cdot \alpha$, $\alpha \in \mathsf{R}$ are considered.

The first problem is related to solving linear homogeneous equations in R and to the existence of possibly finite bases of the respective modules. In case we want effectiveness, we have to require that these bases are computable.

The g-polynomials can successfully be treated when possibly finite (weak) right Gröbner bases exist for finitely generated right ideals in R. Here, in case we want effectiveness, we have to require that the (weak) right Gröbner bases as well as representations for their elements in terms of the generating set are computable.

Using m- and g-polynomials, weak right Gröbner bases can again be characterized as in Section 3.5. The definition of m- and g-polynomials is inspired by Definition 3.5.5. One main difference however is that in function rings multiples of one polynomial by different terms can result in the same head terms for the multiples while the multiples themselves are different. These multiples have to be treated as different ones contributing to the same overlap although they arise from the same polynomial. Hence when looking at sets of polynomials we now have to assume that we have multisets which can contain polynomials more than once. Additionally, while in Definition 3.5.5 we can restrict our attention to overlaps equal to the maximal head term of the polynomials involved now we have to introduce the overlapping term as an additional variable.

Definition 4.2.50
Let $P = \{p_1, \ldots, p_k\}$ be a multiset of not necessarily different polynomials in $\mathcal{F}$ and t an element in $\mathcal{T}$ such that there are $w_1, \ldots, w_k \in \mathcal{T}$ with $\mathsf{HT}(p_i \star w_i) = \mathsf{HT}(\mathsf{HT}(p_i) \star w_i) = t \geq \mathsf{HT}(p_i)$, for all $1 \leq i \leq k$. Further let $\gamma_i = \mathsf{HC}(p_i \star w_i)$ for $1 \leq i \leq k$.
Let G be a (weak) right Gröbner basis of $\{\gamma_1, \ldots, \gamma_k\}$ in R with respect to $\Longrightarrow$. Additionally let

$$\alpha = \sum_{i=1}^{k} \gamma_i \cdot \beta_i^{\alpha}$$

for $\alpha \in G$, $\beta_i^{\alpha} \in \mathsf{R}$, $1 \leq i \leq k$. Then we define the **g-polynomials (Gröbner polynomials)** corresponding to $p_1, \ldots, p_k$ and t by setting

$$g_{\alpha} = \sum_{i=1}^{k} p_i \star w_i \cdot \beta_i^{\alpha}.$$

Notice that $\mathsf{HM}(g_{\alpha}) = \alpha \cdot t$.
For the right module $M = \{(\delta_1, \ldots, \delta_k) \mid \sum_{i=1}^{k} \gamma_i \cdot \delta_i = 0\}$, let the set $\{B_j \mid j \in I_M\}$ be a basis with $B_j = (\beta_{j,1}, \ldots, \beta_{j,k})$ for $\beta_{j,l} \in \mathsf{R}$ and $1 \leq l \leq k$. Then we define the **m-polynomials (module polynomials)** corresponding to P and t by setting

$$h_j = \sum_{i=1}^{k} p_i \star w_i \cdot \beta_{j,i} \text{ for each } j \in I_M.$$

Notice that $\mathsf{HT}(h_j) \prec t$ for each $j \in I_M$. $\diamond$

Given a set of polynomials F, the set of corresponding g- and m-polynomials contains those which are specified by Definition 4.2.50 for each term $t \in \mathcal{T}$ fulfilling the respective conditions. For a set consisting of one polynomial the corresponding m-polynomials reflect the multiplication of the polynomial with zero-divisors of the head monomial, i.e., by a basis of the annihilator of the head monomial. Notice that given a finite set of polynomials the corresponding sets of g- and m-polynomials in general can be infinite.

As in Theorem 4.2.23 we can use g- and m-polynomials instead of s-polynomials to characterize special bases in function rings. As before we also have to take into account right multiples of the generating set as Example 4.2.18 does not require a field as coefficient domain.

Theorem 4.2.51
Let F be a set of polynomials in $\mathcal{F}\backslash\{o\}$. Then F is a weak right Gröbner basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for all f in F and for all m in $\mathsf{M}(\mathcal{F})$, $f \star m$ has a right reductive standard representation in terms of F, and*
2. *all g- and m-polynomials corresponding to F as specified in Definition 4.2.50 have right reductive standard representations in terms of F.*

Proof :
In case F is a weak right Gröbner basis it is also a right reductive standard basis, and since the multiples $f \star m$ and the respective g- and m-polynomials are all elements of $\mathsf{ideal}_r(F)$ they must have right reductive standard representations.
The converse will be proven by showing that every element in $\mathsf{ideal}_r(F)$ has a right reductive standard representation in terms of F. Let $g \in \mathsf{ideal}_r(F)$ have a representation in terms of F of the following form: $g = \sum_{j=1}^{m} f_j \star (w_j \cdot \alpha_j)$ such that $f_j \in F$, $w_j \in \mathcal{T}$ and $\alpha_j \in \mathsf{R}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star (w_j \cdot \alpha_j)) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star (w_j \cdot \alpha_j)$ with head term t. We show our claim by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or $(t' = t$ and $K' < K)$.
Since by our first assumption every multiple $f_j \star (w_j \cdot \alpha_j)$ in this sum has a right reductive standard representation in terms of F, we can assume that $\mathsf{HT}(\mathsf{HT}(f_j) \star w_j) = \mathsf{HT}(f_j \star w_j) \geq \mathsf{HT}(f_j)$ holds. Moreover, without loss of generality we can assume that the polynomial multiples with head term t are just $f_1 \star w_1, \ldots, f_K \star w_K$. Notice that these assumptions on the representation of g neither change t nor K.

Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and by our assumptions our representation is already a right reductive one and we are done. Hence let us assume $K > 1$.

First let $\sum_{j=1}^{K} \mathsf{HM}(f_j \star (w_j \cdot \alpha_j)) = o$. Then by Definition 4.2.50 there exists a tuple $(\alpha_1, \ldots, \alpha_K) \in M$, as $\sum_{j=1}^{K} \mathsf{HC}(f_j \star w_j) \cdot \alpha_j = 0$. Hence there are $\delta_1, \ldots, \delta_K \in \mathsf{R}$ such that $\sum_{i=1}^{l} A_i \cdot \delta_i = (\alpha_1, \ldots, \alpha_K)$ for some $l \in \mathbb{N}$, $A_i = (\alpha_{i,1}, \ldots, \alpha_{i,K}) \in \{A_j \mid j \in I_M\}$, and $\alpha_j = \sum_{i=1}^{l} \alpha_{i,j} \cdot \delta_i$, $1 \leq j \leq K$. By our assumption there are module polynomials $h_i = \sum_{j=1}^{K} f_j \star w_j \cdot \alpha_{i,j}$,$1 \leq i \leq l$, all having right reductive standard representations in terms of F.

Then since

$$
\begin{aligned}
\sum_{j=1}^{K} f_j \star (w_j \cdot \alpha_j) &= \sum_{j=1}^{K} f_j \star w_j \cdot (\sum_{i=1}^{l} \alpha_{i,j} \cdot \delta_i) \\
&= \sum_{j=1}^{K} \sum_{i=1}^{l} (f_j \star w_j \cdot \alpha_{i,j}) \cdot \delta_i \\
&= \sum_{i=1}^{l} (\sum_{j=1}^{K} f_j \star w_j \cdot \alpha_{i,j}) \cdot \delta_i \\
&= \sum_{i=1}^{l} h_i \cdot \delta_i
\end{aligned}
$$

we can change the representation of g to $\sum_{i=1}^{l} h_i \cdot \delta_i + \sum_{j=K+1}^{m} f_j \star (w_j \cdot \alpha_j)$ and replace each h_i by its right reductive standard representation in terms of F. Remember that for all h_i, $1 \leq i \leq l$ we have $\mathsf{HT}(h_i) \prec t$. Hence, for this new representation we now have maximal term smaller than t and by our induction hypothesis we have a right reductive standard representation for g in terms of F and are done.

It remains to study the case where $\sum_{j=1}^{K} \mathsf{HM}(f_j \star (w_j \cdot \alpha_j)) \neq 0$. Then we have $\mathsf{HT}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) = t = \mathsf{HT}(g)$, $\mathsf{HC}(g) = \mathsf{HC}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) \in \mathsf{ideal}_r(\{\mathsf{HC}(f_1 \star w_1), \ldots, \mathsf{HC}(f_K \star w_K)\})$ and $\mathsf{HM}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) = \mathsf{HM}(g)$. Hence $\mathsf{HC}(g) = \alpha \cdot \delta$ with $\delta \in \mathsf{R}$ and $\alpha \in G$[31], G being a (weak) right Gröbner basis of $\mathsf{ideal}_r(\{\mathsf{HC}(f_1 \star w_1), \ldots, \mathsf{HC}(f_K \star w_K)\})$ (compare Definition 4.2.50). Let g_α be the respective g-polynomial corresponding to α. Then the polynomial $g' = g - g_\alpha \cdot \delta$ lies in $\mathsf{ideal}_r(F)$. Since the multiple[32] $g_\alpha \cdot \delta$ has a right reductive standard representation in terms of F, say $\sum_{j=1}^{l} f_j \star m_j$, for the situation $\sum_{j=1}^{K} f_j \star (w_j \cdot \alpha_j) - f_1 \star m_1$ all polynomial multiples involved in this sum have head term t and their head monomials add up to o. Therefore, this

[31] Remember that we assume the reduction relation $\Longrightarrow$ on R based on division, see the remark after Definition 4.2.43.

[32] Note that right reductive standard representations are stable under multiplication with coefficients which are no zero-divisors of the head coefficient.

situation again corresponds to an m-polynomial of F. Hence we can apply our results from above and get that the polynomial g' has a smaller representation than g, especially the maximal term t' is smaller. Moreover, we can assume that g' has a right reductive standard representation in terms of F, say $g' = \sum_{i=1}^{n} f_i \star \tilde{m}_i$. Then $g = \sum_{i=1}^{n} f_i \star \tilde{m}_i + g_\alpha \cdot \delta = \sum_{i=1}^{n} f_i \star \tilde{m}_i + \sum_{j=1}^{l} f_j \star m_j$ is a right reductive standard representation of g in terms of F and we are done.

q.e.d.

Since in general we will have infinitely many g- and m-polynomials related to F, it is important to look for possible localizations of these situations. We are looking for concepts similar to those of weak saturation and stable localizations in the previous section. Remember that Lemma 4.2.26 is central there. It describes when the existence of a right reductive standard representation for some polynomial implies the existence of a right reductive standard representation for a multiple of the polynomial. Unfortunately we cannot establish an analogon to this lemma for right reductive standard representations in $\mathcal{F}$ as defined in Definition 4.2.42.

Example 4.2.52
Let $\mathcal{F}$ be a function ring over the integers with $\mathcal{T} = \{X_1, \ldots, X_7\}$ and multiplication $\star : \mathcal{T} \times \mathcal{T} \mapsto \mathcal{F}$ defined by the following equations: $X_1 \star X_2 = X_4$, $X_4 \star X_3 = X_5$, $X_2 \star X_3 = X_6 + X_7$, $X_1 \star X_6 = 3 \cdot X_5$, $X_1 \star X_7 = -2 \cdot X_5$ and else $X_i \star X_j = o$. Additionally let $X_5 > X_4 > X_1 \succ X_2 \succ X_3 \succ X_6 \succ X_7$.
Then for $p = X_4$, $f = X_1$ and $m = X_3$ we find that

1. p has a right reductive standard representation in terms of $\{f\}$, namely $p = f \star X_2$.
2. $\mathsf{HT}(p \star m) = \mathsf{HT}(\mathsf{HT}(p) \star m) \geq \mathsf{HT}(p)$ as $X_5 = X_4 \star X_3 > X_4$ and for all $X_i \prec X_4$ we have $X_i \star X_3 \prec X_5$.
3. $p \star m = X_5$ has no right reductive standard representation in terms of $\{f\}$ as only $X_1 \star X_j \neq o$ for $j = \{2, 6, 7\}$, namely $X_1 \star X_2 = X_4$, $X_1 \star X_6 = 3 \cdot X_5$, $X_1 \star X_7 = -2 \cdot X_5$, and $X_1 \star (X_j \cdot \alpha) \neq X_5$ for all $j \in \{2, 6, 7\}$, $\alpha \in \mathbb{Z}$.

Notice that these problems are due to the fact that while $(X_1 \star X_2) \star X_3 = X_1 \star (X_2 \star X_3) = X_5$, $X_1 \star (X_2 \star X_3) = X_1 \star (X_6 + X_7) = X_1 \star X_6 + X_1 \star X_7$ does not give us a right reductive standard representation in terms of X_1 as $\mathsf{HT}(X_1 \star X_6) = X_5$ *and* $\mathsf{HT}(X_1 \star X_7) = X_5$ (compare Definition 4.2.42). This was the crucial point in the proof of Lemma 4.2.26 and it is only fulfilled for the weaker form of right reductive standard representations in $\mathcal{F}_{\mathbb{K}}$ as defined in Definition 4.2.15. ◇

As this example shows an analogon to Lemma 4.2.26 does not hold in our general case. Note that the trouble arises from the fact that we allow multiplication of two terms to result in a polynomial. If we restrict ourselves to multiplications where multiples of monomials are again monomials, the proof of Lemma 4.2.26 carries over and we can look for appropriate localizations.

However, the reduction relation defined in Definition 4.2.43 is only one way of defining a reduction relation in $\mathcal{F}$ and we stated that the main motivation behind it is to link the reduction relation with special standard representations as it is done in the case of $\mathcal{F}_{\mathbb{K}}$. The question now arises whether this motivation is as appropriate for $\mathcal{F}$ as it was for $\mathcal{F}_{\mathbb{K}}$. In $\mathcal{F}_{\mathbb{K}}$ any reduction relation based on stable divisibility of terms can be linked to right reductive standard representations as defined in Definition 4.2.15 and hence the approach is very powerful. It turns out that for different reduction relations in $\mathcal{F}$ based on stable right divisibility this is no longer so. Let us look at another familiar way of generalizing a reduction relation for $\mathcal{F}$ from one defined in the reduction ring. From now on we require a (not necessarily Noetherian) partial ordering on R: 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 ensures that reduction in $\mathcal{F}$ is terminating when using a finite set of polynomials.

Definition 4.2.53
Let f, p be two non-zero polynomials in $\mathcal{F}$. We say f **right reduces** p **to** q **at a monomial** $\alpha \cdot t$ **in one step**, denoted by $p \longrightarrow^{\mathrm{r}}_f q$, if there exists $m \in \mathsf{M}(\mathcal{F})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) = t \geq \mathsf{HT}(f)$,
3. $\alpha \Longrightarrow_{\mathsf{HC}(f \star m)} \beta$, with $\alpha = \mathsf{HC}(f \star m) + \beta$ for some $\beta \in \mathsf{R}$, and
4. $q = p - f \star m$.

We write $p \longrightarrow^{\mathrm{r}}_f$ if there is a polynomial q as defined above and p is then called right reducible by f. Further, we can define $\overset{*}{\longrightarrow}^{\mathrm{r}}$, $\overset{+}{\longrightarrow}^{\mathrm{r}}$ and $\overset{n}{\longrightarrow}^{\mathrm{r}}$ as usual. Right reduction by a set $F \subseteq \mathcal{F} \backslash \{o\}$ is denoted by $p \longrightarrow^{\mathrm{r}}_F q$ and abbreviates $p \longrightarrow^{\mathrm{r}}_f q$ for some $f \in F$. ◇

Notice that in specifying this reduction relation we use a special instance of $\alpha \Longrightarrow_{\mathsf{HC}(f \star m)} \beta$, namely the case that $\alpha = \mathsf{HC}(f \star m) + \beta$ for some $\beta \in \mathsf{R}$. Moreover, for this reduction relation we can still have $t \in \mathsf{supp}(q)$. Hence other arguments than used in the proof of Lemma 4.2.44 have to be provided to show termination. It turns out that for infinite subsets of polynomials F in $\mathcal{F}$ the reduction relation $\longrightarrow^{\mathrm{r}}_F$ need not terminate.

Example 4.2.54
Let $\mathsf{R} = \mathbb{Q}[\{X_i \mid i \in \mathbb{N}\}]$ with $X_1 \succ X_2 \succ \ldots$ be the polynomial ring over the

rationals with infinitely many indeterminates. We associate this ring with the reduction relation based on divisibility of terms. Let $\mathcal{F} = \mathsf{R}[Y]$ be our function ring. Elements of $\mathcal{F}$ are polynomials in Y^i, $i \in \mathbb{N}$ with coefficients in R. Then for $p = X_1 \cdot Y$ and the infinite set $F = \{f_i = (X_i - X_{i+1}) \cdot Y \mid i \in \mathbb{N}\}$ we get the infinite reduction sequence $p \longrightarrow^{\mathrm{r}}_{f_1} X_2 \cdot Y \longrightarrow^{\mathrm{r}}_{f_2} X_3 \cdot Y \longrightarrow^{\mathrm{r}}_{f_3} \ldots$ ⋄

However, if we restrict ourselves to finite sets of polynomials the reduction relation is Noetherian.

Lemma 4.2.55
Let F be a finite set of polynomials in $\mathcal{F}\backslash\{o\}$.

1. *For $p, q \in \mathcal{F}$ $p \longrightarrow^{\mathrm{r}}_{F} q$ implies $p \succ q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.*
2. *$\longrightarrow^{\mathrm{r}}_{F}$ is Noetherian.*

Proof :

1. Assuming that the reduction step takes place at a monomial $\alpha \cdot t$, by Definition 4.2.53 we know $\mathsf{HM}(\alpha \cdot t - f \star m) = \beta \cdot t$ which yields $p \succ p - f \star m$ since $\alpha >_{\mathsf{R}} \beta$.
2. This follows from 1. and Axiom (A1) as long as only finite sets of polynomials are involved. Since we have $\mathsf{HT}(f \star m) = \mathsf{HT}(\mathsf{HT}(f) \star m) \geq \mathsf{HT}(f)$ we get $\mathsf{HC}(f \star m) = \mathsf{HC}(f) \cdot \mathsf{HC}(\mathsf{HT}(f) \star m)$. Then $\alpha \Longrightarrow_{\mathsf{HC}(f \star m)} \beta$ implies $\alpha \Longrightarrow_{\mathsf{HC}(f)}$. Hence an infinite reduction sequence would give rise to an infinite reduction sequence in R with respect to the finite set of head coefficients $\{\mathsf{HC}(f) \mid f \in F\}$ contradicting our assumption.

q.e.d.

Now if we try to link the reduction relation in Definition 4.2.53 to special standard representations, we find that this is no longer as natural as in the cases studied before, where for $\mathcal{F}_{\mathbb{K}}$ we linked the reduction relation from Definition 4.2.27 to the right reductive standard representations in Definition 4.2.15 respectively for $\mathcal{F}$ the right reduction relation from Definition 4.2.43 to right reductive standard representations as defined in Definition 4.2.42. Hence we claim that for generalizing Gröbner bases to $\mathcal{F}$, the rewriting approach is more suitable. Hence we use the following definition of weak right Gröbner bases in terms of our reduction relation.

Definition 4.2.56
A set $F \subseteq \mathcal{F}\backslash\{o\}$ is called a weak right Gröbner basis (with respect to $\longrightarrow^{\mathrm{r}}$) of $\mathsf{ideal}_r(F)$ if for all $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}^{\mathrm{r}}_{F} o$. ⋄

Every reduction sequence $g \xrightarrow{*}{}^{\mathrm{r}}_{F} o$ gives rise to a special representation of g in terms of F which could be taken as a new definition of standard representations.

Corollary 4.2.57
Let F be a set of polynomials in $\mathcal{F}$ and g a non-zero polynomial in $\mathsf{ideal}_r(F)$ such that $g \xrightarrow{*}{}^{\mathrm{r}}_{F} o$. Then g has a representation of the form

$$g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) = \mathsf{HT}(f_i \star m_i) \geq \mathsf{HT}(f_i)$ for $1 \leq i \leq k$, and $\mathsf{HT}(g) \succ \mathsf{HT}(f_i \star m_i)$ for all $k+1 \leq i \leq n$.

Proof :
We show our claim by induction on n where $g \xrightarrow{n}{}^{\mathrm{r}}_{F} o$. If $n = 0$ we are done. Else let $g \xrightarrow{1}{}^{\mathrm{r}}_{F} g_1 \xrightarrow{n}{}^{\mathrm{r}}_{F} o$. In case the reduction step takes place at the head monomial, there exists a polynomial $f \in F$ and a monomial $m \in \mathsf{M}(\mathcal{F})$ such that $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) = \mathsf{HT}(g) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g) \Longrightarrow_{\mathsf{HC}(f \star m)} \beta$ with $\mathsf{HC}(g) = \mathsf{HC}(f \star m) + \beta$ for some $\beta \in \mathsf{R}$. Moreover the induction hypothesis then is applied to $g_1 = g - f \star m \cdot \beta$. If the reduction step takes place at a monomial with term smaller $\mathsf{HT}(g)$ for the respective monomial multiple $f \star m$ we immediately get $\mathsf{HT}(g) \succ \mathsf{HT}(f \star m)$ and we can apply our induction hypothesis to the resulting polynomial g_1. In both cases we can arrange the monomial multiples $f \star m$ arising from the reduction steps in such a way that gives us th desired representation.
q.e.d.

Notice that on the other hand the existence of such a representation for a polynomial does not imply reducibility. For example take the polynomial ring $\mathbb{Z}[X]$ with Pan's reduction. Then with respect to the polynomials $F = \{2 \cdot X, 3 \cdot X\}$ the polynomial $g = 5 \cdot X$ has a representation $5 \cdot X = 2 \cdot X + 3 \cdot X$ of the desired form but is neither reducible by $2 \cdot X$ nor $3 \cdot X$. This is of course a consequence of the fact that $\{2, 3\}$ is no Gröbner basis in $\mathbb{Z}$ with respect to Pan's reduction.

In fact Corollary 4.2.57 provides additional information for the head coefficient of g, namely $\mathsf{HC}(g) = \sum_{i=1}^{k} \mathsf{HC}(f_i) \cdot \mathsf{HC}(m_i)$ and this is a standard representation of $\mathsf{HC}(g)$ in terms of $\{\mathsf{HC}(f_i) \mid 1 \leq i \leq k\}$ in the reduction ring R.

We can characterize weak right Gröbner bases similar to Theorem 4.2.51. Of course the g-polynomials in Definition 4.2.50 depend on the reduction relation $\Longrightarrow$ in R which now is defined according to Definition 4.2.53. Notice that the characterization will only hold for finite sets as the proof requires the reduction relation to be Noetherian. Additionally we need that the reduction ring fulfills

Axiom (A4), i.e., for $\alpha, \beta, \gamma, \delta \in \mathsf{R}$, $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_\gamma \delta$ imply $\alpha \Longrightarrow_\gamma$ or $\alpha \Longrightarrow_\delta$[33].

Theorem 4.2.58
Let F be a finite set of polynomials in $\mathcal{F}\backslash\{o\}$ where the reduction ring satisfies (A4). Then F is a weak right Gröbner basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for all f in F and for all m in $\mathsf{M}(\mathcal{F})$ we have $f \star m \xrightarrow{*}{}^{\mathrm{r}}_F o$, and*
2. *all g- and m-polynomials corresponding to F as specified in Definition 4.2.50 reduce to o using F.*

Proof :
In case F is a weak right Gröbner basis, since the multiples $f \star m$ and the respective g- and m-polynomials are all elements of $\mathsf{ideal}_r(F)$ they must reduce to zero using F.
The converse will be proven by showing that every element in $\mathsf{ideal}_r(F)$ is reducible by F. Then as $g \in \mathsf{ideal}_r(F)$ and $g \longrightarrow^{\mathrm{r}}_F g'$ implies $g' \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}^{\mathrm{r}}_F o$. Notice that this only holds in case the reduction relation $\longrightarrow^{\mathrm{r}}_F$ is Noetherian. This follows as by our assumption F is finite (Lemma 4.2.55).
Let $g \in \mathsf{ideal}_r(F)$ have a representation in terms of F of the following form: $g = \sum_{j=1}^{m} f_j \star (w_j \cdot \alpha_j)$ such that $f_j \in F$, $w_j \in \mathcal{T}$, $\alpha_j \in \mathsf{R}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_\succeq\{\mathsf{HT}(f_j \star (w_j \cdot \alpha_j)) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $f_j \star (w_j \cdot \alpha_j)$ with head term t. We show our claim by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$).
Since by our first assumption every multiple $f_j \star (w_j \cdot \alpha_j)$ in this sum reduces to zero using F and hence has a right representation as defined in Corollary 4.2.57, we can assume that $\mathsf{HT}(\mathsf{HT}(f_j) \star w_j) = \mathsf{HT}(f_j \star w_j) \geq \mathsf{HT}(f_j)$ holds. Moreover, without loss of generality we can assume that the polynomial multiples with head term t are just $f_1 \star (w_1 \cdot \alpha_1), \ldots, f_K \star (w_K \cdot \alpha_K)$. Notice that these assumptions neither change t nor K for our representation of g.
Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and even $\mathsf{HM}(g) = \mathsf{HM}(f_1 \star (w_1 \cdot \alpha_1))$, implying that g is right reducible at $\mathsf{HM}(g)$ by f_1. Hence let us assume $K > 1$.
First let $\sum_{j=1}^{K} \mathsf{HM}(f_j \star (w_j \cdot \alpha_j)) = o$. Then by Definition 4.2.50 we know $(\alpha_1, \ldots, \alpha_K) \in M$, as $\sum_{j=1}^{K} \mathsf{HC}(f_j \star w_j) \cdot \alpha_j = 0$. Hence there are $\delta_1, \ldots, \delta_K \in \mathsf{R}$ such that $\sum_{i=1}^{l} A_i \cdot \delta_i = (\alpha_1, \ldots, \alpha_K)$ for some $l \in \mathbb{N}$, $A_i = (\alpha_{i,1}, \ldots, \alpha_{i,K}) \in \{A_j \mid j \in I_M\}$, and $\alpha_j = \sum_{i=1}^{l} \alpha_{i,j} \cdot \delta_i$, $1 \leq j \leq K$. By our assumption there are module

[33] Notice that (A4) is no basis for localizing test sets, as this would require that $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_\gamma \delta$ imply $\alpha \Longrightarrow_\gamma$. Hence even if the reduction relation in $\mathcal{F}$ satisfies (A4), this does not substitute Lemma 4.2.26 or its variants.

polynomials $h_i = \sum_{j=1}^{K} f_j \star w_j \cdot \alpha_{i,j}$,$1 \leq i \leq l$, all having representations in terms of F as defined in Corollary 4.2.57.
Then since

$$\begin{aligned}
\sum_{j=1}^{K} f_j \star (w_j \cdot \alpha_j) &= \sum_{j=1}^{K} f_j \star w_j \cdot (\sum_{i=1}^{l} \alpha_{i,j} \cdot \delta_i) \\
&= \sum_{j=1}^{K} \sum_{i=1}^{l} (f_j \star w_j \cdot \alpha_{i,j}) \cdot \delta_i \\
&= \sum_{i=1}^{l} (\sum_{j=1}^{K} f_j \star w_j \cdot \alpha_{i,j}) \cdot \delta_i \\
&= \sum_{i=1}^{l} h_i \cdot \delta_i
\end{aligned}$$

we can change the representation of g to $\sum_{i=1}^{l} h_i \cdot \delta_i + \sum_{j=K+1}^{m} f_j \star (w_j \cdot \alpha_j)$ and replace each h_i by its respective representation in terms of F. Remember that for all h_i, $1 \leq i \leq l$ we have $\mathsf{HT}(h_i) \prec t$. Hence, for this new representation we now have maximal term smaller than t and by our induction hypothesis g is reducible by F and we are done.
It remains to study the case where $\sum_{j=1}^{K} \mathsf{HM}(f_j \star (w_j \cdot \alpha_j)) \neq 0$. Then we have $\mathsf{HT}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) = t = \mathsf{HT}(g)$, $\mathsf{HC}(g) = \mathsf{HC}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) \in \mathsf{ideal}_r(\{\mathsf{HC}(f_1 \star w_1), \ldots, \mathsf{HC}(f_K \star w_K)\})$ and even $\mathsf{HM}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) = \mathsf{HM}(g)$. Hence $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by some α, $\alpha \in G$, a (weak) right Gröbner basis of $\mathsf{ideal}_r(\{\mathsf{HC}(f_1 \star w_1), \ldots, \mathsf{HC}(f_K \star w_K)\})$ in R with respect to the reduction relation $\Longrightarrow$. Let g_α be the respective g-polynomial corresponding to α and t. Then we know that $g_\alpha \xrightarrow{*}{}^{\mathrm{r}}_F o$. Moreover, we know that the head monomial of g_α is reducible by some polynomial $f \in F$ and we assume $\mathsf{HT}(g_\alpha) = \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g_\alpha) \Longrightarrow_{\mathsf{HC}(f \star m)}$. Then, as $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by $\mathsf{HC}(g_\alpha)$, $\mathsf{HC}(g_\alpha)$ is $\Longrightarrow$-reducible and (A4) holds, the head monomial of g is also reducible by some $f' \in F$ and we are done.

q.e.d.

Of course this theorem is also true for infinite F if we can show that for the respective function ring the reduction relation is terminating.

Now the question arises when the critical situations in this characterization can be localized to subsets of the respective sets as in Theorem 4.2.41. Reviewing the Proof of Theorem 4.2.41 we find that Lemma 4.2.26 is central as it describes when multiples of polynomials which have a right reductive standard representation in terms of some set F again have such a representation. As we have seen above, this will not hold for function rings over reduction rings in general. Now one way to introduce localizations would be to restrict the attention to those $\mathcal{F}$ satisfying

Lemma 4.2.26. Then appropriate adaptions of Definition 4.2.34, 4.2.35 and 4.2.38 would allow a localization of the critical situations. However, we have stated that it is not natural to link right reduction as defined in Definition 4.2.43 to special standard representations. Hence, to give localizations of Theorem 4.2.58 another property for $\mathcal{F}$ is sufficient:

Definition 4.2.59
A set $C \subset S \subseteq \mathcal{F}$ is called a **stable localization** of S if for every $g \in S$ there exists $f \in C$ such that $g \longrightarrow^{\mathrm{r}}_{f} o$. ◇

In case $\mathcal{F}$ and $\longrightarrow^{\mathrm{r}}$ allow such stable localizations, we can rephrase Theorem 4.2.58 as follows:

Theorem 4.2.60
Let F be a finite set of polynomials in $\mathcal{F}\backslash\{o\}$ where the reduction ring satisfies (A4). Then F is a weak right Gröbner basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for all s in a stable localization of $\{f \star m \mid f \in \mathcal{F}, m \in \mathsf{M}(\mathcal{F})\}$ we have $s \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} o$, and*
2. *for all h in a stable localization of the g- and m-polynomials corresponding to F as specified in Definition 4.2.50 we have $h \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} o$.*

We have stated that for arbitrary reduction relations in $\mathcal{F}$ it is not natural to link them to special standard representations. Still, when proving Theorem 4.2.60, we will find that in order to change the representation of an arbitrary right ideal element, Definition 4.2.59 is not enough to ensure reducibility. However, we can substitute the critical situation using an analogon of Lemma 4.2.26, which, while not related to reducibility, in this case will still be sufficient to make the representation smaller.

Lemma 4.2.61
Let F be a subset of polynomials in $\mathcal{F}\backslash\{o\}$ and f, p non-zero polynomials in $\mathcal{F}$. If $p \longrightarrow^{\mathrm{r}}_{f} o$ and $f \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} o$, then p has a standard representation of the form

$$p = \sum_{i=1}^{n} f_i \star l_i, f_i \in F, l_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$$

such that $\mathsf{HT}(p) = \mathsf{HT}(\mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(f_i \star l_i) \geq \mathsf{HT}(f_i)$ for $1 \leq i \leq k$ and $\mathsf{HT}(p) \succ \mathsf{HT}(f_i \star l_i)$ for all $k+1 \leq i \leq n$ (compare Definition 4.2.15).

Proof :
If $p \longrightarrow^{\mathrm{r}}_{f} o$ then $p = f \star m$ with $m \in \mathsf{M}(\mathcal{F})$ and $\mathsf{HT}(p) = \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)$. Similarly $f \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} o$ implies $f = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in$

$\mathsf{M}(\mathcal{F}), n \in \mathbb{N}$ such that $\mathsf{HT}(f) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) = \mathsf{HT}(f_i \star m_i) \geq \mathsf{HT}(f_1)$, $1 \leq i \leq k$, and $\mathsf{HT}(f) \succ \mathsf{HT}(f_i \star m_i)$ for all $k+1 \leq i \leq n$ (compare Corollary 4.2.57).

Let us first analyze $f_i \star m_i \star m$ with $\mathsf{HT}(f_i \star m_i) = \mathsf{HT}(f)$, $1 \leq i \leq k$.

Let $\mathsf{T}(f_i \star m_i) = \{s^i_1, \ldots, s^i_{k_i}\}$ with $s^i_1 \succ s^i_j$, $2 \leq j \leq k_i$, i.e., $s^i_1 = \mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) = \mathsf{HT}(f)$. Hence $\mathsf{HT}(f) \star m = s^i_1 \star m \geq \mathsf{HT}(f) = s^i_1$ and as $s^i_1 \succ s^i_j$, $2 \leq j \leq k_i$, by Definition 4.2.13 we can conclude that $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(s^i_1 \star m) \succ s^i_j \star m \succeq \mathsf{HT}(s^i_j \star m)$ for $2 \leq j \leq k_i$. This implies $\mathsf{HT}(\mathsf{HT}(f_i \star m_i) \star m) = \mathsf{HT}(f_i \star m_i \star m)$. Hence we get

$$\begin{aligned} \mathsf{HT}(f \star m) &= \mathsf{HT}(\mathsf{HT}(f) \star m) \\ &= \mathsf{HT}(\mathsf{HT}(f_i \star m_i) \star m), \text{ as } \mathsf{HT}(f) = \mathsf{HT}(f_i \star m_i) \\ &= \mathsf{HT}(f_i \star m_i \star m) \end{aligned}$$

and since $\mathsf{HT}(f \star m) \geq \mathsf{HT}(f) \geq \mathsf{HT}(f_i)$ we can conclude $\mathsf{HT}(f_i \star m_i \star m) \geq \mathsf{HT}(f_i)$. It remains to show that the $f_i \star m_i \star m$ have representations of the desired form in terms of F. First we show that $\mathsf{HT}(\mathsf{HT}(f_i) \star m_i \star m) \geq \mathsf{HT}(f_i)$. We know $\mathsf{HT}(f_i) \star m_i \succeq \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) = \mathsf{HT}(f_i \star m_i)$[34] and hence $\mathsf{HT}(\mathsf{HT}(f_i) \star m_i \star m) = \mathsf{HT}(\mathsf{HT}(f_i \star m_i) \star m) = \mathsf{HT}(f_i \star m_i \star m) \geq \mathsf{HT}(f_i)$. Then in case $m_i \star m \in \mathsf{M}(\mathcal{F})$ we are done as then $f_i \star (m_i \star m)$ is a representation of the desired form.

Hence let us assume $m_i \star m = \sum_{r=1}^{k_i} \tilde{m}^i_r$, $\tilde{m}^i_r \in \mathsf{M}(\mathcal{F})$. Let $\mathsf{T}(f_i) = \{t^i_1, \ldots, t^i_{w_i}\}$ with $t^i_1 \succ t^i_l$, $2 \leq l \leq w_i$, i.e., $t^i_1 = \mathsf{HT}(f_i)$. As $\mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \geq \mathsf{HT}(f_i) \succ t^i_l$, $2 \leq l \leq w_i$, again by Definition 4.2.13 we can conclude that $\mathsf{HT}(\mathsf{HT}(f_i) \star m_i) \succ t^i_l \star m_i \succeq \mathsf{HT}(t^i_l \star m_i)$, $2 \leq l \leq w_i$, and $\mathsf{HT}(f_i) \star m_i \succ \sum_{l=2}^{w_i} t^i_l \star m_i$. Then for each s^i_j, $2 \leq j \leq k_i$, there exists $t^i_l \in \mathsf{T}(f_i)$ such that $s \in \mathsf{supp}(t^i_l \star m_i)$. Since $\mathsf{HT}(f) \succ s^i_j$ and even $\mathsf{HT}(f) \succ t^i_l \star m_i$ we find that either $\mathsf{HT}(f \star m) \succeq \mathsf{HT}((t^i_l \star m_i) \star m) = \mathsf{HT}(t^i_l \star (m_i \star m))$ in case $\mathsf{HT}(t^i_l \star m_i) = \mathsf{HT}(f_i \star m_i)$ or $\mathsf{HT}(f \star m) \succ (t^i_l \star m_i) \star m = t^i_l \star (m_i \star m)$. Hence we can conclude $f_i \star \tilde{m}^i_r \preceq \mathsf{HT}(f \star m)$, $1 \leq r \leq k_i$ and for at least one $\tilde{m}^i_r$ we get $\mathsf{HT}(f_i \star \tilde{m}^i_r) = \mathsf{HT}(f_i \star m_i \star m) \geq \mathsf{HT}(f_i)$.

It remains to analyze the situation for the function $(\sum_{i=k+1}^n f_i \star m_i) \star m$. Again we find that for all terms s in the $f_i \star m_i$, $k+1 \leq i \leq n$, we have $\mathsf{HT}(f) \succ s$ and we get $\mathsf{HT}(f \star m) \succ \mathsf{HT}(s \star m)$. Hence all polynomial multiples of the f_i in the representation $\sum_{i=k+1}^n \sum_{j=1}^{k_i} f_i \star \tilde{m}^i_j$, where $m_i \star m = \sum_{j=1}^{k_i} \tilde{m}^i_j$, are bounded by $\mathsf{HT}(f \star m)$.

q.e.d.

Now we are able to prove Theorem 4.2.60.

Proof of Theorem 4.2.60:

The proof is basically the same as for Theorem 4.2.58. Due to Lemma 4.2.61

[34] Notice that $\mathsf{HT}(f_i) \star m_i$ can be a polynomial and hence we cannot conclude $\mathsf{HT}(f_i) \star m_i = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i)$.

we can substitute the multiples $f_j \star m_j$ by appropriate representations without changing (t, K). Hence, we only have to ensure that despite testing less polynomials we are able to apply our induction hypothesis. Taking the notations from the proof of Theorem 4.2.58, let us first check the situation for m-polynomials.
Let $\sum_{j=1}^{K} \mathsf{HM}(f_j \star (w_j \cdot \alpha_j)) = o$. Then by Definition 4.2.50 we know $(\alpha_1, \ldots, \alpha_K) \in M$, as $\sum_{j=1}^{K} \mathsf{HC}(f_j \star w_j) \cdot \alpha_j = 0$. Hence there are $\delta_1, \ldots, \delta_K \in \mathsf{R}$ such that $\sum_{i=1}^{l} A_i \cdot \delta_i = (\alpha_1, \ldots, \alpha_K)$ for some $l \in \mathbb{N}$, $A_i = (\alpha_{i,1}, \ldots, \alpha_{i,K}) \in \{A_j \mid j \in I_M\}$, and $\alpha_j = \sum_{i=1}^{l} \alpha_{i,j} \cdot \delta_i$, $1 \leq j \leq K$. There are module polynomials $h_i = \sum_{j=1}^{K} f_j \star w_j \cdot \alpha_{i,j}$,$1 \leq i \leq l$ and by our assumption there are polynomials h'_i in the stable localization such that $h_i \longrightarrow^{\mathrm{r}}_{h'_i} o$. Moreover, $h'_i \stackrel{*}{\longrightarrow}^{\mathrm{r}}_F o$. Then by Lemma 4.2.61 the m-polynomials h_i all have representations bounded by t. Again we get

$$\begin{aligned}
\sum_{j=1}^{K} f_j \star (w_j \cdot \alpha_j) &= \sum_{j=1}^{K} f_j \star w_j \cdot (\sum_{i=1}^{l} \alpha_{i,j} \cdot \delta_i) \\
&= \sum_{j=1}^{K} \sum_{i=1}^{l} (f_j \star w_j \cdot \alpha_{i,j}) \cdot \delta_i \\
&= \sum_{i=1}^{l} (\sum_{j=1}^{K} f_j \star w_j \cdot \alpha_{i,j}) \cdot \delta_i \\
&= \sum_{i=1}^{l} h_i \cdot \delta_i
\end{aligned}$$

and we can change the representation of g to $\sum_{i=1}^{l} h_i \cdot \delta_i + \sum_{j=K+1}^{m} f_j \star (w_j \cdot \alpha_j)$ and replace each h_i by the respective special standard representation in terms of F. Remember that for all h_i, $1 \leq i \leq l$ we have $\mathsf{HT}(h_i) \prec t$. Hence, for this new representation we now have maximal term smaller than t and by our induction hypothesis g is reducible by F and we are done.
It remains to study the case where $\sum_{j=1}^{K} \mathsf{HM}(f_j \star (w_j \cdot \alpha_j)) \neq 0$. Then we have $\mathsf{HT}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) = t = \mathsf{HT}(g)$, $\mathsf{HC}(g) = \mathsf{HC}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) \in \mathsf{ideal}_r(\{\mathsf{HC}(f_1 \star w_1), \ldots, \mathsf{HC}(f_K \star w_K)\})$ and even $\mathsf{HM}(f_1 \star (w_1 \cdot \alpha_1) + \ldots + f_K \star (w_K \cdot \alpha_K)) = \mathsf{HM}(g)$. Hence $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by some α, $\alpha \in G$, G being a (weak) right Gröbner basis of $\mathsf{ideal}_r(\{\mathsf{HC}(f_1 \star w_1), \ldots, \mathsf{HC}(f_K \star w_K)\})$ in R with respect to the reduction relation $\Longrightarrow$. Let g_α be the respective g-polynomial corresponding to α and t. Then we know that $g_\alpha \longrightarrow^{\mathrm{r}}_{g'_\alpha} o$ for some g'_α in the stable localization and $g'_\alpha \stackrel{*}{\longrightarrow}^{\mathrm{r}}_F o$. Moreover, we know that the head monomial of g'_α is reducible by some polynomial $f \in F$ and we assume $\mathsf{HT}(g_\alpha) = \mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g_\alpha) \Longrightarrow_{\mathsf{HC}(f \star m)}$. Then, as $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by $\mathsf{HC}(g_\alpha)$, $\mathsf{HC}(g_\alpha)$ is $\Longrightarrow$-reducible by $\mathsf{HC}(g'_\alpha)$, $\mathsf{HC}(g'_\alpha)$ is $\Longrightarrow$-reducible to zero and (A4) holds, the head monomial of g is also

reducible by some $f' \in F$ and we are done.

q.e.d.

Again, if for infinite F we can assure that the reduction relation is Noetherian, the proof still holds.

4.2.3 Function Rings over the Integers

In the previous section we have seen that for the reduction relations for $\mathcal{F}$ as defined in Definition 4.2.43 and 4.2.53 the Translation Lemma no longer holds. This is due to the fact that the first definition is based on divisibility in R and hence too weak and the second definition is based on the abstract notion of the reduction relation $\Longrightarrow$ and hence there is not enough information on the reduction step involving the coefficient.

When studying special reduction rings where we have more information on the specific reduction relation $\Longrightarrow$ the situation often can be improved. Here we want to go into the details for the case that R is the ring of the integers $\mathbb{Z}$. Remember that there are various ways of defining a reduction relation for the integers. In Example 3.1.1 two possibilities are presented. Here we want to use the second one based on division with remainders in order to introduce a reduction relation to $\mathcal{F}_{\mathbb{Z}}$. We follow the ideas presented in [MR93b] for characterizing prefix Gröbner bases in monoid rings $\mathbb{Z}[\mathcal{M}]$ where $\mathcal{M}$ is presented by a finite convergent string rewriting system.

In order to use elements of $\mathcal{F}_{\mathbb{Z}}$ as rules for a reduction relation we need an ordering on $\mathbb{Z}$. We specify a total well–founded ordering on $\mathbb{Z}$ as follows[35]:

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

and $\alpha \leq_Z \beta$ iff $\alpha = \beta$ or $\alpha <_Z \beta$. Hence we get $0 \leq_Z 1 \leq_Z 2 \leq_Z 3 \leq_Z \ldots \leq_Z -1 \leq_Z -2 \leq_Z -3 \leq_Z \ldots$. Then we can make the following important observation: Let $\gamma \in \mathbb{N}$. We call the positive numbers $0, \ldots, \gamma - 1$ the remainders of γ. Then for each $\delta \in \mathbb{Z}$ there are unique $\alpha, \beta \in \mathbb{Z}$ such that $\delta = \alpha \cdot \gamma + \beta$ and β is a remainder of γ. We get $\beta < \gamma$ and in case $\delta > 0$ and $\alpha \neq 0$ even $\gamma \leq \delta$. Further γ does not divide $\beta_1 - \beta_2$, if β_1, β_2 are different remainders of γ.

As we will later on only use polynomials with head coefficients in $\mathbb{N}$ for reduction, we will mainly require the part of the ordering on $\mathbb{N}$ which then coincides with

[35] If not stated otherwise $<$ is the usual ordering on $\mathbb{Z}$, i.e. $\ldots < -3 < -2 < -1 < 0 < 1 < 2 < 3 \ldots$.

the natural ordering on this set. Then we will drop the suffix[36].

This ordering $<_Z$ can be used to induce an ordering on $\mathcal{F}_{\mathbb{Z}}$ as follows: for two elements f, g in $\mathcal{F}$ we define $f \succ g$ iff $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ or $((\mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HC}(f) >_Z \mathsf{HC}(g))$ or $((\mathsf{HM}(f) = \mathsf{HM}(g)$ and $\mathsf{RED}(f) \succ \mathsf{RED}(g))$.

The reduction relation presented in Definition 4.2.53 now can be adapted to this special case: Let $\Longrightarrow$ be our reduction relation on $\mathbb{Z}$ where $\alpha \Longrightarrow_\gamma \beta$, if $\gamma > 0$ and for some $\delta \in \mathbb{Z}$ we have $\alpha = \gamma \cdot \delta + \beta$ with $0 \leq \beta < \gamma$, i.e. β is the remainder of α modulo γ.

Definition 4.2.62
Let p, f be two non-zero polynomials in $\mathcal{F}_{\mathbb{Z}}$. We say f **right reduces** p **to** q **at a monomial** $\alpha \cdot t$ **in one step**, i.e. $p \longrightarrow^{\mathrm{r}}_f q$, if there exists $s \in \mathsf{T}(\mathcal{F}_{\mathbb{Z}})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(\mathsf{HT}(f) \star s) = \mathsf{HT}(f \star s) = t \geq \mathsf{HT}(f)$,
3. $\alpha \geq_{\mathbb{Z}} \mathsf{HC}(f \star m) > 0$ and $\alpha \Longrightarrow_{\mathsf{HC}(f \star s)} \delta$ where $\alpha = \mathsf{HC}(f \star s) \cdot \beta + \delta$ with $\beta, \delta \in \mathbb{Z}$, $0 \leq \delta < \mathsf{HC}(f \star s)$, and
4. $q = p - f \star m$ where $m = \beta \cdot s$.

We write $p \longrightarrow^{\mathrm{r}}_f$ if there is a polynomial q as defined above and p is then called right reducible by f. Further, we can define $\stackrel{*}{\longrightarrow}^{\mathrm{r}}$, $\stackrel{+}{\longrightarrow}^{\mathrm{r}}$ and $\stackrel{n}{\longrightarrow}^{\mathrm{r}}$ as usual. Right reduction by a set $F \subseteq \mathcal{F} \backslash \{o\}$ is denoted by $p \longrightarrow^{\mathrm{r}}_F q$ and abbreviates $p \longrightarrow^{\mathrm{r}}_f q$ for some $f \in F$. $\diamond$

As before, for this reduction relation we can still have $t \in \mathsf{supp}(q)$. Hence other arguments than those used in the proof of Lemma 4.2.44 have to be used to show termination. The important part now is that if we still have $t \in \mathsf{supp}(q)$ then its coefficient will be smaller according to our ordering $<_{\mathbb{Z}}$ chosen for $\mathbb{Z}$ and since this ordering is well-founded we are done. Notice that in contrary to Lemma 4.2.55 we do not have to restrict ourselves to finite sets of polynomials in order to ensure termination.

The additional information we have on the coefficients before and after the reduction step now enables us to prove an analogon of the Translation Lemma for function rings over the integers. The first and second part of the lemma are only needed to prove the essential third part.

Lemma 4.2.63
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}}$ and p, q, h polynomials in $\mathcal{F}_{\mathbb{Z}}$.

[36] In the literature other orderings on the integers are used by Buchberger and Stifter [Sti87] and Kapur and Kandri-Rody [KRK88]. They then have to consider s- and t-polynomials as critical situations.

1. *Let $p - q \longrightarrow^{\mathrm{r}}_F h$ such that the reduction step takes place at the monomial $\alpha \cdot t$ and we additionally have $t \notin \mathsf{supp}(h)$. Then there exist $p', q' \in \mathcal{F}_{\mathbb{Z}}$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_F p'$ and $q \xrightarrow{*}{}^{\mathrm{r}}_F q'$ and $h = p' - q'$.*

2. *Let o be the unique normal form of p with respect to F and $t = \mathsf{HT}(p)$. Then there exists a polynomial $f \in F$ such that $p \longrightarrow^{\mathrm{r}}_f p'$ and $t \notin \mathsf{supp}(p')$.*

3. *Let o be the unique normal form of $p - q$ with respect to F. Then there exists $g \in \mathcal{F}_{\mathbb{Z}}$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_F g$ and $q \xrightarrow{*}{}^{\mathrm{r}}_F g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{r}}_F h$ at the monomial $\alpha \cdot t$, i.e., $h = p - q - f \star m$ for some $m = \beta \cdot s \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}})$ such that $\mathsf{HT}(\mathsf{HT}(f) \star s) = \mathsf{HT}(f \star s) = t \geq \mathsf{HT}(f)$ and $\mathsf{HC}(f \star s) > 0$. Remember that α is the coefficient of t in $p - q$. Then as $t \notin \mathsf{supp}(h)$ we know $\alpha = \mathsf{HC}(f \star m)$. Let α_1 respectively α_2 be the coefficients of t in p respectively q and $\alpha_1 = \mathsf{HC}(f \star m) \cdot \beta_1 + \gamma_1$ respectively $\alpha_2 = \mathsf{HC}(f \star m) \cdot \beta_2 + \gamma_2$ for some $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Z}$ where $0 \leq \gamma_1, \gamma_2 < \mathsf{HC}(f \star s) \leq \mathsf{HC}(f \star m)$. Then $\alpha = \mathsf{HC}(f \star m) = \alpha_1 - \alpha_2 = \mathsf{HC}(f \star m) \cdot (\beta_1 - \beta_2) + (\gamma_1 - \gamma_2)$, and as $\gamma_1 - \gamma_2$ is no multiple of $\mathsf{HC}(f \star m)$ we have $\gamma_1 - \gamma_2 = 0$ and hence $\beta_1 - \beta_2 = 1$. We have to distinguish two cases:

   (a) $\beta_1 \neq 0$ and $\beta_2 \neq 0$: Then $p \longrightarrow^{\mathrm{r}}_F p - f \star m \cdot \beta_1 = p'$, $q \longrightarrow^{\mathrm{r}}_F q - f \star m \cdot \beta_2 = q'$ and $p' - q' = p - f \star m \cdot \beta_1 - q + f \star m \cdot \beta_2 = p - q - f \star m = h$.

   (b) $\beta_1 = 0$ and $\beta_2 = -1$ (the case $\beta_2 = 0$ and $\beta_1 = 1$ being symmetric): Then $p' = p$, $q \longrightarrow^{\mathrm{r}}_F q - f \star m \cdot \beta_2 = q + f \star m \cdot \beta = q'$ and $p' - q' = p - q - f \star m = h$.

2. Since $p \xrightarrow{*}{}^{\mathrm{r}}_F o$, $\mathsf{HM}(p) = \alpha \cdot t$ must be F-reducible. Let $f_1, \ldots, f_k \in F$ be all polynomials in F such that $\alpha \cdot t$ is reducible by them. Let $m_1, \ldots m_k$ be the respective monomials involved in possible reduction steps. Moreover, let $\gamma = \min_{1 \leq i \leq k}\{\mathsf{HC}(f_i \star m_i)\}$ and without loss of generality $\mathsf{HM}(f \star m) = \gamma \cdot t$ for some $f \in F$, $\mathsf{HT}(\mathsf{HT}(f) \star m) = \mathsf{HT}(f \star m) \geq \mathsf{HT}(f)$. We claim that for $p \longrightarrow^{\mathrm{r}}_{f_1} p - f \star m = p'$ we have $t \notin \mathsf{supp}(p')$. Suppose $\mathsf{HT}(p') = t$. Then by our definition of reduction we must have $0 < \mathsf{HC}(p') < \mathsf{HC}(f \star m)$. But then p' would no longer be F-reducible contradicting our assumption that o is the unique normal form of p.

3. Since o is the unique normal form of $p - q$ by 2. there exists a reduction sequence $p - q \longrightarrow^{\mathrm{r}}_{f_{i_1}} h_1 \longrightarrow^{\mathrm{r}}_{f_{i_2}} \ldots \longrightarrow^{\mathrm{r}}_{f_{i_k}} o$ such that for the head terms we get $\mathsf{HT}(p-q) \succ \mathsf{HT}(h_1) \succ \ldots$. We show our claim by induction on k, where

$p - q \xrightarrow{k}{}^{\mathrm{r}}_{F} o$ is such a reduction sequence. In the base case $k = 0$ there is nothing to show as then $p = q$. Hence, let $p - q \longrightarrow^{\mathrm{r}}_{F} h \xrightarrow{k}{}^{\mathrm{r}}_{F} o$. Then by 1. there are polynomials $p', q' \in \mathcal{F}_{\mathbb{Z}}$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_{F} p'$ and $q \xrightarrow{*}{}^{\mathrm{r}}_{F} q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \xrightarrow{k}{}^{\mathrm{r}}_{F} o$ yields the existence of a polynomial $g \in \mathcal{F}_{\mathbb{Z}}$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_{F} g$ and $q \xrightarrow{*}{}^{\mathrm{r}}_{F} g$.

q.e.d.

Hence weak Gröbner bases are in fact Gröbner bases and can be characterized as follows:

Definition 4.2.64
A set $F \subseteq \mathcal{F}_{\mathbb{Z}} \backslash \{o\}$ is called a (weak) right Gröbner basis of $\mathsf{ideal}_r(F)$ if for all $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}^{\mathrm{r}}_{F} o$. $\diamond$

Corollary 4.2.65
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}}$ and g a non-zero polynomial in $\mathsf{ideal}_r(F)$ such that $g \xrightarrow{*}{}^{\mathrm{r}}_{F} o$. Then g has a representation of the form

$$g = \sum_{i=1}^{n} f_i \star m_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i) = \mathsf{HT}(f_i \star m_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$, and $\mathsf{HT}(g) \succ \mathsf{HT}(f_i \star m_i) = \mathsf{HT}(\mathsf{HT}(f_i) \star m_i)$ for all $k + 1 \leq i \leq n$.

Proof :
We show our claim by induction on n where $g \xrightarrow{n}{}^{\mathrm{r}}_{F} o$. If $n = 0$ we are done. Else let $g \xrightarrow{1}{}^{\mathrm{r}}_{F} g_1 \xrightarrow{n}{}^{\mathrm{r}}_{F} o$. In case the reduction step takes place at the head monomial, there exists a polynomial $f \in F$ and a monomial $m = \beta \cdot s \in \mathsf{M}(\mathcal{F})$ such that $\mathsf{HT}(\mathsf{HT}(f) \star s) = \mathsf{HT}(f \star s) = \mathsf{HT}(g) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g) \Longrightarrow_{\mathsf{HC}(f \star s)} \delta$ with $\mathsf{HC}(g) = \mathsf{HC}(f \star s) \cdot \beta + \delta$ for some $\beta, \delta \in \mathbb{Z}$, $0 \leq \delta < \mathsf{HC}(f \star s)$. Moreover the induction hypothesis then is applied to $g_1 = g - f \star m$. If the reduction step takes place at a monomial with term smaller $\mathsf{HT}(g)$ for the respective monomial multiple $f \star m$ we immediately get $\mathsf{HT}(g) \succ \mathsf{HT}(f \star m)$ and we can apply our induction hypothesis to the resulting polynomial g_1. In both cases we can arrange the monomial multiples $f \star m$ arising from the reduction steps in such a way that gives us the desired representation.

q.e.d.

We can even state that $\mathsf{HC}(g) \xRightarrow{*}_{\{\mathsf{HC}(f_i \star m_i) | 1 \leq i \leq k\}} 0$. Now right Gröbner bases can be characterized using the concept of s-polynomials combined with the technique of saturation which is necessary in order to describe the whole right ideal congruence by the reduction relation.

Definition 4.2.66
Let p_1, p_2 be two polynomials in $\mathcal{F}_{\mathbb{Z}}$. If there are respective terms $t, u_1, u_2 \in \mathcal{T}$ such that $\mathsf{HT}(\mathsf{HT}(p_i) \star u_i) = \mathsf{HT}(p_i \star u_i) = t \geq \mathsf{HT}(p_i)$ let $HC(p_i \star u_i) = \gamma_i$. Assuming $\gamma_1 \geq \gamma_2 > 0$[37], there are $\beta, \delta \in \mathbb{Z}$ such that $\gamma_1 = \gamma_2 \cdot \beta + \delta$ and $0 \leq \delta < \gamma_2$ and we get the following s-polynomial

$$\mathsf{spol}_r(p_1, p_2, t, u_1, u_2) = p_2 \star u_2 \cdot \beta - p_1 \star u_1.$$

The set $\mathsf{SPOL}(\{p_1, p_2\})$ then is the set of all such s-polynomials corresponding to p_1 and p_2. ◇

These sets can be infinite[38].

Theorem 4.2.67
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}} \backslash \{o\}$. Then F is a right Gröbner basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for all f in F and for all m in $\mathsf{M}(\mathcal{F}_{\mathbb{Z}})$ we have $f \star m \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} o$, and*
2. *all s-polynomials corresponding to F as specified in Definition 4.2.66 reduce to o using F.*

Proof :
In case F is a right Gröbner basis, since the multiples $f \star m$ and the respective s-polynomials are all elements of $\mathsf{ideal}_r(F)$ they must reduce to zero using F.
The converse will be proven by showing that every element in $\mathsf{ideal}_r(F)$ is reducible by F. Then as $g \in \mathsf{ideal}_r(F)$ and $g \longrightarrow^{\mathrm{r}}_{F} g'$ implies $g' \in \mathsf{ideal}_r(F)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{r}}_{F} o$. Notice that this is sufficient as the reduction relation $\longrightarrow^{\mathrm{r}}_{F}$ is Noetherian.
Let $g \in \mathsf{ideal}_r(F)$ have a representation in terms of F of the following form: $g = \sum_{j=1}^{m} f_j \star w_j \cdot \alpha_j$ such that $f_j \in F$, $w_j \in \mathcal{T}$ and $\alpha_j \in \mathbb{Z}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(f_j \star w_j) \mid 1 \leq j \leq m\}$, K as the number of polynomials $f_j \star w_j$ with head term t, and $M = \{\{\mathsf{HC}(f_i \star w_i) \mid \mathsf{HT}(f_j \star w_j) = t\}\}$ a multiset in $\mathbb{Z}$. We show our claim by induction on (t, M), where $(t', M') < (t, M)$ if and only if $t' \prec t$ or ($t' = t$ and $M' \ll M$)[39].
Since by our first assumption every multiple $f_j \star w_j$ in this sum reduces to zero using F and hence has a representation as specified in Corollary 4.2.65, we can assume that $\mathsf{HT}(\mathsf{HT}(f_j) \star w_j) = \mathsf{HT}(f_j \star w_j) \geq \mathsf{HT}(f_j)$ holds. Moreover, without

[37] Notice that $\gamma_i > 0$ can always be achieved by studying the situation for $-p_i$ in case we have $HC(p_i \star u_i) < 0$.
[38] This is due to the fact that in general we cannot always find finite locations for t. One well-studied field are monoid rings.
[39] We define $M' \ll M$ if M can be transformed into M' by substituting elements in M with sets of smaller elements (with respect to our ordering on the integers.

loss of generality we can assume that the polynomial multiples with head term t are just $f_1 \star w_1, \ldots, f_K \star w_K$ and additionally we can assume $\mathsf{HC}(f_j \star w_j) > 0$[40]. Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and even $\mathsf{HM}(g) = \mathsf{HM}(f_1 \star w_1 \cdot \alpha_1)$, implying that g is right reducible at $\mathsf{HM}(g)$ by f_1. Hence let us assume $K > 1$.

Without loss of generality we can assume that $\mathsf{HC}(f_1 \star w_1) \geq \mathsf{HC}(f_2 \star w_2) > 0$ and there are $\alpha, \beta \in \mathbb{Z}$ such that $\mathsf{HC}(f_2 \star w_2) \cdot \alpha + \beta = \mathsf{HC}(f_1 \star w_1)$ and $\mathsf{HC}(f_2 \star w_2) > \beta \geq 0$. Since $t = \mathsf{HT}(f_1 \star w_1) = \mathsf{HT}(f_2 \star w_2)$ by Definition 4.2.66 we have an s-polynomial $\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) = f_2 \star w_2 \cdot \alpha - f_1 \star w_1$. If $\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) \neq o$[41] then $\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) \xrightarrow{*}{}^{\mathrm{r}}_{F} o$ implies $\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) = \sum_{i=1}^{k} \delta_i \cdot h_i \star v_i$, $\delta_i \in \mathbb{Z}$, $h_i \in F$, $v_i \in \mathcal{T}$ where this sum is a representation in the sense of Corollary 4.2.65 with terms bounded by $\mathsf{HT}(\mathsf{spol}_r(f_1, f_2, t, w_1, w_2)) \leq t$. This gives us

$$\begin{aligned}
g &= f_1 \star w_1 \cdot \alpha_1 + f_2 \star w_2 \cdot \alpha_2 + \sum_{j=3}^{m} f_j \star w_j \cdot \alpha_j \qquad (4.5)\\
&= f_1 \star w_1 \cdot \alpha_1 + \underbrace{f_2 \star w_2 \cdot \alpha_1 \cdot \alpha - f_2 \star w_2 \cdot \alpha_1 \cdot \alpha}_{=o} + f_2 \star w_2 \cdot \alpha_2 + \sum_{j=3}^{m} f_j \star w_j \cdot \alpha_j\\
&= f_2 \star w_2 \cdot (\alpha_1 \cdot \alpha + \alpha_2) - \underbrace{(f_2 \star w_2 \cdot \alpha - f_1 \star w_1}_{=\mathsf{spol}_r(f_1, f_2, t, w_1, w_2)} \cdot \alpha_1 + \sum_{j=3}^{m} f_j \star w_j \cdot \alpha_j\\
&= f_2 \star w_2 \cdot (\alpha_1 \cdot \alpha + \alpha_2) - (\sum_{i=1}^{k} \delta_i \cdot h_i \star v_i) \cdot \alpha_1 + \sum_{j=3}^{m} f_j \star w_j \cdot \alpha_j
\end{aligned}$$

and depending on this new representation of g we define $t' = \max_{\succeq}\{\mathsf{HT}(f_j \star w_j), \mathsf{HT}(h_j \star v_j) \mid f_j, h_j \text{ appearing in the new representation }\}$, and $M' = \{\{\mathsf{HC}(f_i \star w_i), \mathsf{HC}(h_j \star v_j) \mid \mathsf{HT}(f_j \star w_j) = \mathsf{HT}(h_j \star v_j) = t'\}\}$ and we either get $t' \prec t$ and have a smaller representation for g or in case $t' = t$ we have to distinguish two cases

1. $\alpha_1 \cdot \alpha + \alpha_2 = 0$.
   Then $M' = M - \{\{\mathsf{HC}(f_1 \star w_1), \mathsf{HC}(f_2 \star w_2)\}\} \cup \{\{\mathsf{HC}(h_j \star v_j) \mid \mathsf{HT}(h_j \star v_j) = t\}\}$. As those polynomials h_j with $\mathsf{HT}(h_j \star v_j) = t$ are used to right reduce the monomial $\beta \cdot t = \mathsf{HM}(\mathsf{spol}_r(f_1, f_2, t, w_1, w_2))$ we know that for them we have $0 < \mathsf{HC}(h_j \star v_j) \leq \beta < \mathsf{HC}(f_2 \star w_2) \leq \mathsf{HC}(f_1 \star w_1)$. Hence $M' \ll M$ and we have a smaller representation for g.

[40] This can easily be achieved by adding $-f$ to F for all $f \in F$ and using $(-f_j) \star w_j$ in case $\mathsf{HC}(f_j \star w_j) < 0$.

[41] In case $\mathsf{spol}_r(f_1, f_2, t, w_1, w_2) = o$ the proof is similar. We just have to substitute o in the equations below which immediately gives us a smaller representation of g.

2. $\alpha_1 \cdot \alpha + \alpha_2 \neq 0$.
   Then $M' = (M - \{\{\mathsf{HC}(f_1 \star w_1)\}\}) \cup \{\{\mathsf{HC}(h_j \star v_j) \mid \mathsf{HT}(h_j \star v_j) = t\}\}$. Again $M' \ll M$ and we have a smaller representation for g.

Notice that the case $t' = t$ and $M' \ll M$ cannot occur infinitely often but has to result in either $t' < t$ or will lead to $t' = t$ and $K = 1$ and hence to reducibility by $\longrightarrow^{\mathrm{r}}_{F}$.

q.e.d.

Now the question arises when the critical situations in this characterization can be localized to subsets of the respective sets as in Theorem 4.2.41. Reviewing the Proof of Theorem 4.2.41 we find that Lemma 4.2.26 is central as it describes when multiples of polynomials which have a right reductive standard representation in terms of some set F again have such a representation. As we have seen before, this will not hold for function rings over reduction rings in general. As in Section 4.2.2, to give localizations of Theorem 4.2.67 the concept of stable subsets is sufficient:

Definition 4.2.68
A set $C \subset S \subseteq \mathcal{F}_{\mathbb{Z}}$ is called a **stable localization** of S if for every $g \in S$ there exists $f \in C$ such that $g \longrightarrow^{\mathrm{r}}_{f} o$. $\diamond$

Stable localizations for the sets of s-polynomials again arise from the appropriate sets of least common multiples as presented on page 4.2.1. In case $\mathcal{F}_{\mathbb{Z}}$ and $\longrightarrow^{\mathrm{r}}$ allow such stable localizations, we can rephrase Theorem 4.2.67 as follows:

Theorem 4.2.69
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}} \backslash \{o\}$. Then F is a right Gröbner basis of $\mathsf{ideal}_r(F)$ if and only if

1. *for all s in a stable localization of $\{f \star m \mid f \in \mathcal{F}_{\mathbb{Z}}, m \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}})\}$ we have $s \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} o$, and*
2. *for all h in a stable localization of the s-polynomials corresponding to F as specified in Definition 4.2.66 we have $h \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} o$.*

When proving Theorem 4.2.69, we can substitute the critical situation using an analogon of Lemma 4.2.26, which will be sufficient to make the representation used in the proof smaller. It is a direct consequence of Lemma 4.2.61.

Corollary 4.2.70
Let $F \subseteq \mathcal{F}_{\mathbb{Z}} \backslash \{o\}$ and f, p non-zero polynomials in $\mathcal{F}_{\mathbb{Z}}$. If $p \longrightarrow^{\mathrm{r}}_{f} o$ and $f \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} o$, then p has a representation of the form

$$p = \sum_{i=1}^{n} f_i \star l_i, f_i \in F, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}}), n \in \mathbb{N}$$

such that $\mathsf{HT}(p) = \mathsf{HT}(\mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(f_i \star l_i) \geq \mathsf{HT}(f_i)$ *for* $1 \leq i \leq k$ *and* $\mathsf{HT}(p) \succ \mathsf{HT}(f_i \star l_i)$ *for all* $k+1 \leq i \leq n$ *(compare Definition 4.2.15).*

Proof Theorem 4.2.69:
The proof is basically the same as for Theorem 4.2.67. Due to Corollary 4.2.70 we can substitute the multiples $f_j \star w_j$ by appropriate representations. Hence, we only have to ensure that despite testing less polynomials we are able to apply our induction hypothesis. Taking the notations from the proof of Theorem 4.2.67, let us check the situation for $K > 1$.
Without loss of generality we can assume that $\mathsf{HC}(f_1 \star w_1) \geq \mathsf{HC}(f_2 \star w_2) > 0$ and there are $\alpha, \beta \in \mathbb{Z}$ such that $\mathsf{HC}(f_2 \star w_2) \cdot \alpha + \beta = \mathsf{HC}(f_1 \star w_1)$ and $\mathsf{HC}(f_2 \star w_2) > \beta \geq 0$. Since $t = \mathsf{HT}(f_1 \star w_1) = \mathsf{HT}(f_2 \star w_2)$ by Definition 4.2.66 we have an s-polynomial $h \in \mathsf{SPOL}(f_1, f_2)$ and $m \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}})$ such that $h \star m = \alpha \cdot f_2 \star w_2 - f_1 \star w_1$. If $h \neq o$[42] then by Corollary 4.2.70 $f_2 \star w_2 \cdot \alpha - f_1 \star w_1 \longrightarrow^{\mathrm{r}}_{h} o$ and $h \xrightarrow{*}^{\mathrm{r}}_{F} o$ imply $f_2 \star w_2 \cdot \alpha - f_1 \star w_1 = \sum_{i=1}^{k} h_i \star v_i \cdot \delta_i$, $\delta_i \in \mathbb{Z}$, $h_i \in F$, $v_i \in \mathcal{T}$ where this sum is a representation in the sense of Corollary 4.2.65 with terms bounded by $\mathsf{HT}(h \star m) \preceq t$. As in the proof of Theorem 4.2.67 we now can use this bounded representation to get a smaller representation of g and are done.

q.e.d.

We close this subsection by outlining how different structures known to allow finite Gröbner bases can be interpreted as function rings. Using the respective interpretations the terminology can be adapted at once to the respective structures and in general the resulting characterizations of Gröbner bases coincide with the results known from literature.

Polynomial Rings

A commutative polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the set of terms $\{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{N}\}$.
- $\succ$ can be any admissible term ordering on $\mathcal{T}$. For the reductive ordering $\geq$ we have $t \geq s$ if s divides t as as term.
- Multiplication $\star$ is specified by the action on terms, i.e. $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ where $x_1^{i_1} \ldots x_n^{i_n} \star x_1^{j_1} \ldots x_n^{j_n} = x_1^{i_1+j_1} \ldots x_n^{i_n+j_n}$.

We do not need the concept of weak saturation.

[42] In case $h = o$ the proof is similar. We just have to substitute o in the equations below which immediately gives us a smaller representation of g.

Since the integers are an instance of euclidean domains, similar reductions to those given by Kandri-Rodi and Kapur in [KRK88] arise. A stable localization of $\mathcal{C}_s(p,q)$ is already provided by the tuple corresponding to the least common multiple of the terms $\mathsf{HT}(p)$ and $\mathsf{HT}(q)$. In contrast to the s- and t-polynomials studied by Kandri-Rodi and Kapur, we restrict ourselves to s-polynomials as described in Definition 4.2.66.

Since this structure is Abelian, one-sided and two-sided ideals coincide. Buchberger's Algorithm provides an effictive procedure to compute finite Gröbner bases.

Non-commutative Polynomial Rings

A non-commutative polynomial ring $\mathbb{Z}[\{x_1,\ldots,x_n\}^*]$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the set of words on $\{x_1,\ldots,x_n\}$.
- $\succ$ can be any admissible ordering on $\mathcal{T}$. For the reductive ordering $\geq$ we can chose $t \geq s$ if s is a subword of t.
- Multiplication $\star$ is specified by the action on words which is just concatenation.

We do not need the concept of weak saturation. A stable localization of $\mathcal{C}_s(p,q)$ is already provided by the tuples corresponding to word overlaps resulting from the equations $u_1\mathsf{HT}(p)v_1 = \mathsf{HT}(q)$, $u_2\mathsf{HT}(q)v_2 = \mathsf{HT}(p)$, $u_3\mathsf{HT}(p) = \mathsf{HT}(q)v_3$ respectively $u_4\mathsf{HT}(q) = \mathsf{HT}(p)v_4$ with the restriction that $|u_3| < |\mathsf{HT}(q)|$ and $|u_4| < |\mathsf{HT}(p)|$, $u_i, v_i \in \mathcal{T}$. The coefficients arise as described in Definition 4.2.66.

This structure is not Abelian. For the case of one-sided ideals finite Gröbner bases can be computed. The case of two-sided ideals only allows an enumerating procedure. This is not surprising as the word problem for monoids can be reduced to the problem of computing the respective Gröbner bases (see e.g. [Mor87, MR98d]).

Monoid and Group Rings

A monoid or group ring $\mathbb{Z}[\mathcal{M}]$ is a function ring according to the following interpretation:

- $\mathcal{T}$ is the monoid or group $\mathcal{M}$. In the cases studied by us as well as in [Ros93, Lo96], it is assumed that the elements of the monoid or group have a certain form. This presentation is essential in the approach. We will assume that the given monoid or group is presented by a convergent semi-Thue system.

- $\succ$ will be the completion ordering induced from the presentation of $\mathcal{M}$ to $\mathcal{M}$ and hence to $\mathcal{T}$. The reductive ordering $\geq$ depends on the choice of the presentation.

- Multiplication $\star$ is specified by lifting the monoid or group operation.

The concept of weak saturation and the choice of stable localizations of $\mathcal{C}_s(p, q)$ again depend on the choice of the presentation. More on this topic can be found in [Rei95].

4.3 Right $\mathcal{F}$-Modules

The concept of modules arises naturally as a generalization of the concept of an ideal in a ring: Remember that an ideal of a ring is an additive subgroup of the ring which is additionally closed under multiplication with ring elements. Extending this idea to arbitrary additive groups then gives us the concept of modules.

In this section we turn our attention to right modules, but left modules can be defined similarly and all results carry over (with the respective modifications of the terms "right" and "left"). Let $\mathcal{F}$ be a function ring with unit $\mathbf{1}$.

Example 4.3.1
Let us provide some examples for right $\mathcal{F}$-modules.

1. Any right ideal in $\mathcal{F}$ is of course a right $\mathcal{F}$-module.

2. The set $\mathcal{M} = \{\mathbf{0}\}$ with right scalar multiplication $\mathbf{0} \star f = \mathbf{0}$ is a right $\mathcal{F}$-module called the trivial right $\mathcal{F}$-module.

3. Given a function ring $\mathcal{F}$ and a natural number k, let $\mathcal{F}^k = \{(f_1, \ldots, f_k) \mid f_i \in \mathcal{F}\}$ be the set of all vectors of length k with coordinates in $\mathcal{F}$. Obviously $\mathcal{F}^k$ is an additive commutative group with respect to ordinary vector addition. Moreover, $\mathcal{F}^k$ is a right $\mathcal{F}$-module with right scalar multiplication $\star : \mathcal{F}^k \times \mathcal{F} \longrightarrow \mathcal{F}^k$ defined by $(f_1, \ldots, f_k) \star f = (f_1 \star f, \ldots, f_k \star f)$. $\diamond$

Definition 4.3.2
A subset of a right $\mathcal{F}$-module $\mathcal{M}$ which is again a right $\mathcal{F}$-module is called a **right submodule** of $\mathcal{M}$. $\diamond$

For example any right ideal of $\mathcal{F}$ is a right submodule of the right $\mathcal{F}$-module $\mathcal{F}^1$. Provided a set of vectors $S \subset \mathcal{M}$ the set $\{\sum_{i=1}^{s} \mathbf{m}_i \star g_i \mid s \in \mathbb{N}, g_i \in \mathcal{F}, \mathbf{m}_i \in S\}$ is a right submodule of $\mathcal{M}$. This set is denoted as $\langle S \rangle_r$ and S is called its generating set. If $\langle S \rangle_r = \mathcal{M}$ then S is a generating set of the right module itself. If S is finite then $\mathcal{M}$ is said to be finitely generated. A generating set is called linearly independent or a basis if for all $s \in \mathbb{N}$, pairwise different $\mathbf{m}_1, \ldots, \mathbf{m}_s \in S$ and $g_1, \ldots, g_s \in \mathcal{F}$, $\sum_{i=1}^{s} \mathbf{m}_i \star g_i = \mathbf{0}$ implies $g_1 = \ldots = g_s = o$. A right $\mathcal{F}$-module is called **free** if it has a basis. The right $\mathcal{F}$-module $\mathcal{F}^k$ is free and one such basis is the set of unit vectors $\mathbf{e}_1 = (\mathbf{1}, o, \ldots, o), \mathbf{e}_2 = (o, \mathbf{1}, o, \ldots, o), \ldots, \mathbf{e}_k = (o, \ldots, o, \mathbf{1})$. Using this basis the elements of $\mathcal{F}^k$ can be written uniquely as $\mathbf{f} = \sum_{i=1}^{k} \mathbf{e}_i \star f_i$ where $\mathbf{f} = (f_1, \ldots, f_k)$. Moreover, $\mathcal{F}^k$ has special properties similar to the special case of $\mathbb{K}[x_1, \ldots, x_n]$ and we will continue to state some of them.

Theorem 4.3.3
Let $\mathcal{F}$ be right Noetherian. Then every right submodule of $\mathcal{F}^k$ is finitely generated.

Proof :
Let $\mathcal{S}$ be a right submodule of $\mathcal{F}^k$. We show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact a right ideal in $\mathcal{F}$ and hence by our hypothesis finitely generated. For $k > 1$ let us look at the set $I = \{f_1 \mid (f_1, \ldots, f_k) \in \mathcal{S}\}$. Then again I is a right ideal in $\mathcal{F}$ and hence finitely generated. Let $\{g_1, \ldots, g_s \mid g_i \in \mathcal{F}\}$ be a generating set of I. Choose $\mathbf{g}_1, \ldots, \mathbf{g}_s \in \mathcal{S}$ such that the first coordinate of $\mathbf{g}_i$ is g_i. Similarly, the set $\{(f_2, \ldots, f_k) \mid (o, f_2, \ldots, f_k) \in \mathcal{S}\}$ is a submodule of $\mathcal{F}^{k-1}$ and hence finitely generated by some set $\{(n_2^i, \ldots, n_k^i), 1 \leq i \leq w\}$. Then the set $\{\mathbf{g}_1, \ldots, \mathbf{g}_s\} \cup \{\mathbf{n}_i = (o, n_2^i, \ldots, n_k^i) \mid 1 \leq i \leq w\}$ is a generating set for $\mathcal{S}$. To see this assume $\mathbf{m} = (m_1, \ldots, m_k) \in \mathcal{S}$. Then $m_1 = \sum_{i=1}^{s} g_i \star h_i$ for some $h_i \in \mathcal{F}$ and $\mathbf{m}' = \mathbf{m} - \sum_{i=1}^{s} \mathbf{g}_i \star h_i \in \mathcal{S}$ with first coordinate o. Hence $\mathbf{m}' = \sum_{i=1}^{w} \mathbf{n}_i \star l_i$ for some $l_i \in \mathcal{F}$ giving rise to

$$\mathbf{m} = \mathbf{m}' + \sum_{i=1}^{s} \mathbf{g}_i \star h_i = \sum_{i=1}^{w} \mathbf{n}_i \star l_i + \sum_{i=1}^{s} \mathbf{g}_i \star h_i.$$

q.e.d.

$\mathcal{F}^k$ is called right Noetherian if and only if all its right submodules are finitely generated.

If $\mathcal{F}$ is a right reduction ring, results on the existence of right Gröbner bases for the right submodules carry over from modifications of the proofs in Section 4.3.

A natural reduction relation using the right reduction relation in $\mathcal{F}$ denoted by $\Longrightarrow$ can be defined using the representation as (module) polynomials with respect to the basis of unit vectors as follows:

Definition 4.3.4
Let $\mathbf{f} = \sum_{i=1}^{k} \mathbf{e}_i \star f_i$, $\mathbf{p} = \sum_{i=1}^{k} \mathbf{e}_i \star p_i \in \mathcal{F}^k$. We say that **f reduces p** to **q** at $\mathbf{e}_s \star p_s$ in one step, denoted by $\mathbf{p} \longrightarrow_{\mathbf{f}} \mathbf{q}$, if

1. $p_j = o$ for $1 \leq j < s$,

2. $p_s \Longrightarrow_{f_s} q_s$,

3. $\mathbf{q} = \mathbf{p} - \sum_{i=1}^{n} \mathbf{f} \cdot d_i$
   $= (0, \ldots, 0, q_s, p_{s+1} - \sum_{i=1}^{n} f_{s+1} \cdot d, \ldots, p_k - \sum_{i=1}^{n} f_k \cdot d)$.

$\diamond$

Notice that item 2 of this definition is dependant on the definition of the reduction relation $\Longrightarrow$ in $\mathcal{F}$. If we assume that the reduction relation is the one specified in Definition 4.2.43 we get $p_s = q_s + f_s \cdot d$, $d \in \mathsf{M}(\mathcal{F})$, but there are other possibilities. Reviewing the introduction of right modules to reduction rings we could substitute 2. by $p_s = q_s + f_s \cdot d$, $d \in \mathcal{F}$ as well (compare Definition 3.4.8).

To show that our reduction relation is terminating we have to extend the ordering from $\mathcal{F}$ to $\mathcal{F}^k$. For two elements $\mathbf{p} = (p_1, \ldots, p_k)$, $\mathbf{q} = (q_1, \ldots, q_k) \in \mathcal{F}^k$ we define $\mathbf{p} \succ \mathbf{q}$ if and only if there exists $1 \leq s \leq k$ such that $p_i = q_i$, $1 \leq i < s$, and $p_s \succ q_s$.

Lemma 4.3.5
Let F be a finite set of module polynomials in $\mathcal{F}^k$.

1. *For $\mathbf{p}, \mathbf{q} \in \mathcal{F}^k$ $\mathbf{p} \longrightarrow_F \mathbf{q}$ implies $\mathbf{p} \succ \mathbf{q}$.*

2. *$\longrightarrow_F$ is Noetherian in case $\Longrightarrow_{F_i}$ is for $1 \leq i \leq k$ and $F_i = \{f_i \mid f = (f_1, \ldots, f_k) \in F\}$.*[43]*.*

Proof :

1. Assuming that the reduction step takes place at $\mathbf{e}_s \star p_s$, by Definition 4.3.4 we know $p_s \Longrightarrow_{f_s} q_s$ and $p_s > q_s$ implying $\mathbf{p} \succ \mathbf{q}$.

2. This follows from 1. and Axiom (A1).

q.e.d.

Definition 4.3.6
A subset B of $\mathcal{F}^k$ is called a **right Gröbner basis** of the right submodule $\mathcal{S} = \langle B \rangle_r$, if $\overset{*}{\longleftrightarrow}_B = \equiv_{\mathcal{S}}$ and $\longrightarrow_B$ is convergent. $\diamond$

For any reduction relation in $\mathcal{F}$ fulfilling the Axioms (A1)–(A3), the following theorem holds.

[43] Notice that $F_i \subseteq \mathcal{F}$.

Theorem 4.3.7
If in $(\mathcal{F}, \Longrightarrow)$ every finitely generated right ideal has a finite right Gröbner basis, then the same holds for finitely generated right submodules in $(\mathcal{F}^k, \longrightarrow)$.

Proof :
Let $\mathcal{S} = \langle\{\mathbf{s}_1, \ldots, \mathbf{s}_n\}\rangle$ be a finitely generated right submodule of $\mathcal{F}^k$. We show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact a finitely generated right ideal in $\mathcal{F}$ and hence by our hypothesis must have a finite right Gröbner basis. For $k > 1$ let us look at the set $I = \{f_1 \mid (f_1, \ldots, f_k) \in \mathcal{S}\}$ which is in fact the right ideal generated by $\{s^i_1 \mid \mathbf{s}_i = (s^i_1, \ldots, s^i_k), 1 \leq i \leq n\}$. Hence I must have a finite right Gröbner basis $H = \{g_1, \ldots, g_s \mid g_i \in \mathcal{F}\}$. Choose $\mathbf{g}_1, \ldots, \mathbf{g}_s \in \mathcal{S}$ such that the first coordinate of $\mathbf{g}_i$ is g_i. Similarly the set $\mathcal{S}' = \{(f_2, \ldots, f_k) \mid (o, f_2, \ldots, f_k) \in \mathcal{S}\}$ is a submodule in $\mathcal{F}^{k-1}$ which by our induction hypothesis then must have a finite right Gröbner basis $\{(\tilde{g}^i_2, \ldots, \tilde{g}^i_k), 1 \leq i \leq w\}$. Then the set $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\} \cup \{\tilde{\mathbf{g}}_i = (o, \tilde{g}^i_2, \ldots, \tilde{g}^i_k) \mid 1 \leq i \leq w\}$ is a right Gröbner basis for $\mathcal{S}$. As shown in the proof of Theorem 4.3.3, G is a generating set for $\mathcal{S}$. It remains to show that G is in fact a right Gröbner basis.
First we have to show $\xleftrightarrow{*}_G = \equiv_{\mathcal{S}}$. By the definition of the reduction relation in $\mathcal{F}^k$ we immediately find $\xleftrightarrow{*}_G \subseteq \equiv_{\mathcal{S}}$. To see the converse let $\mathbf{p} = (p_1, \ldots, p_k) \equiv_{\mathcal{S}} \mathbf{q} = (q_1, \ldots, q_k)$. Then $p_1 \equiv_{\langle\{s^1_i \mid \mathbf{s}_i = (s^i_1, \ldots, s^i_k), 1 \leq i \leq n\}\rangle_r} q_1$ and hence by the definition of G we get $p_1 \xleftrightarrow{*}_{\{g^i_1 \mid \mathbf{g}_i = (g^i_1, \ldots, g^i_k), 1 \leq i \leq s\}} q_1$. But this gives us $\mathbf{p} \xleftrightarrow{*}_H \mathbf{p} + \sum_{i=1}^s \mathbf{g}_i \star r_i = \mathbf{p}' = (q_1, p_2', \ldots, p_k')$, $r_i \in \mathcal{F}$, and we get $(q_1, p_2', \ldots, p_k') \equiv_{\mathcal{S}} (q_1, q_2, \ldots, q_k)$ and hence $(q_1, p_2', \ldots, p_k') - (q_1, q_2, \ldots, q_k) = (o, p_2' - q_2, \ldots, p_k' - q_k) \in \mathcal{S}$ implying $(p_2' - q_2, \ldots, p_k' - q_k) \in \mathcal{S}'$ and $(o, p_2' - q_2, \ldots, p_k' - q_k) = \sum_{i=1}^w \tilde{\mathbf{g}}_i \star \eta_i$ for $\eta_i \in \mathcal{F}$. Hence $(q_1, p_2', \ldots, p_k')$ and $(q_1, q_2, \ldots, q_k) = (q_1, p_2', \ldots, p_k') - (o, p_2' - q_2, \ldots, p_k' - q_k) = (q_1, p_2', \ldots, p_k') - \sum_{i=1}^w \tilde{\mathbf{g}}_i \star \eta_i$ must be joinable by $\{\tilde{\mathbf{g}}_i \mid 1 \leq i \leq w\}$ as the restriction of this set without the first coordinate is a right Gröbner basis of $\mathcal{S}'$.
Since the reduction relation using the finite set G is terminating we only have to show local confluence. Let us assume there are $\mathbf{p}$, $\mathbf{q}_1$, $\mathbf{q}_2 \in \mathcal{F}^k$ such that $\mathbf{p} \longrightarrow_G \mathbf{q}_1$ and $\mathbf{p} \longrightarrow_G \mathbf{q}_2$. Then by the definition of G the first coordinates q^1_1 and q^2_1 are joinable to some element say s by $H = \{g_1, \ldots, g_s\}$ giving rise to the elements $\mathbf{p}_1 = \mathbf{q}_1 + \sum_{i=1}^s \mathbf{g}_i \star h_i$ and $\mathbf{p}_2 = \mathbf{q}_2 + \sum_{i=1}^s \mathbf{g}_i \star \tilde{h}_i$ with first coordinate s. As before, $\mathbf{p}_1 = \mathbf{p}_2 + \sum_{i=1}^w \tilde{\mathbf{g}}_i \star \eta_i$ and hence $\mathbf{p}_1$ and $\mathbf{p}_2$ must be joinable by $\{\tilde{\mathbf{g}}_i \mid 1 \leq i \leq w\}$.

q.e.d.

Now given a right submodule $\mathcal{S}$ of $\mathcal{M}$, we can define $\mathcal{M}/\mathcal{S} = \{\mathbf{f} + \mathcal{S} \mid \mathbf{f} \in \mathcal{M}\}$. Then with addition defined as $(\mathbf{f} + \mathcal{S}) + (\mathbf{g} + \mathcal{S}) = (\mathbf{f} + \mathbf{g}) + \mathcal{S}$ the set $\mathcal{M}/\mathcal{S}$ is an Abelian group and can be turned into a right $\mathcal{F}$-module by the action $(\mathbf{f} + \mathcal{S}) \star g = \mathbf{f} \star g + \mathcal{S}$. $\mathcal{M}/\mathcal{S}$ is called the **right quotient module** of $\mathcal{M}$ by $\mathcal{S}$.

As usual this quotient can be related to homomorphisms. The results carry over from commutative module theory as can be found in [AL94]. Recall that for two right $\mathcal{F}$-modules $\mathcal{M}$ and $\mathcal{N}$, a function $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ is a right $\mathcal{F}$-module homomorphism if

$$\phi(\mathbf{f} + \mathbf{g}) = \phi(\mathbf{f}) + \phi(\mathbf{g}) \text{ for all } \mathbf{f}, \mathbf{g} \in \mathcal{M}$$

and

$$\phi(\mathbf{f}) \star g = \phi(\mathbf{f} \star g) \text{ for all } \mathbf{f} \in \mathcal{M}, g \in \mathcal{F}.$$

The homomorphism is called an **isomorphism** if ϕ is one to one and we then write $\mathcal{M} \cong \mathcal{N}$. Let $\mathcal{S} = \ker(\phi) = \{\mathbf{f} \in \mathcal{M} \mid \phi(\mathbf{f}) = \mathbf{0}\}$. Then $\mathcal{S}$ is a right submodule of $\mathcal{M}$ and $\phi(\mathcal{M})$ is a right submodule of $\mathcal{N}$. Since all are Abelian groups we know $\mathcal{M}/\mathcal{S} \cong \phi(\mathcal{M})$ under the mapping $\mathcal{M}/\mathcal{S} \longrightarrow \phi(\mathcal{M})$ with $\mathbf{f} + \mathcal{S} \mapsto \phi(\mathbf{f})$ which is in fact an isomorphism. All right submodules of the quotient $\mathcal{M}/\mathcal{S}$ are of the form $\mathcal{L}/\mathcal{S}$ where $\mathcal{L}$ is a right submodule of $\mathcal{M}$ containing $\mathcal{S}$.

We can even show that every finitely generated right $\mathcal{F}$-module is of a special form.

Lemma 4.3.8
Every finitely generated right $\mathcal{F}$-module $\mathcal{M}$ is isomorphic to $\mathcal{F}^k/\mathcal{N}$ for some $k \in \mathbb{N}$ and some right submodule $\mathcal{N}$ of $\mathcal{F}^k$.

Proof :
Let $\mathcal{M}$ be a finitely generated right $\mathcal{F}$-module with generating set $\mathbf{f}_1, \ldots \mathbf{f}_k \in \mathcal{M}$. Consider the mapping $\phi : \mathcal{F}^k \longrightarrow \mathcal{M}$ defined by $\phi(g_1, \ldots, g_k) = \sum_{i=1}^{k} \mathbf{f}_i \star g_i$. Then ϕ is an $\mathcal{F}$-module homomorphism with image $\mathcal{M}$. Let $\mathcal{N}$ be the kernel of ϕ, then the First Isomorphism Theorem for modules yields our claim. Note that ϕ is uniquely defined by specifying the image of each unit vector $\mathbf{e}_1, \ldots, \mathbf{e}_k$, namely by $\phi(\mathbf{e}_i) = \mathbf{f}_i$.

q.e.d.

Now, there are two ways to give a finitely generated right $\mathcal{F}$-module $\mathcal{M} \subset \mathcal{F}^k$. One is to be given explicit $\mathbf{f}_1, \ldots \mathbf{f}_t \in \mathcal{F}^k$ such that $\mathcal{M} = \langle\{\mathbf{f}_1, \ldots \mathbf{f}_s\}\rangle_r$. The other way is to give a right submodule $\mathcal{N} = \langle\{\mathbf{g}_1, \ldots \mathbf{g}_s\}\rangle_r$ for explicit $\mathbf{g}_1, \ldots \mathbf{g}_s \in \mathcal{F}^k$ such that $\mathcal{M} \cong \mathcal{F}^k/\mathcal{N}$. This is called a **presentation** of $\mathcal{M}$.

Presentations are chosen when studying right ideals of $\mathcal{F}$ as right $\mathcal{F}$-modules. To see how this is done let $\mathfrak{i}$ be the right ideal generated by $\{f_1, \ldots, f_k\}$ in $\mathcal{F}$. Let us consider the right $\mathcal{F}$-module homomorphism defined as a mapping $\phi : \mathcal{F}^k \longrightarrow \mathfrak{i}$ with $\phi(g_1, \ldots, g_k) = \sum_{i=1}^{k} f_i \star g_i$. Then $\mathfrak{i} \cong \mathcal{F}^k/\ker(\phi)$ as $\mathcal{F}$-modules. $\ker(\phi)$ is called the **right syzygy** of $\{f_1, \ldots, f_k\}$ denoted by $\mathrm{Syz}(f_1, \ldots, f_k)$. In fact $\mathrm{Syz}(f_1, \ldots, f_k)$ is the set of all solutions of the linear equation $f_1X_1 + \ldots + f_kX_k = o$ in $\mathcal{F}$. Syzygies play an important role in Gröbner basis theory for ordinary polynomial rings.

4.4 Ideals and Standard Representations

A subset $\mathfrak{i} \subseteq \mathcal{F}$ is called a (two-sided) **ideal**, if

1. $o \in \mathfrak{i}$,
2. for $f, g \in \mathfrak{i}$ we have $f \oplus g \in \mathfrak{i}$, and
3. for $f \in \mathfrak{i}$, $g, h \in \mathcal{F}$ we have $g \star f \star h \in \mathfrak{i}$.

Ideals can also be specified in terms of a generating set. For $F \subseteq \mathcal{F}\backslash\{o\}$ let $\mathsf{ideal}(F) = \{\sum_{i=1}^{n} g_i \star f_i \star h_i \mid f_i \in F, g_i, h_i \in \mathcal{F}, n \in \mathbb{N}\} = \{\sum_{i=1}^{m} m_i \star f_i \star l_i \mid f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}\}$. These generated sets are in fact subsets of $\mathcal{F}$ since for $f, g \in \mathcal{F}$ we have that $f \star g$ as well as $f \oplus g$ are again elements of $\mathcal{F}$, and it is easily checked that they are in fact ideals:

1. $o \in \mathsf{ideal}(F)$ since o can be written as the empty sum.
2. For two elements $\sum_{i=1}^{n} g_i \star f_i \star h_i$ and $\sum_{i=1}^{m} \tilde{g}_i \star \tilde{f}_i \star \tilde{h}_i$ in $\mathsf{ideal}(F)$, the sum $\sum_{i=1}^{n} g_i \star f_i \star h_i \oplus \sum_{i=1}^{m} \tilde{g}_i \star \tilde{f}_i \star \tilde{h}_i$ is again an element in $\mathsf{ideal}(F)$.
3. For an element $\sum_{i=1}^{n} g_i \star f_i \star h_i$ in $\mathsf{ideal}_r(F)$ and two polynomials g, h in $\mathcal{F}$, the product $g \star (\sum_{i=1}^{n} g_i \star f_i \star h_i) \star h = \sum_{i=1}^{n} (g \star g_i) \star f_i \star (h_i \star h)$ is again an element in $\mathsf{ideal}(F)$.

Given an ideal $\mathfrak{i} \subseteq \mathcal{F}$ we call a set $F \subseteq \mathcal{F}\backslash\{o\}$ a basis of $\mathfrak{i}$ if $\mathfrak{i} = \mathsf{ideal}(F)$. Then every element $g \in \mathsf{ideal}(F)\backslash\{o\}$ can have different representations of the form

$$g = \sum_{i=1}^{n} g_i \star f_i \star h_i, f_i \in F, g_i, h_i \in \mathcal{F}, n \in \mathbb{N}.$$

Notice that the f_i occurring in this sum are not necessarily different. The distributivity law in $\mathcal{F}$ allows to convert such a representation into one of the form

$$g = \sum_{j=1}^{m} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}.$$

Again special representations can be distinguished in order to characterize special ideal bases. An ordering on $\mathcal{F}$ is used to define appropriate standard representations. As in the case of right ideals we will first look at generalizations of standard representations for the case of function rings over fields.

4.4.1 The Special Case of Function Rings over Fields

Let $\mathcal{F}_{\mathbb{K}}$ be a function ring over a field $\mathbb{K}$. We first look at an analogon to Definition 4.2.7

Definition 4.4.1
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and g a non-zero polynomial in $\mathsf{ideal}(F)$. A representations of the form

$$g = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$$

where additionally $\mathsf{HT}(g) \succeq \mathsf{HT}(m_i \star f_i \star l_i)$ holds for $1 \leq i \leq n$ is called a **standard representation** of g in terms of F. If every $g \in \mathsf{ideal}(F) \backslash \{o\}$ has such a representation in terms of F, then F is called a **standard basis** of $\mathsf{ideal}(F)$. $\diamond$

Notice that since we assume $f \cdot \alpha = \alpha \cdot f$, we can also substitute the monomials l_i by terms $w_i \in \mathcal{T}$, i.e. study representations of the form

$$g = \sum_{i=1}^{n} m_i \star f_i \star w_i, f_i \in F, m_i \in \mathsf{M}(\mathcal{F}), w_i \in \mathcal{T}, n \in \mathbb{N}.$$

We will use this additional information in some proofs later on.

As with right standard representations, in order to change an arbitrary representation of an ideal element into a standard representation we have to deal with special sums of polynomials. We get the following analogon to Definition 4.2.8.

Definition 4.4.2
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and t an element in $\mathcal{T}$. Then we define a set $\mathcal{C}(F,t)$ to contain all tuples of the form $(t, f_1, \ldots, f_k, m_1, \ldots, m_k, l_1, \ldots, l_k)$, $k \in \mathbb{N}$, $f_1, \ldots, f_k \in F$, $m_1, \ldots, m_k, l_1, \ldots, l_k \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that

1. $\mathsf{HT}(m_i \star f_i \star l_i) = t$, $1 \leq i \leq k$, and
2. $\sum_{i=1}^{k} \mathsf{HM}(m_i \star f_i \star l_i) = 0$.

We set $\mathcal{C}(F) = \bigcup_{t \in \mathcal{T}} \mathcal{C}(F,t)$. $\diamond$

Notice that this definition is motivated by the definition of syzygies of head monomials in commutative polynomial rings over rings. We can characterize standard bases using this concept (compare Theorem 4.2.9).

Theorem 4.4.3
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a standard basis of $\mathsf{ideal}(F)$ *if and only if for every tuple $(t, f_1, \ldots, f_k, m_1, \ldots, m_k, l_1, \ldots, l_k)$ in $\mathcal{C}(F)$ the polynomial $\sum_{i=1}^{k} m_i \star f_i \star l_i$ (i.e. the element in $\mathcal{F}_{\mathbb{K}}$ corresponding to this sum) has a standard representation with respect to F.*

Proof :
In case F is a standard basis since the polynomials related to the tuples are all elements of $\mathsf{ideal}(F)$ they must have standard representations with respect to F. To prove the converse, it remains to show that every element in $\mathsf{ideal}(F)$ has a standard representation with respect to F. Hence, let $g = \sum_{j=1}^{m} m_j \star f_j \star l_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}(F)$ such that $f_j \in F$, $m_j, l_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$, $m \in \mathbb{N}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(m_j \star f_j \star l_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $m_j \star f_j \star l_j$ with head term t. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that this representation is already a standard one. Else we proceed by induction on t. Without loss of generality let $f_1, \ldots, f_K$ be the polynomials in the corresponding representation such that $t = \mathsf{HT}(m_j \star f_j \star l_j)$, $1 \leq j \leq K$. Then the tuple $(t, f_1, \ldots, f_K, m_1, \ldots, m_K, l_1, \ldots, l_K)$ is in $\mathcal{C}(F)$ and let $h = \sum_{j=1}^{K} m_j \star f_j \star l_j$. We will now change our representation of g in such a way that for the new representation of g we have a smaller maximal term. Let us assume h is not o[44]. By our assumption, h has a standard representation with respect to F, say $\sum_{i=1}^{n} \tilde{m}_i \star \tilde{f}_i \star \tilde{l}_i$, where $\tilde{f}_i \in F$, and $\tilde{m}_i, \tilde{l}_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$. This gives us:

$$\begin{aligned} g &= \sum_{j=1}^{K} m_j \star f_j \star l_j + \sum_{j=K+1}^{m} m_j \star f_j \star l_j \\ &= \sum_{i=1}^{n} \tilde{m}_i \star \tilde{f}_i \star \tilde{l}_i + \sum_{j=K+1}^{m} m_j \star f_j \star l_j \end{aligned}$$

which is a representation of g where the maximal term of the involved monomial multiples is decreased.

q.e.d.

Weak Gröbner bases can be defined as in Definition 4.2.10. Since the ordering $\succeq$ and the multiplication $\star$ in general are not compatible, instead of considering multiples of head terms of the generating set F we look at head terms of monomial multiples of polynomials in F.

[44] In case $h = o$, just substitute the empty sum for the representation of h in the equations below.

Definition 4.4.4
A subset F of $\mathcal{F}_{\mathbb{K}}\backslash\{o\}$ is called a **weak Gröbner basis** of $\mathsf{ideal}(F)$ if $\mathsf{HT}(\mathsf{ideal}(F)\backslash\{o\}) = \mathsf{HT}(\{m \star f \star l \mid f \in F, m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\}\backslash\{o\})$. $\diamond$

In the next lemma we show that in fact both characterizations of special bases, standard bases and weak Gröbner bases, coincide as in the case of polynomial rings over fields (compare Lemma 4.2.11).

Lemma 4.4.5
Let F be a subset of $\mathcal{F}_{\mathbb{K}}\backslash\{o\}$. Then F is a standard basis if and only if it is a weak Gröbner basis.

Proof :
Let us first assume that F is a standard basis, i.e., every polynomial g in $\mathsf{ideal}(F)$ has a standard representation with respect to F. In case $g \neq o$ this implies the existence of a polynomial $f \in F$ and monomials $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(g) = \mathsf{HT}(m \star f \star l)$. Hence $\mathsf{HT}(g) \in \mathsf{HT}(\{m \star f \star l \mid m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F\}\backslash\{o\})$. As the converse, namely $\mathsf{HT}(\{m \star f \star l \mid m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F\}\backslash\{o\}) \subseteq \mathsf{HT}(\mathsf{ideal}(F)\backslash\{o\})$ trivially holds, F then is a weak Gröbner basis.
Now suppose that F is a weak Gröbner basis and again let $g \in \mathsf{ideal}(F)$. We have to show that g has a standard representation with respect to F. This will be done by induction on $\mathsf{HT}(g)$. In case $g = o$ the empty sum is our required standard representation. Hence let us assume $g \neq o$. Since then $\mathsf{HT}(g) \in \mathsf{HT}(\mathsf{ideal}(F)\backslash\{o\})$ by the definition of weak Gröbner bases we know there exists a polynomial $f \in F$ and monomials $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(g) = \mathsf{HT}(m \star f \star l)$. Then there exists a monomial $\tilde{m} \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HM}(g) = \mathsf{HM}(\tilde{m} \star f \star l)$, namely[45] $\tilde{m} = (\mathsf{HC}(g) \cdot \mathsf{HC}(m \star f \star l)^{-1}) \cdot m)$. Let $g_1 = g - \tilde{m} \star f \star l$. Then $\mathsf{HT}(g) \succ \mathsf{HT}(g_1)$ implies the existence of a standard representation for g_1 which can be added to the multiple $\tilde{m} \star f \star l$ to give the desired standard representation of g.

q.e.d.

Inspecting this proof closer we get the following corollary (compare Corollary 4.2.12).

Corollary 4.4.6
Let a subset F of $\mathcal{F}_{\mathbb{K}}\backslash\{o\}$ be a weak Gröbner basis. Then every $g \in \mathsf{ideal}(F)$ has a standard representation in terms of F of the form $g = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$ such that $\mathsf{HM}(g) = \mathsf{HM}(m_1 \star f_1 \star l_1)$ and $\mathsf{HT}(m_1 \star f_1 \star l_1) \succ \mathsf{HT}(m_2 \star f_2 \star l_2) \succ \ldots \succ \mathsf{HT}(m_n \star f_n \star l_n)$.

[45] Notice that this step requires that we can view $\mathcal{F}_{\mathbb{K}}$ as a vector space. In order to get a similar result without introducing vector spaces we would have to use a different definition of weak Gröbner bases. E.g. requiring that $\mathsf{HM}(\mathsf{ideal}(F)\backslash\{o\}) = \mathsf{HM}(\{m \star f \star l \mid f \in F, m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\}\backslash\{o\}\})$ would be a possibility. However, then no localization of critical situations to head terms is possible, which is *the* advantage of having a field as coefficient domain.

Notice that we hence get stronger representations as specified in Definition 4.4.1 for the case that the set F is a weak Gröbner basis or a standard basis.

In order to proceed as before in the case of one-sided ideals we have to extend our restriction of the ordering $\succeq$ on $\mathcal{F}$ to cope with two-sided multiplication similar to Definition 4.2.13.

Definition 4.4.7
We will call an ordering $\geq$ on $\mathcal{T}$ a **reductive restriction** of the ordering $\succeq$ or simply **reductive**, if the following hold:

1. $t \geq s$ implies $t \succeq s$ for $t, s \in \mathcal{T}$.
2. $\geq$ is a partial well-founded ordering on $\mathcal{T}$ which is compatible with multiplication $\star$ in the following sense: if for $t, t_1, t_2, w_1, w_2 \in \mathcal{T}$ $t_2 \geq t_1$, $t_1 \succ t$ and $t_2 = \mathsf{HT}(w_1 \star t_1 \star w_2)$ hold, then $t_2 \succ \mathsf{HT}(w_1 \star t \star w_2)$. $\diamond$

Again we can distiguish special "divisors" of monomials: For $m_1, m_2 \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we call m_1 a **(stable) divisor** of m_2 if and only if $\mathsf{HT}(m_2) \geq \mathsf{HT}(m_1)$ and there exist $l_1, l_2 \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $m_2 = \mathsf{HM}(l_1 \star m_1 \star l_2)$. We then call l_1, l_2 **stable multipliers** of m_1. The intention is that for all terms t with $\mathsf{HT}(m_1) \succ t$ we then can conclude $\mathsf{HT}(m_2) \succ \mathsf{HT}(l_1 \star t \star l_2)$. Reduction relations based on this divisibility of terms will again have the stability properties we desire. In the commutative polynomial ring we can state a reductive restriction of any term ordering by $t \geq s$ for two terms t and s if and only if s divides t as a term. In the non-commutative polynomial ring we can state a reductive restriction of any term ordering by $t \geq s$ for two terms t and s if and only if s is a subword of t. Let us continue with an algebraic consequence related to this reductive ordering by distinguishing special standard representations as we have done in Definition 4.2.15.

Definition 4.4.8
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and g a non-zero polynomial in $\mathsf{ideal}(F)$. A representation of the form

$$g = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(m_i \star f_i \star l_i) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$ for some $k \geq 1$, and $\mathsf{HT}(g) \succ \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i)$ for $k < i \leq n$ is called a **reductive standard representation** in terms of F. $\diamond$

Again the empty sum is taken as reductive standard representation of o.

In case we have $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$ the condition can be rephrased as $\mathsf{HT}(g) = m_i \star f_i \star l_i = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$.

Definition 4.4.9
A set $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ is called a **reductive standard basis** (with respect to the reductive ordering $\geq$) of $\mathsf{ideal}(F)$ if every polynomial $f \in \mathsf{ideal}(F)$ has a reductive standard representation in terms of F. $\diamond$

Again, in order to change an arbitrary representation into one fulfilling our additional condition of Definition 4.4.8 we have to deal with special sums of polynomials.

Definition 4.4.10
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and t an element in $\mathcal{T}$. Then we define the **critical set** $\mathcal{C}_r(t, F)$ to contain all tuples of the form $(t, f_1, \ldots, f_k, m_1, \ldots, m_k, l_1, \ldots, l_k)$, $k \in \mathbb{N}$, $f_1, \ldots, f_k \in F$[46], $m_1, \ldots, m_k, l_1, \ldots, l_k \in \mathsf{M}(\mathcal{F})$ such that

1. $\mathsf{HT}(m_i \star f_i \star l_i) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = t$, $1 \leq i \leq k$,
2. $\mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$, and
3. $\sum_{i=1}^{k} \mathsf{HM}(m_i \star f_i \star l_i) = o$.

We set $\mathcal{C}_r(F) = \bigcup_{t \in \mathcal{T}} \mathcal{C}_r(t, F)$. $\diamond$

Unfortunately, as in the case of right reductive standard bases, these critical situations will not be sufficient to characterize reductive standard bases (compare again Example 4.2.18). But we can give an analogon to Theorem 4.2.19.

Theorem 4.4.11
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a reductive standard basis of $\mathsf{ideal}(F)$ if and only if

1. *for every $f \in F$ and every $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ the multiple $m \star f \star l$ has a reductive standard representation in terms of F,*
2. *for every tuple $(t, f_1, \ldots, f_k, m_1, \ldots, m_k, l_1, \ldots, l_k)$ in $\mathcal{C}_r(F)$ the polynomial $\sum_{i=1}^{k} m_i \star f_i \star l_i$ (i.e., the element in $\mathcal{F}$ corresponding to this sum) has a reductive standard representation with respect to F.*

Proof :
In case F is a reductive standard basis, since these polynomials are all elements of $\mathsf{ideal}(F)$, they must have reductive standard representations with respect to F.

[46] As in the case of commutative polynomials, $f_1, \ldots, f_k$ are not necessarily different polynomials from F.

To prove the converse, it remains to show that every element in $\mathsf{ideal}(F)$ has a reductive standard representation with respect to F. Hence, let $g = \sum_{j=1}^{m} m_j \star f_j \star l_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}(F)$ such that $f_j \in F$, $m_j, l_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$, $m \in \mathbb{N}$. By our first statement every such monomial multiple $m_j \star f_j \star l_j$ has a reductive standard representation in terms of F and we can assume that all multiples are replaced by them. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(m_j \star f_j \star l_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $m_j \star f_j \star l_j$ with head term t. Then for each monomial multiple $m_j \star f_j \star l_j$ with $\mathsf{HT}(m_j \star f_j \star l_j) = t$ we know that $\mathsf{HT}(m_j \star f_j \star l_j) = \mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j) \geq \mathsf{HT}(f_j)$ holds. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that this representation is already a reductive standard one. Else we proceed by induction on t. Without loss of generality let $f_1, \ldots, f_K$ be the polynomials in the corresponding representation such that $t = \mathsf{HT}(m_i \star f_i \star l_i)$, $1 \leq i \leq K$. Then the tuple $(t, f_1, \ldots, f_K, m_1, \ldots, m_K, l_1, \ldots, l_K)$ is in $\mathcal{C}_r(F)$ and let $h = \sum_{i=1}^{K} m_i \star f_i \star l_i$. We will now change our representation of g in such a way that for the new representation of g we have a smaller maximal term. Let us assume h is not o[47]. By our assumption, h has a reductive standard representation with respect to F, say $\sum_{j=1}^{n} \tilde{m}_j \star h_j \star \tilde{l}_j$, where $h_j \in F$, and $\tilde{m}_j, \tilde{l}_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$ as $\sum_{i=1}^{K} \mathsf{HM}(m_i \star f_i \star l_i) = o$. This gives us:

$$
\begin{aligned}
g &= \sum_{i=1}^{K} m_i \star f_i \star l_i + \sum_{i=K+1}^{m} m_i \star f_i \star l_i \\
&= \sum_{j=1}^{n} \tilde{m}_j \star h_j \star \tilde{l}_j + \sum_{i=K+1}^{m} m_i \star f_i \star l_i
\end{aligned}
$$

which is a representation of g where the maximal term is smaller than t.

q.e.d.

An algebraic characterization of weak Gröbner bases again can be given by a property of head monomials based on stable divisors of terms (compare Definition 4.2.20).

Definition 4.4.12
A set $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ is called a **weak reductive Gröbner basis** of $\mathsf{ideal}(F)$ (with respect to the reductive ordering $\geq$) if $\mathsf{HT}(\mathsf{ideal}(F)\backslash\{o\}) = \mathsf{HT}(\{m \star f \star l \mid f \in F, m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), \mathsf{HT}(m \star f \star l) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) \geq \mathsf{HT}(f)\}\backslash\{o\})$. $\diamond$

We will later on see that an analogon of the Translation Lemma holds for the reduction relation related to reductive standard representations. Hence weak

[47] In case $h = o$, just substitute the empty sum for the representation of h in the equations below.

reductive Gröbner bases and Gröbner bases coincide. This is again due to the fact that the coefficient domain is a field and will not carry over for reduction rings as coefficient domains.

The next lemma states that in fact both characterizations of special bases provided so far coincide.

Lemma 4.4.13
Let F be a subset of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a reductive standard basis if and only if it is a weak reductive Gröbner basis.

Proof :
Let us first assume that F is a reductive standard basis, i.e., every polynomial g in $\mathsf{ideal}(F)$ has a reductive standard representation with respect to F. In case $g \neq o$ this implies the existence of a polynomial $f \in F$ and monomials $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(g) = \mathsf{HT}(m \star f \star l) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) \geq \mathsf{HT}(f)$. Hence $\mathsf{HT}(g) \in \mathsf{HT}(\{m \star f \star l \mid m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F, \mathsf{HT}(m \star f \star l) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) \geq \mathsf{HT}(f)\} \backslash \{o\})$. As the converse, namely $\mathsf{HT}(\{m \star f \star l \mid m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), f \in F, \mathsf{HT}(m \star f \star l) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) \geq \mathsf{HT}(f)\} \backslash \{o\}) \subseteq \mathsf{HT}(\mathsf{ideal}(F) \backslash \{o\})$ trivially holds, F is a weak reductive Gröbner basis.
Now suppose that F is a weak reductive Gröbner basis and again let $g \in \mathsf{ideal}(F)$. We have to show that g has a reductive standard representation with respect to F. This will be done by induction on $\mathsf{HT}(g)$. In case $g = o$ the empty sum is our required reductive standard representation. Hence let us assume $g \neq o$. Since then $\mathsf{HT}(g) \in \mathsf{HT}(\mathsf{ideal}(F) \backslash \{o\})$ by the definition of weak reductive Gröbner bases we know there exists a polynomial $f \in F$ and monomials $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(m \star f \star l) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) \geq \mathsf{HT}(f)$ and there exists $\alpha \in \mathbb{K}$ such that $\mathsf{HC}(g) = \mathsf{HC}(m \star f \star l) \cdot \alpha$, i.e., $\mathsf{HM}(g) = \mathsf{HM}(m \star f \star l \cdot \alpha)$. Let $g_1 = g - m \star f \star l \cdot \alpha$. Then $\mathsf{HT}(g) \succ \mathsf{HT}(g_1)$ implies the existence of a reductive standard representation for g_1 which can be added to the multiple $m \star f \star l \cdot \alpha$ to give the desired reductive standard representation of g.

q.e.d.

A close inspection of this proof reveals that in fact we can provide a stronger condition for standard representations in terms of weak reductive Gröbner bases.

Corollary 4.4.14
Let a subset F of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$ be a weak reductive Gröbner basis. Every $g \in \mathsf{ideal}(F)$ has a reductive standard representation in terms of F of the form $g = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}), n \in \mathbb{N}$ such that $\mathsf{HT}(g) = \mathsf{HT}(m_1 \star f_1 \star l_1) \succ \mathsf{HT}(m_2 \star f_2 \star l_2) \succ \ldots \succ \mathsf{HT}(m_n \star f_n \star l_n)$ and $\mathsf{HT}(m_i \star f_i \star l_i) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) \geq \mathsf{HT}(f_i)$ for all $1 \leq i \leq n$.

The importance of Gröbner bases in commutative polynomial rings stems from the fact that they can be characterized by special polynomials, the so-called s-polynomials. This characterization can be combined with a reduction relation to an algorithm which computes finite Gröbner bases.

We provide a first characterization for our function ring over the field $\mathbb{K}$. Here critical situations lead to s-polynomials as in the original case and can be identified by studying term multiples of polynomials. Let p and q be two non-zero polynomials in $\mathcal{F}_{\mathbb{K}}$. We are interested in terms t, u_1, u_2, v_1, v_2 such that $\mathsf{HT}(u_1 \star p \star v_1) = \mathsf{HT}(u_1 \star \mathsf{HT}(p) \star v_1) = t = \mathsf{HT}(u_2 \star q \star v_2) = \mathsf{HT}(u_2 \star \mathsf{HT}(q) \star v_2)$ and $\mathsf{HT}(p) \leq t$, $\mathsf{HT}(q) \leq t$. Let $\mathcal{C}_s(p,q)$ (this is a specialization of Definition 4.4.2) be the set containing all such tuples (t, u_1, u_2, v_1, v_2) (as a short hand for $(t, p, q, u_1, u_2, v_1, v_2)$. We call the polynomial $\mathsf{HC}(u_1 \star p \star v_1)^{-1} \cdot u_1 \star p \star v_1 - \mathsf{HC}(u_2 \star q \star v_2)^{-1} \cdot u_2 \star q \star v_2 = \mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2)$ the **s-polynomial** of p and q related to the tuple (t, u_1, u_2, v_1, v_2).

Again these critical situations are not sufficient to characterize weak Gröbner bases (compare Example 4.2.18) and additionally we have to test monomial multiples of polynomials now from both sides.

Theorem 4.4.15
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a weak Gröbner basis of $\mathsf{ideal}(F)$ *if and only if*

1. *for all f in F and for all m, l in $\mathsf{M}(\mathcal{F}_{\mathbb{K}})$ the multiple $m \star f \star l$ has a reductive standard representation in terms of F, and*
2. *for all p and q in F and every tuple (t, u_1, u_2, v_1, v_2) in $\mathcal{C}_s(p,q)$ the respective s-polynomial* $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2)$ *has a reductive standard representation in terms of F.*

Proof :
In case F is a weak Gröbner basis it is also a reductive standard basis, and since the multiples $m \star f \star l$ as well as the respective s-polynomials are all elements of $\mathsf{ideal}(F)$ they must have reductive standard representations in terms of F.
The converse will be proven by showing that every element in $\mathsf{ideal}(F)$ has a reductive standard representation in terms of F. Now, let $g = \sum_{j=1}^{m} \alpha_j \cdot v_j \star f_j \star w_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}(F)$ such that $\alpha_j \in \mathbb{K}^*$, $f_j \in F$, and $v_j, w_j \in \mathcal{T}$. Since by our first assumption every multiple $v_j \star f_j \star w_j$ in this sum has a reductive standard representation we can assume that $\mathsf{HT}(v_j \star \mathsf{HT}(f_j) \star w_j) = \mathsf{HT}(v_j \star f_j \star w_j) \geq \mathsf{HT}(f_j)$ holds.
Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(v_j \star f_j \star w_j) \mid 1 \leq j \leq m\}$ and K as the number of polynomials $v_j \star f_j \star w_j$ with head term t. Without loss of generality we can assume that the polynomial multiples with head term t are just $v_1 \star f_1 \star w_1, \ldots, v_K \star f_K \star w_K$.

We proceed by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or $(t' = t$ and $K' < K)$[48].

Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and by our assumptions our representation is already of the required form. Hence let us assume $K > 1$. Then for the two polynomials f_1, f_2 in the corresponding representation[49] such that $t = \mathsf{HT}(v_1 \star \mathsf{HT}(f_1) \star w_1) = \mathsf{HT}(v_1 \star f_1 \star w_1) = \mathsf{HT}(v_2 \star f_2 \star w_2) = \mathsf{HT}(v_2 \star \mathsf{HT}(f_2) \star w_2)$ and $t \geq \mathsf{HT}(f_1)$, $t \geq \mathsf{HT}(f_2)$. Then the tuple (t, v_1, v_2, w_1, w_2) is in $\mathcal{C}_s(f_1, f_2)$ and we have an s-polynomial $h = \mathsf{HC}(v_1 \star f_1 \star w_1)^{-1} \cdot v_1 \star f_1 \star w_1 - \mathsf{HC}(v_2 \star f_2 \star w_2)^{-1} \cdot v_2 \star f_2 \star w_2$ corresponding to this tuple. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume the s-polynomial is not o[50]. By our assumption, h has a reductive standard representation in terms of F, say $\sum_{i=1}^{n} \tilde{\alpha}_i \cdot \tilde{v}_i \star \tilde{f}_i \star \tilde{w}_i$, where $\tilde{\alpha}_i \in \mathbb{K}^*$, $\tilde{f}_i \in F$, and $\tilde{v}_i, \tilde{w}_i \in \mathcal{T}$ and all terms occurring in this sum are bounded by $t \succ \mathsf{HT}(h)$. This gives us:

$$\begin{aligned}
& \alpha_1 \cdot v_1 \star f_1 \star w_1 + \alpha_2 \cdot v_2 \star f_2 \star w_2 \\
= \; & \alpha_1 \cdot v_1 \star f_1 \star w_1 + \underbrace{\alpha'_2 \cdot \beta_1 \cdot v_1 \star f_1 \star w_1 - \alpha'_2 \cdot \beta_1 \cdot v_1 \star f_1 \star w_1}_{=0} \\
& + \underbrace{\alpha'_2 \cdot \beta_2}_{\alpha_2} \cdot v_2 \star f_2 \star w_2 \\
= \; & (\alpha_1 + \alpha'_2 \cdot \beta_1) \cdot v_1 \star f_1 \star w_1 - \alpha'_2 \cdot \underbrace{(\beta_1 \cdot v_1 \star f_1 \star w_1 - \beta_2 \cdot v_2 \star f_2 \star w_2)}_{=h} \\
= \; & (\alpha_1 + \alpha'_2 \cdot \beta_1) \cdot v_1 \star f_1 \star w_1 - \alpha'_2 \cdot (\sum_{i=1}^{n} \tilde{\alpha}_i \cdot \tilde{v}_i \star \tilde{f}_i \star \tilde{w}_i) \qquad (4.6)
\end{aligned}$$

where $\beta_1 = \mathsf{HC}(v_1 \star f_1 \star w_1)^{-1}$, $\beta_2 = \mathsf{HC}(v_2 \star f_2 \star w_2)^{-1}$ and $\alpha'_2 \cdot \beta_2 = \alpha_2$. Substituting (4.6) in the representation of g gives rise to a smaller one.

q.e.d.

Notice that both test sets in this characterization in general cannot be described in a finitary manner, i.e., provide no finite test for the property of being a Gröbner basis.

A problem which is related to the fact that the ordering $\succeq$ and the multiplication $\star$ in general are not compatible is that an important property fulfilled for

[48] Note that this ordering is well-founded since $\succ$ is well-founded on $\mathcal{T}$ and $K \in \mathbb{N}$.

[49] Not necessarily $f_2 \neq f_1$.

[50] In case $h = o$, just substitute the empty sum for the reductive representation of h in the equations below.

representations of polynomials in commutative polynomial rings no longer holds: As in the case of right ideals the existence of a standard representation for some polynomial $f \in \mathcal{F}_{\mathbb{K}}$ no longer implies the existence of one for a multiple $m \star f \star l$ where $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. However there are restrictions where this implication will hold (compare Lemma 4.2.26).

Lemma 4.4.16
Let F be a subset of $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$ and p a non-zero polynomial in $\mathcal{F}_{\mathbb{K}}$. If p has a reductive standard representation with respect to F and m, l are monomials such that $\mathsf{HT}(m \star p \star l) = \mathsf{HT}(m \star \mathsf{HT}(p) \star l) \geq \mathsf{HT}(p)$, then the multiple $m \star p \star l$ again has a reductive standard representation with respect to F.

Proof :
Let $p = \sum_{i=1}^{n} m_i \star f_i \star l_i$ with $n \in \mathbb{N}$, $f_i \in F$, $m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ be a reductive standard representation of p in terms of F, i.e., $\mathsf{HT}(p) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$ and $\mathsf{HT}(p) \succeq \mathsf{HT}(m_i \star f_i \star l_i)$ for all $k+1 \leq i \leq n$.
Let us first analyze the multiple $m \star m_j \star f_j \star l_j \star l$.
Let $\mathsf{T}(m_j \star f_j \star l_j) = \{s_1, \ldots, s_k\}$ with $s_1 \succ s_i$, $2 \leq i \leq l$, i.e. $s_1 = \mathsf{HT}(m_j \star f_j \star l_j) = \mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j) = \mathsf{HT}(p)$. Hence $\mathsf{HT}(m \star \mathsf{HT}(p) \star l) = \mathsf{HT}(m \star s_1 \star l) \geq \mathsf{HT}(p) = s_1$ and as $s_1 \succ s_i$, $2 \leq i \leq l$, by Definition 4.4.7 we can conclude $\mathsf{HT}(m \star \mathsf{HT}(p) \star l) = \mathsf{HT}(m \star s_1 \star l) \succ m \star s_i \star l \succeq \mathsf{HT}(m \star s_i \star l)$ for $2 \leq i \leq l$. This implies $\mathsf{HT}(m \star \mathsf{HT}(m_j \star f_j \star l_j) \star l) = \mathsf{HT}(m \star m_j \star f_j \star l_j \star l)$. Hence we get

$$\begin{aligned}
\mathsf{HT}(p \star m) &= \mathsf{HT}(m \star \mathsf{HT}(p) \star l) \\
&= \mathsf{HT}(m \star \mathsf{HT}(m_j \star f_j \star l_j) \star l), \text{ as } \mathsf{HT}(p) = \mathsf{HT}(m_j \star f_j \star l_j) \\
&= \mathsf{HT}(m \star m_j \star f_j \star l_j \star l)
\end{aligned}$$

and since $\mathsf{HT}(m \star p \star l) \geq \mathsf{HT}(p) \geq \mathsf{HT}(f_j)$ we can conclude $\mathsf{HT}(m \star m_j \star f_j \star l_j \star l) \geq \mathsf{HT}(f_j)$. It remains to show that $m \star m_j \star f_j \star l_j \star l$ has a reductive standard representation in terms of F. First we show that $\mathsf{HT}(m \star m_j \star \mathsf{HT}(f_j) \star l_j \star l) \geq \mathsf{HT}(f_j)$. We know $m_j \star \mathsf{HT}(f_j) \star l_j \succeq \mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j) = \mathsf{HT}(m_j \star f_j \star l_j)$[51] and hence $\mathsf{HT}(m \star m_j \star \mathsf{HT}(f_j) \star l_j \star l) = \mathsf{HT}(m \star \mathsf{HT}(m_j \star f_j \star l_j) \star l) = \mathsf{HT}(m \star m_j \star f_j \star l_j \star l) \geq \mathsf{HT}(f_j)$. Now in case $m \star m_j, l_j \star l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we are done as then $(m_j \star m) \star f_j \star (l_j \star l)$ is a reductive standard representation in terms of F.
Hence let us assume $m \star m_j = \sum_{i=1}^{k_1} \tilde{m}_i$, $l_j \star l = \sum_{i'=1}^{k'_1} \tilde{l}_{i'}$, $\tilde{m}_i, \tilde{l}_{i'} \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$. Let $\mathsf{T}(f_j) = \{t_1, \ldots, t_w\}$ with $t_1 \succ t_i$, $2 \leq i \leq w$, i.e. $t_1 = \mathsf{HT}(f_j)$. As $\mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j) \geq \mathsf{HT}(f_j) \succ t_p$, $2 \leq p \leq w$, again by Definition 4.4.7 we can conclude $\mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j) \succ m_j \star t_p \star l_j \succeq \mathsf{HT}(m_j \star t_p \star l_j)$, and $m_j \star \mathsf{HT}(f_j) \star l_j \succ \sum_{p=2}^{w} m_j \star t_p \star l_j$. Then for each s_i, $2 \leq i \leq l$ there exists $t_q \in \mathsf{T}(f_1)$ such that

[51] Notice that $m_j \star \mathsf{HT}(f_j) \star l_j$ can be a polynomial and hence we cannot conclude $m_j \star \mathsf{HT}(f_j) \star l_j = \mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j)$.

$s_i \in \mathsf{supp}(m_j \star t_q \star l_j)$. Since $\mathsf{HT}(p) \succ s_i$ and even $\mathsf{HT}(p) \succeq m_j \star t_q \star l_j$ we find that either $\mathsf{HT}(m \star p \star l) \succeq \mathsf{HT}(m \star (m_j \star t_q \star l_j) \star l) = \mathsf{HT}((m \star m_j) \star t_q \star (l_j \star l))$ in case $\mathsf{HT}(m_j \star t_q \star l_j) = \mathsf{HT}(m_j \star f_j \star l_j)$ or $\mathsf{HT}(m \star p \star l) \succ \mathsf{HT}(m \star (m_j \star t_q \star l_j) \star l) = \mathsf{HT}((m \star m_j) \star t_q \star (l_j \star l))$. Hence we can conlude $\tilde{m}_i \star f_j \star \tilde{l}_{i'} \preceq \mathsf{HT}(m \star p \star l)$, $1 \leq i \leq k_1$, $1 \leq i' \leq k'_1$ and for at least one such multiple we get $\mathsf{HT}(\tilde{m}_i \star f_1 \star \tilde{l}_{i'}) = \mathsf{HT}(m \star m_j \star f_j \star l_j \star l) \geq \mathsf{HT}(f_j)$.
It remains to analyze the situation for the function $(\sum_{i=k+1}^{n} m \star (m_i \star f_i \star l_i) \star l$. Again we find that for all terms s in the $m_i \star f_i \star l_i$, $k+1 \leq i \leq n$, we have $\mathsf{HT}(p) \succ s$ and we get $\mathsf{HT}(m \star p \star l) \succeq \mathsf{HT}(m \star s \star l)$. Hence all polynomial multiples of the f_i in the representation $\sum_{i=k+1}^{n}((\sum_{j=1}^{k_i} \tilde{m}^i_j) \star f_i \star (\sum_{j=1}^{k'_i} \tilde{l}^i_j))$, where $m \star m_i = \sum_{j=1}^{k_i} \tilde{m}^i_j$, $l_i \star l = \sum_{j=1}^{k'_i} \tilde{l}^i_j$, are bounded by $\mathsf{HT}(m \star p \star l)$.

q.e.d.

Notice that this lemma no longer holds in case we only require $\mathsf{HT}(m \star \mathsf{HT}(p) \star l) = \mathsf{HT}(m \star p \star l) \succeq \mathsf{HT}(p)$, as then $\mathsf{HT}(p) \succ s$ no longer implies $\mathsf{HT}(m \star p \star l) \succ \mathsf{HT}(m \star s \star l)$.

Our standard representations from Definition 4.4.8 are closely related to a reduction relation based on the divisibility of terms as defined in the context of reductive restrictions of orderings on page 135.

Definition 4.4.17
Let f, p be two non-zero polynomials in $\mathcal{F}_{\mathbb{K}}$. We say f **reduces** p **to** q **at a monomial** $\alpha \cdot t$ **in one step**, denoted by $p \longrightarrow_f q$, if there exist $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) = t \geq \mathsf{HT}(f)$,
3. $\mathsf{HM}(m \star f \star l) = \alpha \cdot t$, and
4. $q = p - m \star f \star l$.

We write $p \longrightarrow_f$ if there is a polynomial q as defined above and p is then called reducible by f. Further, we can define $\stackrel{*}{\longrightarrow}$, $\stackrel{+}{\longrightarrow}$ and $\stackrel{n}{\longrightarrow}$ as usual. Reduction by a set $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ is denoted by $p \longrightarrow_F q$ and abbreviates $p \longrightarrow_f q$ for some $f \in F$. $\diamond$

Due to the fact that the coefficients lie in a field, again if for some terms $w_1, w_2 \in \mathcal{T}$ we have $\mathsf{HT}(w_1 \star f \star w_2) = \mathsf{HT}(w_1 \star \mathsf{HT}(f) \star w_2) = t \geq \mathsf{HT}(f)$ this implies reducibility at the monomial $\alpha \cdot t$.

Lemma 4.4.18
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$.

1. *For $p, q \in \mathcal{F}_{\mathbb{K}}$ we have that $p \longrightarrow_F q$ implies $p \succ q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.*

2. *$\longrightarrow_F$ is Noetherian.*

Proof :

1. Assuming that the reduction step takes place at a monomial $\alpha \cdot t$, by Definition 4.4.17 we know $\mathsf{HM}(m_1 \star f \star m_2) = \alpha \cdot t$ which yields $p \succ p - m_1 \star f \star m_2$ since $\mathsf{HM}(m_1 \star f \star m_2) \succ \mathsf{RED}(m_1 \star f \star m_2)$.

2. This follows directly from 1. as the ordering $\succeq$ on $\mathcal{T}$ is well-founded (compare Lemma 4.2.3).

q.e.d.

The next lemma shows how reduction sequences and reductive standard representations are related.

Lemma 4.4.19
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and p a non-zero polynomial in $\mathcal{F}_{\mathbb{K}}$. Then $p \xrightarrow{*}_F o$ implies that p has a reductive standard representation in terms of F.

Proof :
This follows directly by adding up the polynomials used in the reduction steps occurring in the reduction sequence $p \xrightarrow{*}_F o$.

q.e.d.

If $p \xrightarrow{*}_F q$, then p has a reductive standard representation in terms of $F \cup \{q\}$, especially $p - q$ has one in terms of F.

As stated before an analogon to the Translation Lemma holds.

Lemma 4.4.20
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}$ and p, q, h polynomials in $\mathcal{F}_{\mathbb{K}}$.

1. *Let $p - q \longrightarrow_F h$. Then there exist $p', q' \in \mathcal{F}_{\mathbb{K}}$ such that $p \xrightarrow{*}_F p'$ and $q \xrightarrow{*}_F q'$ and $h = p' - q'$.*

2. *Let o be a normal form of $p - q$ with respect to F. Then there exists $g \in \mathcal{F}_{\mathbb{K}}$ such that $p \xrightarrow{*}_F g$ and $q \xrightarrow{*}_F g$.*

Proof :

1. Let $p - q \longrightarrow_F h$ at the monomial $\alpha \cdot t$, i.e., $h = p - q - m \star f \star l$ for some $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) = t \geq \mathsf{HT}(f)$ and $\mathsf{HM}(m \star f \star l) = \alpha \cdot t$. We have to distinguish three cases:
   (a) $t \in \mathsf{supp}(p)$ and $t \in \mathsf{supp}(q)$: Then we can eliminate the occurence of t in the respective polynomials by reduction and get $p \longrightarrow_f p - \alpha_1 \cdot (m \star f \star l) = p'$, $q \longrightarrow_f q - \alpha_2 \cdot (m \star f \star l) = q'$, where $\alpha_1 \cdot \mathsf{HC}(m \star f \star l)$ and $\alpha_2 \cdot \mathsf{HC}(m \star f \star l)$ are the coefficients of t in p respectively q. Moreover, $\alpha_1 \cdot \mathsf{HC}(m \star f \star l) - \alpha_2 \cdot \mathsf{HC}(m \star f \star l) = \alpha$ and hence $\alpha_1 - \alpha_2 = 1$, as $\mathsf{HC}(m \star f \star l) = \alpha$. This gives us $p' - q' = p - \alpha_1 \cdot (m \star f \star l) - q + \alpha_2 \cdot (m \star f \star l) = p - q - (\alpha_1 - \alpha_2) \cdot (m \star f \star l) = p - q - m \star f \star l = h$.
   (b) $t \in \mathsf{supp}(p)$ and $t \notin \mathsf{supp}(q)$: Then we can eliminate the term t in the polynomial p by right reduction and get $p \longrightarrow_f p - m \star f \star l = p'$, $q = q'$, and, therefore, $p' - q' = p - m \star f \star l - q = h$.
   (c) $t \in \mathsf{supp}(q)$ and $t \notin \mathsf{supp}(p)$: Then we can eliminate the term t in the polynomial q by right reduction and get $q \longrightarrow_f q + m \star f \star l = q'$, $p = p'$, and, therefore, $p' - q' = p - (q + m \star f \star l) = h$.
2. We show our claim by induction on k, where $p - q \overset{k}{\longrightarrow}_F o$. In the base case $k = 0$ there is nothing to show as then $p = q$. Hence, let $p - q \longrightarrow_F h \overset{k}{\longrightarrow}_F o$. Then by 1. there are polynomials $p', q' \in \mathcal{F}_{\mathbb{K}}$ such that $p \overset{*}{\longrightarrow}_F p'$ and $q \overset{*}{\longrightarrow}_F q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \overset{k}{\longrightarrow}_F o$ yields the existence of a polynomial $g \in \mathcal{F}_{\mathbb{K}}$ such that $p \overset{*}{\longrightarrow}_F g$ and $q \overset{*}{\longrightarrow}_F g$.

q.e.d.

The essential part of the proof is that reducibility as defined in Definition 4.4.17 is connected to stable divisors of terms and not to coefficients. We will later see that for function rings over reduction rings, when the coefficient is also involved in the reduction step, this lemma no longer holds.

Next we state the definition of Gröbner bases based on the reduction relation.

Definition 4.4.21
A subset G of $\mathcal{F}_{\mathbb{K}}$ is called a **Gröbner basis** (with respect to the reduction relation $\longrightarrow$) of the ideal $\mathfrak{i} = \mathsf{ideal}(G)$, if $\overset{*}{\longleftrightarrow}_G \; = \; \equiv_{\mathfrak{i}}$ and $\longrightarrow_G$ is confluent.

Remember the free group ring in Example 4.2.18 where the polynomial $b + \lambda$ lies in the ideal generated by the polynomial $a + \lambda$. Then of course $b + \lambda$ also lies in the ideal generated by $a + \lambda$. Unlike in the case of polynomial rings over fields where for any set of polynomials F we have $\overset{*}{\longleftrightarrow}^{\mathrm{b}}_{F} = \equiv_{\mathsf{ideal}(F)}$, here we have $b + \lambda \equiv_{\mathsf{ideal}(\{a+\lambda\})} 0$ but $b + \lambda \overset{*}{\not\longleftrightarrow}_{a+\lambda} 0$. Hence the first condition of Definition 4.4.21 is again neccessary.

Now by Lemma 4.4.20 and Theorem 3.1.5 weak Gröbner bases are Gröbner bases and can be characterized as follows:

Corollary 4.4.22
Let G be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. G is a (weak) Gröbner basis of $\mathsf{ideal}(G)$ if and only if for every $g \in \mathsf{ideal}(G)$ we have $g \overset{*}{\longrightarrow}_{G} o$.

Finally we can characterize Gröbner bases similar to Theorem 2.3.11.

Theorem 4.4.23
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}} \backslash \{o\}$. Then F is a Gröbner basis of $\mathsf{ideal}(G)$ if and only if

1. *for all f in F and for all m, l in $\mathsf{M}(\mathcal{F}_{\mathbb{K}})$ we have $m \star f \star l \overset{*}{\longrightarrow}_{F} o$, and*
2. *for all p and q in F and every tuple (t, u_1, u_2, v_1, v_2) in $\mathcal{C}(p, q)$ and the respective s-polynomial $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2)$ we have $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2) \overset{*}{\longrightarrow}_{F} o$.*

We will later on prove a stronger version of this theorem.

The importance of Gröbner bases in the classical case stems from the fact that we only have to check a finite set of s-polynomials for F in order to decide, whether F is a Gröbner basis. Hence, we are interested in localizing the test sets in Theorem 4.4.23 – if possible to finite ones.

Definition 4.4.24
A set of polynomials $F \subseteq \mathcal{F}_{\mathbb{K}} \backslash \{o\}$ is called **weakly saturated**, if for all monomials m, l in $\mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and every polynomial $f \in F$ we have $m \star f \star l \overset{*}{\longrightarrow}_{F} o$. ◇

This of course implies that for a weakly saturated set F and any $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$, $f \in F$ the multiple $m \star f \star l$ has a reductive standard representation in terms of F.

Notice that since the coefficient domain is a field we could restrict ourselves to multiples with elements of $\mathcal{T}$. However, as we will later on allow reduction rings as coefficient domains, we present this more general definition.

Definition 4.4.25
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{0\}$. A set $\mathsf{SAT}(F) \subseteq \{m \star f \star l \mid f \in F, m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})\}$ is called a **stable saturator** for F if for any $f \in F$, $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ there exist $s \in \mathsf{SAT}(F)$, $m', l' \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $m \star f \star l = m' \star s \star l'$, $\mathsf{HT}(m \star f \star l) = \mathsf{HT}(m' \star \mathsf{HT}(s) \star l') \geq \mathsf{HT}(s)$.

Corollary 4.4.26
Let $\mathsf{SAT}(F)$ be a stable saturator of a set $F \subseteq \mathcal{F}_{\mathbb{K}}$. Then for any $f \in F$, $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ there exists $s \in \mathsf{SAT}(F)$ such that $m \star f \star l \longrightarrow_s o$.

Lemma 4.4.27
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{0\}$. If for all $s \in \mathsf{SAT}(F)$ we have $s \overset{*}{\longrightarrow}_F o$, then for every m, l in $\mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and every polynomial f in F the multiple $m \star f \star l$ has a reductive standard representation in terms of F.

Proof :
This follows immediately from Lemma 4.4.16 and Lemma 4.4.19.

q.e.d.

Definition 4.4.28
Let p and q be two non-zero polynomials in $\mathcal{F}_{\mathbb{K}}$. Then a subset $C \subseteq \{\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2) \mid (t, u_1, u_2, v_1, v_2) \in \mathcal{C}_s(p, q)\}$ is called a **stable localization** for the critical situations if for every s-polynomial $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2)$ related to a tuple (t, u_1, u_2, v_1, v_2) in $\mathcal{C}_s(p, q)$ there exists a polynomial $h \in C$ and monomials $\alpha \cdot w_1, 1 \cdot w_2 \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that

1. $\mathsf{HT}(h) \leq \mathsf{HT}(\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2))$,
2. $\mathsf{HT}(w_1 \star h \star w_2) = \mathsf{HT}(w_1 \star \mathsf{HT}(h) \star w_2) = \mathsf{HT}(\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2))$,
3. $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2) = (\alpha \cdot w_1) \star h \star w_2$. $\diamond$

The idea behind this definition is to reduce the number of s-polynomials, which have to be considered when checking for the Gröbner basis property.

Corollary 4.4.29
Let $C \subseteq \{\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2) \mid (t, u_1, u_2, v_1, v_2) \in \mathcal{C}_s(p, q)\}$ be a stable localization for two polynomials $p, q \in \mathcal{F}_{\mathbb{K}}$. Then for any s-polynomial $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2)$ there exists $h \in C$ such that $\mathsf{spol}(p, q, t, u_1, u_2, v_1, v_2) \longrightarrow_h o$.

Lemma 4.4.30
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{0\}$. If for all h in a stable localization $C \subseteq \{\mathsf{spol}(p,q,t,u_1,u_2,v_1,v_2) \mid (t,u_1,u_2,v_1,v_2) \in \mathcal{C}_s(p,q)\}$, we have $h \xrightarrow{*}_F o$, then for every (t,u_1,u_2,v_1,v_2) in $\mathcal{C}_s(p,q)$ the s-polynomial $\mathsf{spol}(p,q,t,u_1,u_2,v_1,v_2)$ has a reductive standard representation in terms of F.

Proof :
This follows immediately from Lemma 4.4.16 and Lemma 4.4.19.

q.e.d.

Theorem 4.4.31
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{K}}\backslash\{0\}$. Then F is a Gröbner basis if and only if

1. *for all s in $\mathsf{SAT}(F)$ we have $s \xrightarrow{*}_F o$, and*
2. *for all p and q in F, and every polynomial h in a stable localization $C \subseteq \{\mathsf{spol}(p,q,t,u_1,u_2,v_1,v_2) \mid (t,u_1,u_2,v_1,v_2) \in \mathcal{C}(p,q)\}$, we have $h \xrightarrow{*}_F o$.*

Proof :
In case F is a Gröbner basis by Lemma 4.4.22 all elements of $\mathsf{ideal}(F)$ must reduce to zero by F. Since the polynomials in the saturator and the respective localizations of the s-polynomials all belong to the ideal generated by F we are done.
The converse will be proven by showing that every element in $\mathsf{ideal}(F)$ has a reductive standard representation in terms of F. Now, let $g = \sum_{j=1}^{n}(\alpha_j \cdot w_j) \star f_j \star z_j$ be an arbitrary representation of a non-zero polynomial $g \in \mathsf{ideal}(F)$ such that $\alpha_j \in \mathbb{K}^*$, $f_j \in F$, and $w_j, z_j \in \mathcal{T}$.
By the definition of the stable saturator for every multiple $w_j \star f_j \star z_j$ in this sum we have some $s \in \mathsf{SAT}(F)$, $m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $w_j \star f_j \star z_j = m \star s \star l$ and $\mathsf{HT}(w_j \star f_j \star z_j) = \mathsf{HT}(m \star s \star l) = \mathsf{HT}(m \star \mathsf{HT}(s) \star l) \geq \mathsf{HT}(s)$. Since we have $s \xrightarrow{*}_F o$, by Lemma 4.4.16 we can conclude that each $w_j \star f_j \star z_j$ has a reductive standard representation in terms of F. Therefore, we can assume that $\mathsf{HT}(w_j \star \mathsf{HT}(f_j) \star z_j) = \mathsf{HT}(w_j \star f_j \star z_j) \geq \mathsf{HT}(f_j)$ holds.
Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(w_j \star f_j \star z_j) \mid 1 \leq j \leq n\}$ and K as the number of polynomials $w_j \star f_j \star z_j$ with head term t.
Without loss of generality we can assume that the polynomial multiples with head term t are just $(\alpha_1 \cdot w_1) \star f_1 \star z_1, \ldots, (\alpha_K \cdot w_K) \star f_K \star z_K$. We proceed by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and

$K' < K)$[52].

Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and by our assumption our representation is already of the required form.

Hence let us assume $K > 1$, then for the two not necessarily different polynomials f_1, f_2 in the corresponding representation we have $t = \mathsf{HT}(w_1 \star \mathsf{HT}(f_1) \star z_1) = \mathsf{HT}(w_1 \star f_1 \star z_1) = \mathsf{HT}(w_2 \star f_2 \star z_2) = \mathsf{HT}(w_2 \star \mathsf{HT}(f_2) \star z_2)$ and $t \geq \mathsf{HT}(f_1)$, $t \geq \mathsf{HT}(f_2)$. Then the tuple (t, w_1, w_2, z_1, z_2) is in $\mathcal{C}(f_1, f_2)$ and we have a polynomial h in a stable localization $C \subseteq \{\mathsf{spol}(f_1, f_2, t, w_1, w_2, z_1, z_2) \mid (t, w_1, w_2, z_1, z_2) \in \mathcal{C}(f_1, f_2)\}$ and $\alpha \cdot w, 1 \cdot z \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ such that $\mathsf{spol}(f_1, f_2, t, w_1, w_2, z_1, z_2) = \mathsf{HC}(w_1 \star f_1 \star z_1)^{-1} \cdot w_1 \star f_1 \star z_1 - \mathsf{HC}(w_2 \star f_2 \star z_2)^{-1} \cdot w_2 \star f_2 \star z_2 = (\alpha \cdot w) \star h \star z$ and $\mathsf{HT}(\mathsf{spol}(f_1, f_2, t, w_1, w_2, z_1, z_2) = \mathsf{HT}(w \star h \star z) = \mathsf{HT}(w \star \mathsf{HT}(h) \star z) \geq \mathsf{HT}(h)$.

We will now change our representation of g by using the additional information on this situation in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume the s-polynomial is not o[53]. By our assumption, $h \xrightarrow{*}_F o$ and by Lemma 4.4.19 h has a reductive standard representation in terms of F. Then by Lemma 4.4.16 the multiple $(\alpha \cdot w) \star h \star z$ again has a right reductive standard representation in terms of F, say $\sum_{i=1}^n m_i \star h_i \star l_i$, where $h_i \in F$, and $m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and all terms occurring in this sum are bounded by $t \succ \mathsf{HT}((\alpha \cdot w) \star h \star z)$. This gives us:

$$\begin{aligned}
& (\alpha_1 \cdot w_1) \star f_1 \star z_1 + (\alpha_2 \cdot w_2) \star f_2 \star z_2 \\
= \;& (\alpha_1 \cdot w_1) \star f_1 \star z_1 + \underbrace{(\alpha_2' \cdot \beta_1 \cdot w_1) \star f_1 \star z_1 - (\alpha_2' \cdot \beta_1 \cdot w_1) \star f_1 \star z_1}_{=0} \\
& + (\underbrace{\alpha_2' \cdot \beta_2}_{=\alpha_2} \cdot w_2) \star f_2 \star z_2 \\
= \;& ((\alpha_1 + \alpha_2' \cdot \beta_1) \cdot w_1) \star f_1 \star z_1 - \alpha_2' \cdot \underbrace{((\beta_1 \cdot w_1) \star f_1 \star z_1 - (\beta_2 \cdot w_2) \star f_2 \star z_2)}_{=(\alpha \cdot w) \star h \star z} \\
= \;& ((\alpha_1 + \alpha_2' \cdot \beta_1) \cdot w_1) \star f_1 \star z_1 - \alpha_2' \cdot (\sum_{i=1}^{n} m_i \star h_i \star l_i) \qquad (4.7)
\end{aligned}$$

where $\beta_1 = \mathsf{HC}(w_1 \star f_1 \star z_1)^{-1}$, $\beta_2 = \mathsf{HC}(w_2 \star f_2 \star z_2)^{-1}$ and $\alpha_2' \cdot \beta_2 = \alpha_2$. By substituting (4.7) in our representation of g the representation becomes smaller.

q.e.d.

Obviously this theorem states a criterion for when a set is a Gröbner basis. As in the case of completion procedures such as the Knuth-Bendix procedure or

[52] Note that this ordering is well-founded since $\succ$ is well-founded on $\mathcal{T}$ and $K \in \mathbb{N}$.

[53] In case $h = o$, just substitute the empty sum for the right reductive representation of h in the equations below.

Buchberger's algorithm, elements from these test sets which do not reduce to zero can be added to the set being tested, to gradually describe a not necessarily finite Gröbner basis. Of course in order to get a computable completion procedure certain assumptions on the test sets have to be made, e.g. they should themselves be recursively enumerable, and normal forms with respect to finite sets have to be computable. The examples from page 97 can also be studied with respect to two-sided ideals. For polynomial rings, skew-polynomial rings commutative monoid rings and commutative respectively poly-cyclic group rings finite Gröbner bases can be computed in the respective setting.

4.4.2 Function Rings over Reduction Rings

The situation becomes more complicated if R is not a field.

Let R be a non-commutative ring with a reduction relation $\Longrightarrow_B$ associated with subsets $B \subseteq \mathsf{R}$ as described in Section 3.1.

When following the path of linking special standard representations and reduction relations we get the same results as in Section 4.2.2, i.e., such representations naturally arise from the respective reduction relations. Hence we proceed by studying a special reduction relation which subsumes the two reduction relations presented for one-sided ideals in function rings over reduction rings. As before for our ordering $>_{\mathsf{R}}$ on R we require: 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 will ensure that the reduction relation on $\mathcal{F}$ is terminating. The reduction relation on R can be used to define various reduction relations on the function ring. Here we want to present a reduction relation which in some sense is based on the "divisibility" of the term to be reduced by the head term of the polynomial used for reduction.

Definition 4.4.32
Let f, p be two non-zero polynomials in $\mathcal{F}$. We say f **reduces** p **to** q **at a monomial** $\alpha \cdot t$ **in one step**, denoted by $p \longrightarrow_f q$, if there exist monomials $m, l \in \mathsf{M}(\mathcal{F})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) = t \geq \mathsf{HT}(f)$,
3. $\alpha \Longrightarrow_{\mathsf{HC}(m \star f \star l)} \beta$, with[54] $\alpha = \sum_{i=1}^{k} \gamma_i \cdot \mathsf{HC}(m \star f \star l) \cdot \delta_i + \beta$ for some $\beta, \gamma_i, \delta_i \in \mathsf{R}$, $1 \leq i \leq k$, and
4. $q = p - \sum_{i=1}^{k} \gamma_i \cdot m \star f \star l \cdot \delta_i$.

[54]Remember that by Axiom (A2) for reduction rings $\alpha \Longrightarrow_\gamma \beta$ implies $\alpha - \beta \in \mathsf{ideal}(\gamma)$ and hence $\alpha = \sum_{i=1}^{k} \gamma_i \cdot \gamma \cdot \delta_i + \beta$, $\gamma_i, \delta_i \in \mathsf{R}$.

We write $p \longrightarrow_f$ if there is a polynomial q as defined above and p is then called reducible by f. Further, we can define $\stackrel{*}{\longrightarrow}$, $\stackrel{+}{\longrightarrow}$ and $\stackrel{n}{\longrightarrow}$ as usual. Reduction by a set $F \subseteq \mathcal{F}\backslash\{o\}$ is denoted by $p \longrightarrow_F q$ and abbreviates $p \longrightarrow_f q$ for some $f \in F$. $\diamond$

By specializing item 3. of this definition to

$$3.\ \alpha \Longrightarrow_{\mathsf{HC}(m\star f\star l)} \text{ such that } \alpha = \mathsf{HC}(m \star f \star l)$$

we get an analogon to Definition 4.2.43. Similarly, specializing 3. to

$$3.\ \alpha \Longrightarrow_{\mathsf{HC}(m\star f\star l)} \beta \text{ such that } \mathsf{HC}(m \star f \star l) + \beta$$

gives us an analogon to Definition 4.2.53.

Reviewing Example 4.2.54 we find that the reduction relation is not terminating when using infinite sets of polynomials for reduction. But for finite sets we get the following analogon of Lemma 4.2.55.

Lemma 4.4.33
Let F be a finite set of polynomials in $\mathcal{F}\backslash\{o\}$.

1. *For $p, q \in \mathcal{F}$, $p \longrightarrow_F q$ implies $p \succ q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.*
2. *$\longrightarrow_F$ is Noetherian.*

Proof :

1. Assuming that the reduction step takes place at a monomial $\alpha \cdot t$, by Definition 4.4.32 we know $\mathsf{HM}(p - \sum_{i=1}^{k} \gamma_i \cdot m_1 \star f \star m_2 \cdot \delta_i) = \beta \cdot t$ which yields $p \succ p - \sum_{i=1}^{k} \gamma_i \cdot m_1 \star f \star m_2 \cdot \delta_i$ since $\alpha >_{\mathsf{R}} \beta$.
2. This follows from 1. and Axiom (A1) as long as only finite sets of polynomials are involved.

q.e.d.

As for the one-sided case a Translation Lemma does not hold for this reduction relation. Hence we have to distinguish between weak Gröbner bases and Gröbner bases.

Definition 4.4.34
A set $F \subseteq \mathcal{F}\backslash\{o\}$ is called a weak Gröbner basis of $\mathsf{ideal}(F)$ if for all $g \in \mathsf{ideal}(F)$ we have $g \stackrel{*}{\longrightarrow}_F o$. $\diamond$

Now as for one-sided weak Gröbner bases, weak Gröbner bases allow special representations of the polynomials in the ideal they generate.

Corollary 4.4.35
Let F be a set of polynomials in $\mathcal{F}$ and g a non-zero polynomial in $\mathsf{ideal}(F)$ *such that $g \xrightarrow{*}_F o$. Then g has a representation of the form*

$$g = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$ for $1 \leq i \leq k$, and $\mathsf{HT}(g) \succ \mathsf{HT}(m_i \star f_i \star l_i)$ for all $k+1 \leq i \leq n$.

Proof :
We show our claim by induction on n where $g \xrightarrow{n}_F o$. If $n = 0$ we are done. Else let $g \xrightarrow{1}_F g_1 \xrightarrow{n}_F o$. In case the reduction step takes place at the head monomial, there exists a polynomial $f \in F$ and monomial $m, l \in \mathsf{M}(\mathcal{F})$ such that $\mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) = \mathsf{HT}(g) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g) \Longrightarrow_{\mathsf{HC}(m \star f \star l)} \beta$ with $\mathsf{HC}(g) \Longrightarrow_{\mathsf{HC}(m \star f \star l)} \beta$ with $\mathsf{HC}(g) = \beta + \sum_{i=1}^{k} \gamma_i \cdot \mathsf{HC}(m \star f \star l) \cdot \delta_i$ for some $\gamma_i, \delta_i \in \mathsf{R}$, $1 \leq i \leq k$. Moreover the induction hypothesis then is applied to $g_1 = g - \sum_{i=1}^{k} \gamma_i \cdot m \star f \star l \cdot \delta_i$. If the reduction step takes place at a monomial with term smaller $\mathsf{HT}(g)$ for the respective monomial multiple $m \star f \star l$ we immediately get $\mathsf{HT}(g) \succ \mathsf{HT}(m \star f \star l)$ and we can apply our induction hypothesis to the resulting polynomial g_1. In both cases we can arrange the monomial multiples $m \star f \star l$ arising from the reduction steps in such a way that gives us th desired representation.

q.e.d.

As in Theorem 4.4.15 we can characterize weak Gröbner bases using g- and m-polynomials instead of s-polynomials.

Definition 4.4.36
Let $P = \{p_1, \ldots, p_k\}$ be a multiset of (not necessarily different) polynomials in $\mathcal{F}$ and t an element in $\mathcal{T}$ such that there are $u_1, \ldots, u_k, v_1, \ldots, v_k \in \mathcal{T}$ with $\mathsf{HT}(u_i \star p_i \star v_i) = \mathsf{HT}(u_i \star \mathsf{HT}(p_i) \star v_i) = t$, for all $1 \leq i \leq k$. Further let $\gamma_i = \mathsf{HC}(u_i \star p_i \star v_i)$ for $1 \leq i \leq k$.
Let G be a (weak) Gröbner basis of $\{\gamma_1, \ldots, \gamma_k\}$ with respect to $\Longrightarrow$ in R and

$$\alpha = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j} \cdot \gamma_i \cdot \delta_{i,j}$$

for $\alpha \in G$, $\beta_{i,j}, \delta_{i,j} \in \mathsf{R}$, $1 \leq i \leq k$, and $1 \leq j \leq n_i$. Then we define the **g-polynomials (Gröbner polynomials)** corresponding to $p_1, \ldots, p_k$ and t by setting

$$g_\alpha = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j} \cdot u_i \star p_i \star v_i \cdot \delta_{i,j}.$$

Notice that $\mathsf{HM}(g_\alpha) = \alpha \cdot t$.
We define the **m-polynomials (module polynomials)** corresponding to P and t as those

$$h = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j} \cdot u_i \star p_i \star v_i \cdot \delta_{i,j}$$

where $\sum_{i=1}^{k} \sum_{j=1}^{n_i} \beta_{i,j} \cdot \gamma_i \cdot \delta_{i,j} = 0$. Notice that $\mathsf{HT}(h) \prec t$. $\diamond$

Notice that while we allow the multiplication of two terms to have influence on the coefficients of the result[55] we require that $t \cdot \alpha = \alpha \cdot t$.

Given a set of polynomials F, the set of corresponding g- and m-polynomials is again defined for all possible multisets of polynomials in F and appropriate terms t as specified by Definition 4.4.36. Notice that given a finite set of polynomials the corresponding sets of g- and m-polynomials in general will be infinite.

We can use g- and m-polynomials to characterize special bases in function rings over reduction rings satisfying Axiom (A4) in case we add an additional condition as before.

Theorem 4.4.37
Let F be a finite set of polynomials in $\mathcal{F}\backslash\{o\}$ where the reduction ring satisfies (A4). Then F is a weak Gröbner basis if and only if

1. *for all f in F and for all m, l in $\mathsf{M}(\mathcal{F})$ we have $m \star f \star l \xrightarrow{*}_F o$, and*
2. *all g- and all m-polynomials corresponding to F as specified in Definition 4.4.36 reduce to zero using F.*

Proof :
In case F is a weak Gröbner basis, since the multiples $m \star f \star l$ as well as the respective g- and m-polynomials are all elements of $\mathsf{ideal}(F)$ they must reduce to zero using F.
The converse will be proven by showing that every element in $\mathsf{ideal}(F)$ is reducible by F. Then as $g \in \mathsf{ideal}(F)$ and $g \longrightarrow_F g'$ implies $g' \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}_F o$. Notice that this only holds in case the reduction relation $\longrightarrow_F$ is Noetherian. This follows as by our assumption F is finite.
Let $g \in \mathsf{ideal}(F)$ have a representation in terms of F of the following form: $g = \sum_{j=1}^{n} m_j \star f_j \star l_j$, $f_j \in F$ and $m_j, l_j \in \mathsf{M}(\mathcal{F})$. Depending on this representation of g

[55] Skew-polynomial rings are a classical example, see Section 4.2.1.

and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(m_j \star f_j \star l_j) \mid 1 \leq j \leq n\}$ and K as the number of polynomials $m_j \star f_j \star l_j$ with head term t. We show our claim by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$).

Since by our first assumption every multiple $m_j \star f_j \star l_j$ in this sum reduces to zero using F and hence has a representation as described in Corollary 4.4.35 we can assume that $\mathsf{HT}(m_j \star \mathsf{HT}(f_j) \star l_j) = \mathsf{HT}(m_j \star f_j \star l_j) \geq \mathsf{HT}(f_j)$ holds. Without loss of generality we can assume that the polynomial multiples with head term t are just $m_1 \star f_1 \star l_1, \ldots, m_K \star f_K \star l_K$.

Obviously, $t \succeq \mathsf{HT}(g) = \mathsf{HT}(m_1 \star \mathsf{HT}(f_1) \star l_1) \geq \mathsf{HT}(f_1)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and even $\mathsf{HM}(g) = \mathsf{HM}(m_1 \star f_1 \star l_1)$, implying that g is reducible at $\mathsf{HM}(g)$ by f_1.

Hence let us assume $K > 1$.

First let $\sum_{j=1}^{K} \mathsf{HM}(m_j \star f_j \star l_j) = o$. Then there is a m-polynomial h, corresponding to the polynomials $f_1, \ldots, f_K$ and the term t such that $\sum_{j=1}^{K} l_j \star f_j \star m_j = h$. We will now change our representation of g by using the additional information on this m-polynomial in such a way that for the new representation of g we have a smaller maximal term. Let us assume the m-polynomial is not o[56]. By our assumption, h is reducible to zero using F and hence has a representation with respect to F as described in Corollary 4.4.35, say $\sum_{i=1}^{n} \tilde{m}_i \star \tilde{f}_i \star \tilde{l}_i$, where $\tilde{f}_i \in F$, $\tilde{m}_i, \tilde{l}_i \in \mathsf{M}(\mathcal{F})$ and all terms occurring in the sum are bounded by $t \succ \mathsf{HT}(h)$. Hence replacing the sum $\sum_{j=1}^{K} m_j \star f_j \star l_j$ by $\sum_{i=1}^{n} \tilde{m}_i \star \tilde{f}_i \star \tilde{l}_i$ gives us a smaller representation of g.

Hence let us assume $\sum_{j=1}^{K} \mathsf{HM}(m_j \star f_j \star l_j) \neq 0$. Then we have $\mathsf{HT}(m_1 \star f_1 \star l_1 + \ldots + m_K \star f_K \star l_K) = t = \mathsf{HT}(g)$, $\mathsf{HC}(g) = \mathsf{HC}(m_1 \star f_1 \star l_1 + \ldots + m_K \star f_K \star l_K) \in \mathsf{ideal}_r(\{\mathsf{HC}(m_1 \star f_1 \star l_1), \ldots, \mathsf{HC}(m_K \star f_K \star l_K)\})$ and even $\mathsf{HM}(m_1 \star f_1 \star l_1 + \ldots + m_K \star f_K \star l_K) = \mathsf{HM}(g)$. Hence $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by α, $\alpha \in G$, G¡a (weak) right Gröbner basis of $\mathsf{ideal}_r(\{\mathsf{HC}(m_1 \star f_1 \star l_1), \ldots, \mathsf{HC}(m_K \star f_K \star l_K)\})$ in R with respect to the reduction relation $\Longrightarrow$. Let g_α be the respective g-polynomial corresponding to α. Then we know that $g_\alpha \xrightarrow{*}_F o$. Moreover, we know that the head monomial of g_α is reducible by some polynomial $f \in F$ and we assume $\mathsf{HT}(g_\alpha) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g_\alpha) \Longrightarrow_{\mathsf{HC}(m \star f \star l)}$. Then, as $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by $\mathsf{HC}(g_\alpha)$, $\mathsf{HC}(g_\alpha)$ is $\Longrightarrow$-reducible to zero and (A4) holds, the head monomial of g is also reducible by some $f' \in F$ and we are done.

q.e.d.

Of course this theorem is still true for infinite F if we can show that for the respective function ring the reduction relation is terminating.

[56]In case $h = o$, just substitute the empty sum for the reductive representation of h in the equations below.

Now the question arises when the critical situations in this characterization can be localized to subsets of the respective sets. Reviewing the Proof of Theorem 4.4.31 we find that Lemma 4.4.16 is central as it describes when multiples of polynomials which have a reductive standard representation in terms of some set F again have such a representation. As before, this does not hold for function rings over reduction rings in general. We have stated that it is not natural to link right reduction as defined in Definition 4.4.32 to special standard representations. Hence, to give localizations of Theorem 4.4.37 another property for $\mathcal{F}$ is sufficient:

Definition 4.4.38
A set $C \subset S \subseteq \mathcal{F}$ is called a **stable localization** of S if for every $g \in S$ there exists $f \in C$ such that $g \longrightarrow_f o$. $\diamond$

In case $\mathcal{F}$ and $\longrightarrow$ allow such stable localizations, we can rephrase Theorem 4.4.37 as follows:

Theorem 4.4.39
Let F be a finite set of polynomials in $\mathcal{F}\backslash\{o\}$ where the reduction ring satisfies (A4). Then F is a weak Gröbner basis of $\mathsf{ideal}(F)$ if and only if

1. *for all s in a stable localization of $\{m \star f \star l \mid f \in \mathcal{F}, m, l \in \mathsf{M}(\mathcal{F})\}$ we have $s \xrightarrow{*}_F o$, and*
2. *for all h in a stable localization of the g- and m-polynomials corresponding to F as specified in Definition 4.4.36 we have $h \xrightarrow{*}_F o$.*

We have stated that for arbitrary reduction relations in $\mathcal{F}$ it is not natural to link them to special standard representations. Still, when proving Theorem 4.4.39, we will find that in order to change the representation of an arbitrary ideal element, Definition 4.4.38 is not enough to ensure reducibility. However, we can substitute the critical situation using an analogon of Lemma 4.4.16, which while not related to reducibility in this case will still be sufficient to make the representation smaller.

Lemma 4.4.40
Let $F \subseteq \mathcal{F}\backslash\{o\}$ and f, p non-zero polynomials in $\mathcal{F}$. If $p \longrightarrow_f o$ and $f \xrightarrow{*}_F o$, then p has a standard representation of the form

$$p = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$$

such that $\mathsf{HT}(p) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$ for $1 \leq i \leq k$ and $\mathsf{HT}(p) \succ \mathsf{HT}(m_i \star f_i \star l_i)$ for all $k+1 \leq i \leq n$.

Proof :

If $p \longrightarrow_f o$ then $p = \sum_{j=1}^{s} \gamma_j \cdot m' \star f \star l' \cdot \delta_j$ with $m', l' \in \mathsf{M}(\mathcal{F})$, $\gamma_j, \delta_j \in \mathsf{R}$, and $\mathsf{HT}(p) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) \geq \mathsf{HT}(f)$. Similarly $f \xrightarrow{*}_F o$ implies[57] $f = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}), n \in \mathbb{N}$ such that $\mathsf{HT}(f) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$, and $\mathsf{HT}(f) \succ \mathsf{HT}(m_i \star f_i \star l_i)$ for all $k+1 \leq i \leq n$.

We show our claim for all multiples with $\gamma_j \cdot m'$ and $l' \cdot \delta_j$ for $1 \leq j \leq s$. Let $m = \gamma_j \star m'$ and $l = l' \cdot \delta_j$ and let us analyze $m \star m_i \star f_i \star l_i \star l$ with $\mathsf{HT}(m_i \star f_i \star l_i) = \mathsf{HT}(f)$, $1 \leq i \leq k$. Let $\mathsf{T}(m_i \star f_i \star l_i) = \{s_1^i, \ldots, s_{w_i}^i\}$ with $s_1^i \succ s_j^i$, $2 \leq j \leq w_i$, i.e. $s_1^i = \mathsf{HT}(m_i \star f_i \star l_i) = \mathsf{HT}(p)$. Hence $m \star \mathsf{HT}(p) \star l = m \star s_1^i \star l \geq \mathsf{HT}(p) = s_1^i$ and as $s_1^i \succ s_j^i$, $2 \leq j \leq w_i$, by Definition 4.4.7 we can conclude $\mathsf{HT}(m \star \mathsf{HT}(p) \star l) = \mathsf{HT}(m \star s_1^i \star l) \succ m \star s_j^i \star l \succeq \mathsf{HT}(m \star s_j^i \star l)$ for $2 \leq j \leq w_i$. This implies $\mathsf{HT}(m \star \mathsf{HT}(m_i \star f_i \star l_i) \star l) = \mathsf{HT}(m \star m_i \star f_i \star l_i \star l)$ Hence we get

$$\begin{aligned} & \mathsf{HT}(m \star f \star l) \\ = \; & \mathsf{HT}(m \star \mathsf{HT}(f) \star l) \\ = \; & \mathsf{HT}(m \star \mathsf{HT}(m_i \star f_i \star l_i) \star l), \text{ as } \mathsf{HT}(p) = \mathsf{HT}(m_i \star f_i \star l_i) \\ = \; & \mathsf{HT}(m \star m_i \star f_i \star l_i \star l) \end{aligned}$$

and since $\mathsf{HT}(m \star f \star l) \geq \mathsf{HT}(f) \geq \mathsf{HT}(f_i)$ we can conclude $\mathsf{HT}(m \star m_i \star f_i \star l_i \star l) \geq \mathsf{HT}(f_i)$. It remains to show that $m \star (m_i \star f_i \star l_i) \star l = (m \star m_i) \star f_i \star (l_i \star l)$ has representations of the desired form in terms of F. First we show that $\mathsf{HT}((m \star m_i \star \mathsf{HT}(f_i) \star l_i \star l) \geq \mathsf{HT}(f_i)$. We know $m_i \star \mathsf{HT}(f_i) \star l_i \succeq \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i)$ and hence $\mathsf{HT}(m \star m_i \star \mathsf{HT}(f_i) \star l_i \star l) = \mathsf{HT}(m \star \mathsf{HT}(m_i \star f_i \star l_i) \star l) = \mathsf{HT}(m \star m_i \star f_i \star l_i \star l) \geq \mathsf{HT}(f_i)$.

Now in case $m \star m_i, l_i \star l \in \mathsf{M}(\mathcal{F})$ we are done as then $(m \star m_i) \star f_i \star (l_i \star l)$ is a representation of the desired form.

Hence let us assume $m \star m_i = \sum_{j=1}^{k_i} \tilde{m}_j^i, l_i \star l = \sum_{j'=1}^{k_i'} \tilde{l}_j^i \; \tilde{m}_j^i, \tilde{l}_{j'}^i \in \mathsf{M}(\mathcal{F})$. Let $\mathsf{T}(f_i) = \{t_1^i, \ldots, t_w^i\}$ with $t_1^i \succ t_j^i$, $2 \leq j \leq w$, i.e. $t_1^i = \mathsf{HT}(f_i)$. As $\mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) \geq \mathsf{HT}(f_i) \succ t_j$, $2 \leq j \leq w$, again by Definition 4.4.7 we can conclude that $\mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) \succ m_i \star t_j^i \star l_i \succeq \mathsf{HT}(m_i \star t_j^i \star l_i)$, $2 \leq j \leq l$, and $m_i \star \mathsf{HT}(f_i) \star l_i \succ \sum_{j=2}^{w} m_i \star t_j^i \star l_i$. Then for each s_j^i, $2 \leq j \leq w_i$, there exists $t_{j'}^i \in \mathsf{T}(f_i)$ such that $s_j^i \in \mathsf{supp}(m_i \star t_{j'}^i \star l_i)$. Since $\mathsf{HT}(f) \succ s_j^i$ and even $\mathsf{HT}(f) \succ m_i \star t_{j'}^i \star l_i$ we find that either $\mathsf{HT}(m \star f \star l) \succeq \mathsf{HT}(m \star (m_i \star t_{j'}^i \star l_i) \star l) = \mathsf{HT}((m \star m_i) \star t_{j'}^i \star (l_i \star l))$ in case $\mathsf{HT}(m_i \star t_{j'}^i \star l_i) = \mathsf{HT}(m_i \star f_1 \star l_i)$ or $\mathsf{HT}(m \star f \star l) \succ m \star (m_i \star t_{j'}^i \star l_i) \star l = (m \star m_i) \star t_{j'}^i \star (l_i \star l)$. Hence we can conclude $\tilde{m}_j^i \star f_i \star \tilde{l}_{j'}^i \preceq \mathsf{HT}(m \star f \star l)$, $1 \leq j \leq k_i$, $1 \leq j' \leq K_i$ and for at least one $\tilde{m}_j^i, \tilde{l}_{j'}^i$ we get $\mathsf{HT}(\tilde{m}_j^i \star f_i \star \tilde{l}_{j'}^i) = \mathsf{HT}(m \star m_i \star f_i \star l_i \star l) \geq \mathsf{HT}(f_i)$. It remains to analyze the situation for the functions $(\sum_{i=k+1}^{n} m \star (m_i \star f_i \star l_i) \star l$.

[57]Notice that in this representation we write the products of the form $\gamma \cdot m$ respectively $l \cdot \delta$ arising in the reduction steps as simple monomials.

Again we find that for all terms s in the $m_i \star f_i \star l_i$, $k+1 \leq i \leq n$, we have $\mathsf{HT}(f) \succeq s$ and we get $\mathsf{HT}(m \star f \star l) \succeq \mathsf{HT}(m \star s \star l)$. Hence all polynomial multiples of the f_i in the representation $\sum_{i=k+1}^{n}(\sum_{j=1}^{k_i} \tilde{m}_j^i) \star f_i \star (\sum_{j=1}^{K_i} \tilde{l}_{j'}^i)$, where $m \star m_i = \sum_{j=1}^{k_i} \tilde{m}_j^i$, $l_i \star l = \sum_{j=1}^{K_i} \tilde{l}_{j'}^i$, are bounded by $\mathsf{HT}(m \star f \star l)$.

q.e.d.

Proof Theorem 4.4.39:
The proof is basically the same as for Theorem 4.4.37. Due to Lemma 4.4.40 we can substitute the multiples $m_j \star f_j \star l_j$ by appropriate representations without changing (t, K). Hence, we only have to ensure that despite testing less polynomials we are able to apply our induction hypothesis. Taking the notations from the proof of Theorem 4.4.37, let us first check the situation for m-polynomials.
Let $\sum_{j=1}^{K} \mathsf{HM}(m_j \star f_j \star l_j) = o$. Then by Definition 4.4.36 there exists a module polynomial $h = \sum_{j=1}^{K} m_j \star f_j \star l_j$ and by our assumption there is a polynomial h' in the stable localization such that $h \longrightarrow_{h'} o$. Moreover, $h' \xrightarrow{*}_F o$. Then by Lemma 4.4.40 the m-polynomial h has a standard representations bounded by t. Hence we can change the representation of g by substituting h by its representation giving us a smaller representation and by our induction hypothesis g is reducible by F and we are done.
It remains to study the case where $\sum_{j=1}^{K} \mathsf{HM}(m_j \star f_j \star l_j) \neq 0$. Then we have $\mathsf{HT}(\sum_{j=1}^{K} m_j \star f_j \star l_j) = t = \mathsf{HT}(g)$, $\mathsf{HC}(g) = \mathsf{HC}(\sum_{j=1}^{K} m_j \star f_j \star l_j) \in \mathsf{ideal}(\{\mathsf{HC}(m_1 \star f_1 \star l_1), \ldots, \mathsf{HC}(m_K \star f_K \star l_K)\})$ and even $\mathsf{HM}(\sum_{j=1}^{K} m_j \star f_j \star l_j) = \mathsf{HM}(g)$. Hence $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by α, $\alpha \in G$, G a (weak) Gröbner basis of $\mathsf{ideal}(\{\mathsf{HC}(m_1 \star f_1 \star l_1), \ldots, \mathsf{HC}(m_K \star f_K \star l_K)\})$ in R with respect to the reduction relation $\Longrightarrow$. Let g_α be the respective g-polynomial corresponding to α. Then we know that $g_\alpha \longrightarrow_{g'_\alpha} o$ for some g'_α in the stable localization and $g'_\alpha \xrightarrow{*}_F o$. Moreover, we know that the head monomial of g'_α is reducible by some polynomial $f \in F$ and we assume $\mathsf{HT}(g_\alpha) = \mathsf{HT}(m \star \mathsf{HT}(f) \star l) = \mathsf{HT}(m \star f \star l) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g_\alpha) \Longrightarrow_{\mathsf{HC}(m \star f \star l)}$. Then, as $\mathsf{HC}(g)$ is $\Longrightarrow$-reducible by $\mathsf{HC}(g_\alpha)$, $\mathsf{HC}(g_\alpha)$ is $\Longrightarrow$-reducible by $\mathsf{HC}(g'_\alpha)$, $\mathsf{HC}(g'_\alpha)$ is $\Longrightarrow$-reducible to zero and (A4) holds, the head monomial of g is also reducible by some $f' \in F$ and we are done.

q.e.d.

Again, if for infinite F we can assure that the reduction relation is Noetherian, the proof still holds.

4.4.3 Function Rings over the Integers

In the previous section we have seen that for the reduction relation for $\mathcal{F}$ based on the abstract notion of the reduction relation $\Longrightarrow_{\mathsf{R}}$ there is not enough information on the reduction step involving the coefficient and hence we cannot prove an analogon of the Translation Lemma.

As in the case of studying one-sided ideals, when studying special reduction rings where we have more information on the specific reduction relation $\Longrightarrow_{\mathsf{R}}$ the situation often can be improved. Again we go into the details for the case that R is the ring of the integers $\mathbb{Z}$. The reduction relation presented in Definition 4.4.32 then can be reformulated for this special case as follows:

Definition 4.4.41
Let p, f be two non-zero polynomials in $\mathcal{F}_{\mathbb{Z}}$. We say f **reduces** p **to** q **at** $\alpha \cdot t$ **in one step**, i.e. $p \longrightarrow_f q$, if there exist $u, v \in \mathsf{T}(\mathcal{F}_{\mathbb{Z}})$ such that

1. $t \in \mathsf{supp}(p)$ and $p(t) = \alpha$,
2. $\mathsf{HT}(u \star \mathsf{HT}(f) \star v) = \mathsf{HT}(u \star f \star v) = t \geq \mathsf{HT}(f)$,
3. $\alpha \geq_{\mathbb{Z}} \mathsf{HC}(u \star f \star v) > 0$ and $\alpha \Longrightarrow_{\mathsf{HC}(u \star f \star v)} \delta$ where $\alpha = \mathsf{HC}(u \star f \star v) \cdot \beta + \delta$ with $\beta, \delta \in \mathbb{Z}$, $0 \leq \delta < \mathsf{HC}(u \star f \star v)$, and
4. $q = p - u \star f \star v \cdot \beta$.

We write $p \longrightarrow_f$ if there is a polynomial q as defined above and p is then called reducible by f. Further, we can define $\stackrel{*}{\longrightarrow}$, $\stackrel{+}{\longrightarrow}$ and $\stackrel{n}{\longrightarrow}$ as usual. Reduction by a set $F \subseteq \mathcal{F} \backslash \{o\}$ is denoted by $p \longrightarrow_F q$ and abbreviates $p \longrightarrow_f q$ for some $f \in F$. $\diamond$

As before, for this reduction relation we can still have $t \in \mathsf{supp}(q)$. The important part in showing termination now is that if we still have $t \in \mathsf{supp}(q)$ then its coefficient will be smaller according to our ordering chosen for $\mathbb{Z}$ (compare Section 4.2.3) and since this ordering is well-founded we are done. Due to the additional information on the coefficents, again we do not have to restrict ourselves to finite sets of polynomials in order to ensure termination.

Corollary 4.4.42
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}} \backslash \{o\}$.

1. *For $p, q \in \mathcal{F}_{\mathbb{Z}}$, $p \longrightarrow_F q$ implies $p \succ q$, in particular $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.*
2. *$\longrightarrow_F$ is Noetherian.*

Similarly, the additional information we have on the coefficients before and after the reduction step now enables us to prove an analogon of the Translation Lemma for function rings over the integers. The first and second part of the lemma are only needed to prove the essential third part.

Lemma 4.4.43
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}}$ and p, q, h polynomials in $\mathcal{F}_{\mathbb{Z}}$.

1. *Let $p - q \longrightarrow_F h$ such that the reduction step takes place at the monomial $\alpha \cdot t$ and we additionally have $t \notin \mathsf{supp}(h)$. Then there exist $p', q' \in \mathcal{F}_{\mathbb{Z}}$ such that $p \stackrel{*}{\longrightarrow}_F p'$ and $q \stackrel{*}{\longrightarrow}_F q'$ and $h = p' - q'$.*
2. *Let o be the unique normal form of p with respect to F and $t = \mathsf{HT}(p)$. Then there exists a polynomial $f \in F$ such that $p \longrightarrow_f p'$ and $t \notin \mathsf{supp}(p')$.*
3. *Let o be the unique normal form of $p - q$ with respect to F. Then there exists $g \in \mathcal{F}_{\mathbb{Z}}$ such that $p \stackrel{*}{\longrightarrow}_F g$ and $q \stackrel{*}{\longrightarrow}_F g$.*

Proof :

1. Let $p - q \longrightarrow_F h$ at the monomial $\alpha \cdot t$, i.e., $h = p - q - u \star f \star v \cdot \beta$ for some $u, v \in \mathsf{T}(\mathcal{F}_{\mathbb{Z}})$, $\beta \in \mathbb{Z}$ such that $\mathsf{HT}(u \star \mathsf{HT}(f) \star v) = \mathsf{HT}(u \star f \star v) = t \geq \mathsf{HT}(f)$ and $\mathsf{HC}(u \star f \star v) > 0$. Remember that α is the coefficient of t in $p - q$. Then as $t \notin \mathsf{supp}(h)$ we know $\alpha = \mathsf{HC}(u \star f \star v) \cdot \beta$. Let α_1 respectively α_2 be the coefficients of t in p respectively q and $\alpha_1 = (\mathsf{HC}(u \star f \star v) \cdot \beta) \cdot \beta_1 + \gamma_1$ respectively $\alpha_2 = (\mathsf{HC}(u \star f \star v) \cdot \beta) \cdot \beta_2 + \gamma_2$ for some $\beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathbb{Z}$ where $0 \leq \gamma_1, \gamma_2 < \mathsf{HC}(u \star f \star v) \cdot \beta$. Then $\alpha = \mathsf{HC}(u \star f \star v) \cdot \beta = \alpha_1 - \alpha_2 = (\mathsf{HC}(u \star f \star v) \cdot \beta) \cdot (\beta_1 - \beta_2) + (\gamma_1 - \gamma_2)$, and as $\gamma_1 - \gamma_2$ is no multiple of $\mathsf{HC}(u \star f \star v) \cdot \beta$ we have $\gamma_1 - \gamma_2 = 0$ and hence $\beta_1 - \beta_2 = 1$. We have to distinguish two cases:
   (a) $\beta_1 \neq 0$ and $\beta_2 \neq 0$: Then $p \longrightarrow_F p - u \star f \star v \cdot \beta \cdot \beta_1 = p'$, $q \longrightarrow_F q - u \star f \star v \cdot \beta \cdot \beta_2 = q'$ and $p' - q' = p - u \star f \star v \cdot \beta \cdot \beta_1 - q + u \star f \star v \cdot \beta \cdot \beta_2 = p - q - u \star f \star v \cdot \beta \cdot \beta = h$.
   (b) $\beta_1 = 0$ and $\beta_2 = -1$ (the case $\beta_2 = 0$ and $\beta_1 = 1$ being symmetric): Then $p' = p$, $q \longrightarrow_F q - u \star f \star v \cdot \beta \cdot \beta_2 = q + u \star f \star v \cdot \beta = q'$ and $p' - q' = p - q - u \star f \star v \cdot \beta = h$.
2. Since $p \stackrel{*}{\longrightarrow}_F o$, $\mathsf{HM}(p) = \alpha \cdot t$ must be F-reducible. Let $f_i \in F$, $i \in I$ be a series of all not necessarily different polynomials in F such that $\alpha \cdot t$ is reducible by them involving terms u_i, v_i. Then $\mathsf{HC}(u_i \star f_i \star v_i) > 0$. Moreover, let $\gamma = \min_{\leq}\{\mathsf{HC}(u_i \star f_i \star v_i) \mid i \in I\}$ and without loss of generality $\mathsf{HM}(u \star f \star v) = \gamma \cdot t$ for some $f \in F$, $\mathsf{HT}(u \star \mathsf{HT}(f) \star v) = \mathsf{HT}(u \star f \star v) \geq \mathsf{HT}(f)$. We claim that for $p \longrightarrow_f p - \beta \cdot u \star f \star v = p'$ where $\alpha = \beta \cdot \gamma + \delta$, $\beta, \delta \in \mathbb{Z}$, $0 \leq \delta < \gamma$, we have $t \notin \mathsf{supp}(p')$. Suppose $\mathsf{HT}(p') = t$. Then by our definition of reduction we must have $0 < \mathsf{HC}(p') < \mathsf{HC}(u \star f \star v)$. But then p' would no longer be F-reducible contradicting our assumption that o is the unique normal form of p.

3. Since o is the unique normal form of $p - q$ by 2. there exists a reduction sequence $p - q \longrightarrow_{f_{i_1}} h_1 \longrightarrow_{f_{i_2}} h_2 \longrightarrow_{f_{i_3}} \ldots \longrightarrow_{f_{i_k}} o$ such that $\mathsf{HT}(p-q) \succ \mathsf{HT}(h_1) \succ \mathsf{HT}(h_2) \succ \ldots$. We show our claim by induction on k, where $p - q \stackrel{k}{\longrightarrow}_F o$ is such a reduction sequence. In the base case $k = 0$ there is nothing to show as then $p = q$. Hence, let $p - q \longrightarrow_F h \stackrel{k}{\longrightarrow}_F o$. Then by 1. there are polynomials $p', q' \in \mathcal{F}_{\mathbb{Z}}$ such that $p \stackrel{*}{\longrightarrow}_F p'$ and $q \stackrel{*}{\longrightarrow}_F q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \stackrel{k}{\longrightarrow}_F o$ yields the existence of a polynomial $g \in \mathcal{F}_{\mathbb{Z}}$ such that $p \stackrel{*}{\longrightarrow}_F g$ and $q \stackrel{*}{\longrightarrow}_F g$.

q.e.d.

Hence weak Gröbner bases are in fact Gröbner bases and can hence be characterized as follows (compare Definition 4.2.10):

Definition 4.4.44
A set $F \subseteq \mathcal{F}_{\mathbb{Z}} \backslash \{o\}$ is called a (weak) Gröbner basis of $\mathsf{ideal}(F)$ if for all $g \in \mathsf{ideal}(F)$ we have $g \stackrel{*}{\longrightarrow}_F o$. $\diamond$

Corollary 4.4.45
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}}$ and g a non-zero polynomial in $\mathsf{ideal}(F)$ such that $g \stackrel{*}{\longrightarrow}_F o$. Then g has a representation of the form

$$g = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}}), n \in \mathbb{N}$$

such that $\mathsf{HT}(g) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$, $1 \leq i \leq k$, and $\mathsf{HT}(g) \succ \mathsf{HT}(m_i \star f_i \star l_i) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i)$ for all $k+1 \leq i \leq n$.
In case o is the unique normal form of g with respect to F we even can find a representation where additionally $\mathsf{HT}(m_1 \star f_1 \star l_1) \succ \mathsf{HT}(m_2 \star f_2 \star l_2) \succ \ldots \succ \mathsf{HT}(m_n \star f_n \star l_n)$.

Proof :
We show our claim by induction on n where $g \stackrel{n}{\longrightarrow}_F o$. If $n = 0$ we are done. Else let $g \stackrel{1}{\longrightarrow}_F g_1 \stackrel{n}{\longrightarrow}_F o$. In case the reduction step takes place at the head monomial, there exists a polynomial $f \in F$ and $u, v \in \mathsf{T}(\mathcal{F}_{\mathbb{Z}}), \beta \in \mathbb{Z}$ such that $\mathsf{HT}(u \star \mathsf{HT}(f) \star v) = \mathsf{HT}(u \star f \star v) = \mathsf{HT}(g) \geq \mathsf{HT}(f)$ and $\mathsf{HC}(g) \Longrightarrow_{\mathsf{HC}(u \star f \star v)} \delta$ with $\mathsf{HC}(g) = \mathsf{HC}(u \star f \star v) \cdot \beta + \delta$ for some $\beta, \delta \in \mathbb{Z}$, $0 \leq \delta < \mathsf{HC}(u \star f \star v)$. Moreover the induction hypothesis then is applied to $g_1 = g - u \star f \star v \cdot \beta$. If the reduction step takes place at a monomial with term smaller $\mathsf{HT}(g)$ for the respective monomial multiple $u \star f \star v \cdot \beta$ we immediately get $\mathsf{HT}(g) \succ u \star f \star v \cdot \beta$ and we can apply our induction hypothesis to the resulting polynomial g_1. In

both cases we can arrange the monomial multiples $u \star f \star v \cdot \beta$ arising from the reduction steps in such a way that gives us the desired representation.

q.e.d.

Now Gröbner bases can be characterized using the concept of s-polynomials combined with the technique of saturation which is neccessary in order to describe the whole ideal congruence by the reduction relation.

Definition 4.4.46
Let p_1, p_2 be polynomials in $\mathcal{F}_{\mathbb{Z}}$. If there are respective terms $t, u_1, u_2, v_1, v_2 \in \mathcal{T}$ such that $\mathsf{HT}(u_i \star \mathsf{HT}(p_i) \star v_i) = \mathsf{HT}(u_i \star p_i \star v_i) = t \geq \mathsf{HT}(p_i)$ let $HC(u_i \star p_i \star v_i) = \gamma_i$. Assuming $\gamma_1 \geq \gamma_2 > 0$[58], there are $\beta, \delta \in \mathbb{Z}$ such that $\gamma_1 = \gamma_2 \cdot \beta + \delta$ and $0 \leq \delta < \gamma_2$ and we get the following s-polynomial

$$\mathsf{spol}(p_1, p_2, t, u_1, u_2, v_1, v_2) = u_2 \star p_2 \star v_2 \cdot \beta - u_1 \star p_1 \star v_1.$$

The set $\mathsf{SPOL}(\{p_1, p_2\})$ then is the set of all such s-polynomials corresponding to p_1 and p_2. $\diamond$

Again these sets in general are not finite.

Theorem 4.4.47
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}} \backslash \{o\}$. Then F is a Gröbner basis if and only if

1. *for all f in F and for all m, l in $\mathsf{M}(\mathcal{F}_{\mathbb{Z}})$ we have $m \star f \star l \xrightarrow{*}_F o$, and*
2. *all s-polynomials corresponding to F as specified in Definition 4.4.46 reduce to o using F.*

Proof :
In case F is a Gröbner basis, since these polynomials are all elements of $\mathsf{ideal}(F)$ they must reduce to zero using F.
The converse will be proven by showing that every element in $\mathsf{ideal}(F)$ is reducible by F. Then as $g \in \mathsf{ideal}(F)$ and $g \longrightarrow_F g'$ implies $g' \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}_F o$. Notice that this is sufficient as the reduction relation $\longrightarrow_F$ is Noetherian.
Let $g \in \mathsf{ideal}(F)$ have a representation in terms of F of the following form: $g = \sum_{j=1}^{n} v_j \star f_j \star w_j \cdot \alpha_j$ such that $f_j \in F$, $v_j, w_j \in \mathcal{T}$ and $\alpha_j \in \mathbb{Z}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{T}$ we define $t = \max_{\succeq}\{\mathsf{HT}(v_j \star f_j \star w_j) \mid 1 \leq j \leq m\}$, K as the number of polynomials $f_j \star w_j$ with head term t, and $M = \{\{\mathsf{HC}(v_j \star f_j \star w_j) \mid \mathsf{HT}(v_j \star f_j \star w_j) = t\}\}$ a multiset

[58]Notice that $\gamma_i > 0$ can always be achieved by studying the situation for $-p_i$ in case we have $HC(u_i \star p_i \star v_i) < 0$.

in $\mathbb{Z}$. We show our claim by induction on (t, M), where $(t', M') < (t, M)$ if and only if $t' \prec t$ or ($t' = t$ and $M' \ll M$).
Since by our first assumption every multiple $v_j \star f_j \star w_j$ in this sum reduces to zero using F and hence has a representation as specified in Corollary 4.4.45, we can assume that $\mathsf{HT}(v_j \star \mathsf{HT}(f_j) \star w_j) = \mathsf{HT}(v_j \star f_j \star w_j) \geq \mathsf{HT}(f_j)$ holds. Moreover, without loss of generality we can assume that the polynomial multiples with head term t are just $v_1 \star f_1 \star w_1, \ldots, v_K \star f_K \star w_K$ and additionally we can assume $\mathsf{HC}(v_j \star f_j \star w_j) > 0$[59].
Obviously, $t \succeq \mathsf{HT}(g)$ must hold. If $K = 1$ this gives us $t = \mathsf{HT}(g)$ and even $\mathsf{HM}(g) = \mathsf{HM}(v_1 \star f_1 \star w_1 \cdot \alpha_1)$, implying that g is right reducible at $\mathsf{HM}(g)$ by f_1. Hence let us assume $K > 1$.
Without loss of generality we can assume that $\mathsf{HC}(v_1 \star f_1 \star w_1) \geq \mathsf{HC}(v_2 \star f_2 \star w_2) > 0$ and there are $\alpha, \beta \in \mathbb{Z}$ such that $\mathsf{HC}(v_2 \star f_2 \star w_2) \cdot \alpha + \beta = \mathsf{HC}(v_1 \star f_1 \star w_1)$ and $\mathsf{HC}(v_2 \star f_2 \star w_2) > \beta \geq 0$. Since $t = \mathsf{HT}(v_1 \star f_1 \star w_1) = \mathsf{HT}(v_2 \star f_2 \star w_2)$ by Definition 4.4.46 we have an s-polynomial $\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2) = v_2 \star f_2 \star w_2 \cdot \alpha - v_1 \star f_1 \star w_1$.
If $\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2) \neq o$[60] then $\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2) \xrightarrow{*}_F o$ implies $\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2) = \sum_{i=1}^{k} m_i \star h_i \star l_i$, $h_i \in F$, $m_i, l_i \in \mathsf{M}(\mathcal{F}_\mathbb{Z})$ where this sum is a representation in the sense of Corollary 4.4.45 with terms bounded by $\mathsf{HT}(\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2)) \leq t$. This gives us

$$
\begin{aligned}
& v_1 \star f_1 \star w_1 \cdot \alpha_1 + v_2 \star f_2 \star w_2 \cdot \alpha_2 \qquad (4.8)\\
= \; & v_1 \star f_1 \star w_1 \cdot \alpha_1 + \underbrace{v_2 \star f_2 \star w_2 \cdot \alpha_1 \cdot \alpha - v_2 \star f_2 \star w_2 \cdot \alpha_1 \cdot \alpha}_{=o} + v_2 \star f_2 \star w_2 \cdot \alpha_2 \\
= \; & v_2 \star f_2 \star w_2 \cdot (\alpha_1 \cdot \alpha + \alpha_2) - \underbrace{(v_2 \star f_2 \star w_2 \cdot \alpha - v_1 \star f_1 \star w_1)}_{=\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2)} \cdot \alpha_1 \\
= \; & v_2 \star f_2 \star w_2 \cdot (\alpha_1 \cdot \alpha + \alpha_2) - (\sum_{i=1}^{k} m_i \star h_i \star l_i) \cdot \alpha_1
\end{aligned}
$$

and substituting this in the representation of g we get a new representation with $t' = \max_{\succeq}\{\mathsf{HT}(v_j \star f_j \star w_j), \mathsf{HT}(m_j \star h_j \star l_j) \mid f_j, h_j$ appearing in the new representation $\}$, and $M' = \{\{\mathsf{HC}(v_j \star f_j \star w_j), \mathsf{HC}(m_j \star h_j \star l_j) \mid \mathsf{HT}(v_j \star f_j \star w_j) = \mathsf{HT}(m_j \star h_j \star l_j) = t'\}\}$ and either $t' \prec t$ and we have a smaller representation for g or in case $t' = t$ we have to distinguish two cases:

1. $\alpha_1 \cdot \alpha + \alpha_2 = 0$.
   Then $M' = (M - \{\{\mathsf{HC}(v_1 \star f_1 \star w_1), \mathsf{HC}(v_2 \star f_2 \star w_2)\}\}) \cup \{\{\mathsf{HC}(m_j \star h_j \star l_j) \mid$

[59] This can easily be achieved by adding $-f$ to F for all $f \in F$ and using $v_j \star (-f_j) \star w_j \cdot (-\alpha_j)$ in case $\mathsf{HC}(v_j \star f_j \star w_j) < 0$.

[60] In case $\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2) = o$ the proof is similar. We just have to subsitute o in the equations below which immediately gives us a smaller representation of g.

$\mathsf{HT}(m_j \star h_j \star l_j) = t\}\}$. As those polynomials h_j with $\mathsf{HT}(m_j \star h_j \star l_j) = t$ are used to reduce the monomial $\beta \cdot t = \mathsf{HM}(\mathsf{spol}(f_1, f_2, t, v_1, v_2, w_1, w_2))$ we know that for them we have $0 < \mathsf{HC}(m_j \star h_j \star l_j) \leq \beta < \mathsf{HC}(v_2 \star f_2 \star w_2) \leq \mathsf{HC}(v_1 \star f_1 \star w_1)$ and hence $M' \ll M$ and we have a smaller representation for g.

2. $\alpha_1 \cdot \alpha + \alpha_2 \neq 0$.
   Then $M' = (M - \{\{\mathsf{HC}(v_1 \star f_1 \star w_1)\}\}) \cup \{\{\mathsf{HC}(m_j \star h_j \star l_j) \mid \mathsf{HT}(m_j \star h_j \star l_j) = t\}\}$. Again $M' \ll M$ and we have a smaller representation for g.

Notice that the case $t' = t$ and $M' \ll M$ cannot occur infinitely often but has to result in either $t' < t$ or will lead to $t' = t$ and $K = 1$ and hence to reducibility by $\longrightarrow_F$.

q.e.d.

Now the question arises when the critical situations in this characterization can be localized to subsets of the respective sets as in Theorem 4.4.31. Reviewing the Proof of Theorem 4.4.31 we find that Lemma 4.4.16 is central as it describes when multiples of polynomials which have a reductive standard representation in terms of some set F again have such a representation. As we have seen before, this will not hold for function rings over reduction rings in general. As in Section 4.4.2, to give localizations of Theorem 4.4.47 the concept of stable subsets is sufficient:

Definition 4.4.48
A set $C \subset S \subseteq \mathcal{F}_{\mathbb{Z}}$ is called a **stable localization** of S if for every $g \in S$ there exists $f \in C$ such that $g \longrightarrow_f o$. $\diamond$

In case $\mathcal{F}_{\mathbb{Z}}$ and $\longrightarrow$ allow such stable localizations, we can rephrase Theorem 4.4.47 as follows:

Theorem 4.4.49
Let F be a set of polynomials in $\mathcal{F}_{\mathbb{Z}} \backslash \{o\}$. Then F is a Gröbner basis of $\mathsf{ideal}(F)$ *if and only if*

1. *for all s in a stable localization of $\{m \star f \star l \mid f \in \mathcal{F}_{\mathbb{Z}}, m, l \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}})\}$ we have $s \xrightarrow{*}_F o$, and*

2. *for all h in a stable localization of the s-polynomials corresponding to F as specified in Definition 4.4.46 we have $h \xrightarrow{*}_F o$.*

When proving Theorem 4.4.49, we can substitute the critical situation using an analogon of Lemma 4.4.16, which will be sufficient to make the representation used in the proof smaller. It is a direct consequence of Lemma 4.4.40.

Corollary 4.4.50
Let $F \subseteq \mathcal{F}_{\mathbb{Z}} \backslash \{o\}$ and f, p non-zero polynomials in $\mathcal{F}_{\mathbb{Z}}$. If $p \longrightarrow_f o$ and $f \xrightarrow{*}_F o$, then p has a representation of the form

$$p = \sum_{i=1}^{n} m_i \star f_i \star l_i, f_i \in F, m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}}), n \in \mathbb{N}$$

such that $\mathsf{HT}(p) = \mathsf{HT}(m_i \star \mathsf{HT}(f_i) \star l_i) = \mathsf{HT}(m_i \star f_i \star l_i) \geq \mathsf{HT}(f_i)$ for $1 \leq i \leq k$ and $\mathsf{HT}(p) \succ \mathsf{HT}(m_i \star f_i \star l_i)$ for all $k+1 \leq i \leq n$.

Proof Theorem 4.4.49:
The proof is basically the same as for Theorem 4.4.47. Due to Corollary 4.4.50 we can substitute the multiples $v_j \star f_j \star w_j$ by appropriate representations. Hence, we only have to ensure that despite testing less polynomials we are able to apply our induction hypothesis. Taking the notations from the proof of Theorem 4.4.47, let us check the situation for $K > 1$.
Without loss of generality we can assume that $\mathsf{HC}(v_1 \star f_1 \star w_1) \geq \mathsf{HC}(v_2 \star f_2 \star w_2) > 0$ and there are $\alpha, \beta \in \mathbb{Z}$ such that $\mathsf{HC}(v_2 \star f_2 \star w_2) \cdot \alpha + \beta = \mathsf{HC}(v_1 \star f_1 \star w_1)$ and $\mathsf{HC}(v_2 \star f_2 \star w_2) > \beta \geq 0$. Since $t = \mathsf{HT}(v_1 \star f_1 \star w_1) = \mathsf{HT}(v_2 \star f_2 \star w_2)$ by Definition 4.4.46 we have an s-polynomial h in the stable localization of $\mathsf{SPOL}(f_1, f_2)$ such that $v_2 \star f_2 \star w_2 \cdot \alpha - v_1 \star f_1 \star w_1 \longrightarrow_h o$. If $h \neq o$[61] then by Corollary 4.4.50 $h \xrightarrow{*}_F o$ implies $v_2 \star f_2 \star w_2 \cdot \alpha - v_1 \star f_1 \star w_1 = \sum_{i=1}^{k} m_i \star h_i \star l_i$, $h_i \in F$, $m_i, l_i \in \mathsf{M}(\mathcal{F}_{\mathbb{Z}})$ where this sum is a representation in the sense of Corollary 4.4.45 with terms bounded by $\mathsf{HT}(m \star h \star l) \leq t$. This gives us

$$\begin{aligned}
& v_1 \star f_1 \star w_1 \cdot \alpha_1 + v_2 \star f_2 \star w_2 \cdot \alpha_2 && (4.9)\\
= \; & v_1 \star f_1 \star w_1 \cdot \alpha_1 + \underbrace{v_2 \star f_2 \star w_2 \cdot \alpha_1 \cdot \alpha - v_2 \star f_2 \star w_2 \cdot \alpha_1 \cdot \alpha}_{=o} + v_2 \star f_2 \star w_2 \cdot \alpha_2 \\
= \; & v_2 \star f_2 \star w_2 \cdot (\alpha_1 \cdot \alpha + \alpha_2) - (v_2 \star f_2 \star w_2 \cdot \alpha - v_1 \star f_1 \star w_1) \cdot \alpha_1 \\
= \; & v_2 \star f_2 \star w_2 \cdot (\alpha_1 \cdot \alpha + \alpha_2) - (\sum_{i=1}^{k} m_i \star h_i \star l_i) \cdot \alpha_1
\end{aligned}$$

and substituting this in the representation of g we get a new representation with $t' = \max_{\succeq}\{\mathsf{HT}(v_j \star f_j \star w_j), \mathsf{HT}(m_j \star h_j \star l_j) \mid f_j, h_j \text{ appearing in the new representation }\}$, and $M' = \{\{\mathsf{HC}(v_j \star f_j \star w_j), \mathsf{HC}(m_j \star h_j \star l_j) \mid \mathsf{HT}(v_j \star f_j \star w_j) = \mathsf{HT}(m_j \star h_j \star l_j) = t'\}\}$ and either $t' \prec t$ or ($t' = t$ and $M' \ll M$) and in both cases we have a smaller representation for g. Notice that the case $t' = t$ and $M' \ll M$ cannot occur infinitely often but has to result in either $t' < t$ or will lead to $t' = t$ and $K = 1$ and hence to

[61] In case $h = o$ the proof is similar. We just have to subsitute o in the equations below which immediately gives us a smaller representation of g.

reducibility by $\longrightarrow_F$.

q.e.d.

4.5 Two-sided Modules

Given a function ring $\mathcal{F}$ with unit $\mathbf{1}$ and a natural number k, let $\mathcal{F}^k = \{(f_1, \dots, f_k) \mid f_i \in \mathcal{F}\}$ be the set of all vectors of length k with coordinates in $\mathcal{F}$. Obviously $\mathcal{F}^k$ is an additive commutative group with respect to ordinary vector addition. Moreover, $\mathcal{F}^k$ is such an **$\mathcal{F}$-module** with respect to the scalar multiplication $f \star (f_1, \dots, f_k) = (f \star f_1, \dots, f \star f_k)$ and $(f_1, \dots, f_k) \star f = (f_1 \star f, \dots, f_k \star f)$. Additionally $\mathcal{F}^k$ is called **free** as it has a basis[62]. One such basis is the set of unit vectors $\mathbf{e}_1 = (\mathbf{1}, o, \dots, o), \mathbf{e}_2 = (o, \mathbf{1}, o, \dots, o), \dots, \mathbf{e}_k = (o, \dots, o, \mathbf{1})$. Using this basis the elements of $\mathcal{F}^k$ can be written uniquely as $\mathbf{f} = \sum_{i=1}^{k} f_i \star \mathbf{e}_i$ where $\mathbf{f} = (f_1, \dots, f_k)$.

Definition 4.5.1
A subset of $\mathcal{F}^k$ which is again an $\mathcal{F}$-module is called a **submodule** of $\mathcal{F}^k$.

As before any ideal of $\mathcal{F}$ is an $\mathcal{F}$-module and even a submodule of the $\mathcal{F}$-module $\mathcal{F}^1$. Provided a set of vectors $S = \{\mathbf{f}_1, \dots, \mathbf{f}_s\}$ the set $\{\sum_{i=1}^{s} \sum_{j=1}^{n_i} g_{ij} \star \mathbf{f}_i \star h_{ij} \mid g_{ij}, h_{ij} \in \mathcal{F}\}$ is a submodule of $\mathcal{F}^k$. This set is denoted as $\langle S \rangle$ and S is called a generating set.

Theorem 4.5.2
Let $\mathcal{F}$ be Noetherian. Then every submodule of $\mathcal{F}^k$ is finitely generated.

Proof :
Let $\mathcal{S}$ be a submodule of $\mathcal{F}^k$. Again we show our claim by induction on k. For $k = 1$ we find that $\mathcal{S}$ is in fact an ideal in $\mathcal{F}$ and hence by our hypothesis finitely generated. For $k > 1$ let us look at the set $I = \{f_1 \mid (f_1, \dots, f_k) \in \mathcal{S}\}$. Then again I is an ideal in $\mathcal{F}$ and hence finitely generated. Let $\{g_1, \dots, g_s \mid g_i \in \mathcal{F}\}$ be a generating set of I. Choose $\mathbf{g}_1, \dots, \mathbf{g}_s \in \mathcal{S}$ such that the first coordinate of $\mathbf{g}_i$ is g_i. Note that the set $\{(f_2, \dots, f_k) \mid (o, f_2, \dots, f_k) \in \mathcal{S}\}$ is a submodule of $\mathcal{F}^{k-1}$ and hence finitely generated by some set $\{(n_2^i, \dots, n_k^i), 1 \le i \le w\}$. Then the set $\{\mathbf{g}_1, \dots, \mathbf{g}_s\} \cup \{\mathbf{n}_i = (o, n_2^i, \dots, n_k^i) \mid 1 \le i \le w\}$ is a generating set for $\mathcal{S}$. To see this assume $\mathbf{m} = (m_1, \dots, m_k) \in \mathcal{S}$. Then $m_1 = \sum_{i=1}^{s} \sum_{j=1}^{n_i} h_{ij} \star g_i \star h_{ij}'$ for some

[62] Here the term *basis* is used in the meaning of being a linearly independent set of generating vectors.

$h_{ij}, h_{ij}{}' \in \mathcal{F}$ and $\mathbf{m}' = \mathbf{m} - \sum_{i=1}^{s}\sum_{j=1}^{n_i} h_{ij} \star \mathbf{g}_i \star h_{ij}{}' \in \mathcal{S}$ with first coordinate o. Hence $\mathbf{m}' = \sum_{i=1}^{w}\sum_{j=1}^{m_i} l_{ij} \star \mathbf{n}_i \star l_{ij}{}'$ for some $l_{ij}, l_{ij}{}' \in \mathcal{F}$ giving rise to

$$\mathbf{m} = \mathbf{m}' + \sum_{i=1}^{s}\sum_{j=1}^{n_i} h_{ij} \star \mathbf{g}_i \star h_{ij}{}' = \sum_{i=1}^{w}\sum_{j=1}^{m_i} l_{ij} \star \mathbf{n}_i \star l_{ij}{}' + \sum_{i=1}^{s}\sum_{j=1}^{n_i} h_{ij} \star \mathbf{g}_i \star h_{ij}{}'.$$

q.e.d.

$\mathcal{F}^k$ is called Noetherian if and only if all its submodules are finitely generated.

If $\mathcal{F}$ is a reduction ring Section 4.5 outlines how the existence of Gröbner bases for submodules can be shown.

Now given a submodule $\mathcal{S}$ of $\mathcal{F}^k$, we can define $\mathcal{F}^k/\mathcal{S} = \{\mathbf{f} + \mathcal{S} \mid \mathbf{f} \in \mathcal{F}^k\}$. Then with addition defined as $(\mathbf{f}+\mathcal{S})+(\mathbf{g}+\mathcal{S}) = (\mathbf{f}+\mathbf{g})+\mathcal{S}$ the set $\mathcal{F}^k/\mathcal{S}$ is an abelian group and can be turned into an $\mathcal{F}$-module by the action $g\star(\mathbf{f}+\mathcal{S})\star h = g\star\mathbf{f}\star h+\mathcal{S}$ for $g, h \in \mathcal{F}$. $\mathcal{F}^k/\mathcal{S}$ is called the **quotient module** of $\mathcal{F}^k$ by $\mathcal{S}$.

As usual this quotient can be related to homomorphisms. The results carry over from commutative module theory as can be found in [AL94]. Recall that for two $\mathcal{F}$-modules $\mathcal{M}$ and $\mathcal{N}$, a function $\phi : \mathcal{M} \longrightarrow \mathcal{N}$ is an $\mathcal{F}$-module homomorphism if

$$\phi(\mathbf{f} + \mathbf{g}) = \phi(\mathbf{f}) + \phi(\mathbf{g}) \text{ for all } \mathbf{f}, \mathbf{g} \in \mathcal{M}$$

and

$$\phi(g \star \mathbf{f} \star h) = g \star \phi(\mathbf{f}) \star h \text{ for all } \mathbf{f} \in \mathcal{M}, g, h \in \mathcal{F}.$$

The homomorphism is called an **isomorphism** if ϕ is one to one and we write $\mathcal{M} \cong \mathcal{N}$. Let $\mathcal{S} = \ker(\phi) = \{\mathbf{f} \in \mathcal{M} \mid \phi(\mathbf{f}) = \mathbf{0}\}$. Then $\mathcal{S}$ is a submodule of $\mathcal{M}$ and $\phi(\mathcal{M})$ is a submodule of $\mathcal{N}$. Since all are abelian groups we know $\mathcal{M}/\mathcal{S} \cong \phi(\mathcal{M})$ under the mapping $\mathcal{M}/\mathcal{S} \longrightarrow \phi(\mathcal{M})$ with $\mathbf{f} + \mathcal{S} \mapsto \phi(\mathbf{f})$ which is in fact an isomorphism. All submodules of the quotient $\mathcal{M}/\mathcal{S}$ are of the form $\mathcal{L}/\mathcal{S}$ where $\mathcal{L}$ is a submodule of $\mathcal{M}$ containing $\mathcal{S}$.

Unfortunately, contrary to the one-sided case we can no longer show that every finitely generated $\mathcal{F}$-module $\mathcal{M}$ is isomorphic to some quotient of $\mathcal{F}^k$. Let $\mathcal{M}$ be a finitely generated $\mathcal{F}$-module with generating set $\mathbf{f}_1, \ldots \mathbf{f}_k \in \mathcal{M}$. Consider the mapping $\phi : \mathcal{F}^k \longrightarrow \mathcal{M}$ defined by $\phi(g_1, \ldots, g_k) = \sum_{i=1}^{k} g_i \star \mathbf{f}_i$ for $\mathcal{M}$. The image of the $\mathcal{F}$-module homomorphis is no longer $\mathcal{M}$.

Chapter 5

Applications of Gröbner Bases

In this chapter we outline how the concept of Gröbner bases can be used to describe algebraic questions and when solutions can be achieved. We will describe the problems in the following manner

Problem

Given:	A description of the algebraic setting of the problem.
Problem:	A description of the problem itself.
Proceeding:	A description of how the problem can be analyzed using Gröbner bases.

In a first step we do not require finiteness or computability of the operations, especially of a Gröbner basis. Since an ideal itself is always a Gröbner basis itself, the assumption "Let G be a respective Gröbner basis" always holds and means a Gröbner basis of the ideal generated by G.

In case a Gröbner basis is computable (though not necessarily finite) and the normal form computation for a polynomial with respect to a finite set is effective, our so-called proceedings give rise to procedures which can then be used to treat the problem in a constructive manner. If additionally the Gröbner basis computation terminates, these procedures terminate as well and the instance of the problem is decidable. In case Gröbner basis computation always terminates for a chosen setting the whole problem is decidable in this setting.

Of course "termination" here is meant in a theoretical sense while as we know practical "termination" is already often not achievable for the Gröbner basis computation in the ordinary polynomial ring due to complexity issues although finite Gröbner bases always exist.

The terminology extends to one-sided ideals and we note those problems, where the one-sided case also makes sense.

We will also note when weak Gröbner bases are sufficient for the solution of a problem.

5.1 Natural Applications

The most obvious problem related to Gröbner bases is the ideal membership problem. Characterizing Gröbner bases with respect to a reduction relation uses the important fact that an element belonging to the ideal will reduce to zero using the Gröbner basis.

Ideal Membership Problem

Given:		A set $F \subseteq \mathcal{F}$ and an element $f \in \mathcal{F}$.
Problem:		$f \in \mathsf{ideal}(F)$?
Proceeding:	1.	Let G be a Gröbner basis of $\mathsf{ideal}(F)$.
	2.	If $f \xrightarrow{*}_G o$, then $f \in \mathsf{ideal}(F)$.

Hence Gröbner bases give a semi-answer to this question in case they are computable and the normal form computation is effective. To give a negative answer the Gröbner basis computation must either terminate or one must explicitly prove, e.g. using properties of the enumerated Gröbner basis, that the element will never reduce to zero.

These results carry over to one-sided ideals using the appropriate one-sided Gröbner bases.

Moreover, weak Gröbner bases are sufficient to solve the problem.

A normal form computation always gives rise to a special representation in terms of the polynomials used for reduction and in case the normal form is zero such representations are special standard representations. We give two instances of this problem.

Representation Problem 1

Given:	A Gröbner basis $G \subseteq \mathcal{F}$ and an element $f \in \mathsf{ideal}(G)$.
Problem:	Give a representation of f in terms of G.
Proceeding:	Reducing f to o using G yields such a representation.

In case the normal form computation is effective, we can collect the polynomials and multiples used in the reduction process and combine them to the desired representation. Notice that since we know that the element is in the ideal, it is enough to additionally require that the Gröbner basis is recursively enumerable as a set.

The result carries over to one-sided ideals using the appropriate one-sided Gröbner bases.

Again, weak Gröbner bases are sufficient to solve the problem.

Often the ideal is not presented in terms of a Gröbner basis. Then additional information is necessary which in the computational case is related to collecting the history of polynomials created during completion. Notice that the proceedings in this case require some equivalent to Lemma 4.4.16 to hold and hence the problem is restricted to function rings over fields.

Representation Problem 2

Given: A set $F \subseteq \mathcal{F}_{\mathbb{K}}$ and an element $f \in \mathsf{ideal}(F)$.

Problem: Give a representation of f in terms of F.

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}(F)$.
2. Let $g = \sum_{i=1}^{k_g} m_i \star f_i \star \tilde{m}_i$ be representations of the elements $g \in G$ in terms of F.
3. Let $f = \sum_{j=1}^{k} n_i \star g_i \star \tilde{n}_i$ be a representation of f in terms of G.
4. The sums in 2. and 3. yield a representation of f in terms of F.

In case the Gröbner basis is computable by a completion procedure the procedure has to keep track of the history of polynomials by storing their representations in terms of F. If the completion stops we can reduce f to zero and substitute the representations of the polynomials used by their "history representation". If the Gröbner basis is only recursively enumerable both processes have to be interwoven and to continue until the normal form computation for f reaches o.

The result carries over to one-sided ideals using the appropriate one-sided Gröbner bases.

Moreover, weak Gröbner bases are sufficient to solve the problem.

Other problems are related to the comparison of ideals. For example given two ideals one can ask whether one is included in the other.

Ideal Inclusion Problem

Given: Two sets $F_1, F_2 \subseteq \mathcal{F}$.

Problem: $\mathsf{ideal}(F_1) \subseteq \mathsf{ideal}(F_2)$?

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}(F_2)$.
2. If $F_1 \xrightarrow{*}_G o$, then $\mathsf{ideal}(F_1) \subseteq \mathsf{ideal}(F_2)$.

In case the Gröbner basis is computable and the normal form computation is effective this yields a semi-decision procedure for the problem. If additionally the Gröbner basis computation terminates for F_1 or we can prove that some element of the set F_1 does not belong to $\mathsf{ideal}(F_2)$, e.g. by deriving knowledge from the enumerated Gröbner basis, we can also give a negative answer.

The result carries over to one-sided ideals using the appropriate one-sided Gröbner bases.

Weak Gröbner bases are sufficient to solve the problem.

Applying the inclusion problem in both directions we get a characterization for equality of ideals.

Ideal Equality Problem

Given: Two sets $F_1, F_2 \subseteq \mathcal{F}$.

Problem: $\mathsf{ideal}(F_1) = \mathsf{ideal}(F_2)$?

Proceeding:

1. Let G_1, G_2 be Gröbner bases of $\mathsf{ideal}(F_1)$ respectively $\mathsf{ideal}(F_2)$.
2. If $F_1 \xrightarrow{*}_{G_2} o$, then $\mathsf{ideal}(F_1) \subseteq \mathsf{ideal}(F_2)$.
3. If $F_2 \xrightarrow{*}_{G_1} o$, then $\mathsf{ideal}(F_2) \subseteq \mathsf{ideal}(F_1)$.
4. If 2. and 3. both hold, then $\mathsf{ideal}(F_1) = \mathsf{ideal}(F_2)$.

Again, Gröbner bases at least give a semi-answer in case they are computable and the normal form procedure is effective. We can confirm whether two generating sets are bases of one ideal. Of course, in case the computed Gröbner bases are finite, we can also give a negative answer. However, if the Gröbner bases are not finite, a negative answer is only possible, if we can prove either $F_1 \not\subseteq \mathsf{ideal}(F_2)$ or $F_2 \not\subseteq \mathsf{ideal}(F_1)$.

The result carries over to one-sided ideals using the appropriate one-sided Gröbner bases.

Again, weak Gröbner bases are sufficient to solve the problem.

In case $\mathcal{F}$ contains a unit say $\mathbf{1}$, we can ask whether an ideal is equal to the trivial ideal in $\mathcal{F}$ generated by the unit.

Ideal Triviality Problem 1

Given: A set $F \subseteq \mathcal{F}$.

Problem: $\mathsf{ideal}(F) = \mathsf{ideal}(\{\mathbf{1}\})$?

Proceeding:

1. Let G be a respective Gröbner basis.
2. If $\mathbf{1} \xrightarrow{*}_{G} o$, then $\mathsf{ideal}(F) = \mathsf{ideal}(\{\mathbf{1}\})$.

Again Gröbner bases give a semi-answer in case they can be computed. If the Gröbner basis is additionally finite or we can prove that $\mathbf{1} \notin \mathsf{ideal}(F)$, then we can also confirm $\mathsf{ideal}(F) \neq \mathsf{ideal}(\{\mathbf{1}\})$.

Since $\mathsf{ideal}(\{1\}) = \mathcal{F}$ one can also rephrase the question for rings without a unit.

IDEAL TRIVIALITY PROBLEM 2

Given: A set $F \subseteq \mathcal{F}$.

Problem: $\mathsf{ideal}(F) = \mathcal{F}$?

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}(F)$.
2. If for every $t \in \mathcal{T}$, $t \xrightarrow{*}_G o$, then $\mathsf{ideal}(F) = \mathcal{F}$.

Of course now we have the problem that the test set $\mathcal{T}$ in general will not be finite. Hence a Gröbner basis can give a semi-answer in case we can restrict this test set to a finite subset. If the Gröbner basis is additionally finite or we can prove that $t \not\xrightarrow{*}_G o$ for some t in the finite sub test set of $\mathcal{T}$, then we can also confirm $\mathsf{ideal}(F) \neq \mathcal{F}$.

Both of these result carry over to one-sided ideals using the appropriate one-sided Gröbner bases.

As before, weak Gröbner bases are sufficient to solve the problem.

IDEAL UNION PROBLEM

Given: Two sets $F_1, F_2 \subseteq \mathcal{F}$ and an element $f \in \mathcal{F}$.

Problem: $f \in \mathsf{ideal}(F_1) \cup \mathsf{ideal}(F_2)$?

Proceeding:
1. Let G_1, G_2 be Gröbner bases of $\mathsf{ideal}(F_1)$ respectively $\mathsf{ideal}(F_2)$.
2. If $f \xrightarrow{*}_{G_1} o$, then $f \in \mathsf{ideal}(F_1) \cup \mathsf{ideal}(F_2)$.
3. If $f \xrightarrow{*}_{G_2} o$, then $f \in \mathsf{ideal}(F_1) \cup \mathsf{ideal}(F_2)$.

Notice that $\mathsf{ideal}(F_1) \cup \mathsf{ideal}(F_2) \neq \mathsf{ideal}(F_1 \cup F_2)$. Moreover $G_1 \cup G_2$ is neither a Gröbner basis of $\mathsf{ideal}(F_1) \cup \mathsf{ideal}(F_2)$, which in general is no ideal itself, nor of $\mathsf{ideal}(F_1 \cup F_2)$.

Again, weak Gröbner bases are sufficient to solve the problem.

The ideal generated by the set $F_1 \cup F_2$ is called the sum of the two ideals.

Definition 5.1.1
For two ideals $\mathfrak{i}, \mathfrak{j} \subseteq \mathcal{F}$ the **sum** is defined as the set

$$\mathfrak{i} + \mathfrak{j} = \{f \oplus g \mid f \in \mathfrak{i}, g \in \mathfrak{j}\}.$$

As in the case of commutative polynomials one can show the following theorem.

Theorem 5.1.2
For two ideals $\mathfrak{i}, \mathfrak{j} \subseteq \mathcal{F}$ the sum $\mathfrak{i} + \mathfrak{j}$ is again an ideal. In fact, it is the smallest ideal containing both, $\mathfrak{i}$ and $\mathfrak{j}$. If F and G are the respective generating sets for $\mathfrak{i}$ and $\mathfrak{j}$, then $F \cup G$ is a generating set for $\mathfrak{i} + \mathfrak{j}$.

Proof : First we check that the sum is indeed an ideal:

1. as $o \oplus o = o$ we get $o \in \mathfrak{i} + \mathfrak{j}$,
2. for $h_1, h_2 \in \mathfrak{i} + \mathfrak{j}$ we have that there are $f_1, f_2 \in \mathfrak{i}$ and $g_1, g_2 \in \mathfrak{j}$ such that $h_1 = f_1 \oplus g_1$ and $h_2 = f_2 \oplus g_2$. Then $h_1 \oplus h_2 = (f_1 \oplus g_1) \oplus (f_2 \oplus g_2) = (f_1 \oplus f_2) \oplus (g_1 \oplus g_2) \in \mathfrak{i} + \mathfrak{j}$, and
3. for $h_1 \in \mathfrak{i} + \mathfrak{j}$, $h_2 \in \mathcal{F}$ we have that there are $f \in \mathfrak{i}$ and $g \in \mathfrak{j}$ such that $h_1 = f \oplus g$. Then $h_1 \star h_2 = (f \oplus g) \star h_2 = f \star h_2 \oplus g \star h_2 \in \mathfrak{i} + \mathfrak{j}$ as well as $h_2 \star h_1 = h_2 \star (f \oplus g) = h_2 \star f \oplus h_2 \star g \in \mathfrak{i} + \mathfrak{j}$.

Since any ideal containing $\mathfrak{i}$ and $\mathfrak{j}$ contains $\mathfrak{i}+\mathfrak{j}$, this is the smallest ideal containing them. It is easy to see that $F \cup G$ is a generating set for the sum. q.e.d.

Of course $F \cup G$ in general will not be a Gröbner basis. This becomes immediately clear when looking at the following corollary.

Corollary 5.1.3
For $F \subseteq \mathcal{F}$ we have

$$\mathsf{ideal}(F) = \bigcup_{f \in F} \mathsf{ideal}(f).$$

But we have already seen that for function rings a polynomial in general is no Gröbner basis of the ideal or one-sided ideal it generates.

IDEAL SUM PROBLEM

Given:		Two sets $F_1, F_2 \subseteq \mathcal{F}$ and an element $f \in \mathcal{F}$.
Problem:		$f \in \mathsf{ideal}(F_1) + \mathsf{ideal}(F_2)$?
Proceeding:	1.	Let G be a Gröbner basis of $\mathsf{ideal}(F_1 \cup F_2)$.
	2.	If $f \xrightarrow{*}_G o$, then $f \in \mathsf{ideal}(F_1) + \mathsf{ideal}(F_2)$.

Both of these result carry over to one-sided ideals using the appropriate one-sided Gröbner bases.

As before, weak Gröbner bases are sufficient to solve the problem.

Similar to sums for commutative function rings we can define products of ideals.

Definition 5.1.4
For two ideals $\mathfrak{i}, \mathfrak{j}$ in a commutative function ring $\mathcal{F}$ the **product** is defined as the set

$$\langle \mathfrak{i} \star \mathfrak{j} \rangle = \mathsf{ideal}(\{f_i \star g_i \mid f_i \in \mathfrak{i}, g_i \in \mathfrak{j}\}).$$

$\diamond$

Theorem 5.1.5
For two ideals $\mathfrak{i}, \mathfrak{j}$ in a commutative function ring $\mathcal{F}$ the product $\langle \mathfrak{i} \star \mathfrak{j} \rangle$ is again an ideal. If F and G are the respective generating sets for $\mathfrak{i}$ and $\mathfrak{j}$, then $F \star G = \{f \star g \mid f \in F, g \in G\}$ is a generating set for $\mathfrak{i} \star \mathfrak{j}$.

Proof : First we check that the product is indeed an ideal:

1. as $o \in \mathfrak{i}$ and $o \in \mathfrak{j}$ we get $o \in \mathfrak{i} \star \mathfrak{j}$,
2. for $f, g \in \mathfrak{i} \star \mathfrak{j}$ we have $f \oplus g \in \mathfrak{i} \star \mathfrak{j}$ by our definition, and
3. for $f \in \mathfrak{i} \star \mathfrak{j}$, $h \in \mathcal{F}$ we have that there are $f_i \in \mathfrak{i}$ and $g_i \in \mathfrak{j}$ such that $f = \sum_{i=1}^{k} f_i \star g_i$ and then $f \star h = (\sum_{i=1}^{k} f_i \star g_i) \star h = \sum_{i=1}^{k} f_i \star (g_i \star h) \in \mathfrak{i} \star \mathfrak{j}$.

It is obvious that $\mathsf{ideal}(F \star G) \subseteq \langle \mathfrak{i} \star \mathfrak{j} \rangle$ as $F \star G \subseteq \mathfrak{i} \star \mathfrak{j}$. On the other hand every polynomial in $\langle \mathfrak{i} \star \mathfrak{j} \rangle$ can be written as a sum of products $\tilde{f} \star \tilde{g}$ where $\tilde{f} = \sum_{i=1}^{n} h_i \star f_i \in \mathfrak{i}$, $f_i \in F$, $h_i \in \mathcal{F}$ and $\tilde{g} = \sum_{j=1}^{m} g_j \star \tilde{h}_j$, $g_j \in G$, $\tilde{h}_j \in \mathcal{F}$. Hence every such product $\tilde{f} \star \tilde{g}$ is again of the desired form.

q.e.d.

Ideal Product Problem

Given:		Two subsets F_1, F_2 of a commutative function ring $\mathcal{F}$ and an element $f \in \mathcal{F}$.
Problem:		$f \in \langle \mathsf{ideal}(F_1) \star \mathsf{ideal}(F_2) \rangle$?
Proceeding:	1.	Let G be a Gröbner basis of $\mathsf{ideal}(F_1 \star F_2)$.
	2.	If $f \xrightarrow{*}_G o$, then $f \in \langle \mathsf{ideal}(F_1) \star \mathsf{ideal}(F_2) \rangle$.

Again, weak Gröbner bases are sufficient to solve the problem.

We close this section by showing how Gröbner bases can help to detect the existence of inverse elements in $\mathcal{F}$ in case $\mathcal{F}$ has a unit say $\mathbf{1}$.

Definition 5.1.6
Let $\mathcal{F}$ be a function ring with unit $\mathbf{1}$ and $f \in \mathcal{F}$. An element $g \in \mathcal{F}$ is called a **right inverse** of f in $\mathcal{F}$ if $f \star g = \mathbf{1}$. Similarly g is called a **left inverse** of f in $\mathcal{F}$ if $g \star f = \mathbf{1}$. $\diamond$

Inverse Element Problem

Given: An element $f \in \mathcal{F}$.

Problem: Does f have a right or left inverse in $\mathcal{F}$?

Proceeding: 1. Let G_r be a respective right Gröbner basis of $\mathsf{ideal}_r(f)$.

2. If $\mathbf{1} \xrightarrow{*}{}^{\mathrm{r}}_{G_r} o$, then f has a right inverse.

1'. Let G_ℓ be a respective left Gröbner basis of $\mathsf{ideal}_\ell(f)$.

2'. If $\mathbf{1} \xrightarrow{*}{}^{\mathrm{r}}_{G_\ell} o$, then f has a left inverse.

To see that this is correct we give the following argument for the right inverse case: It is clear that f has a right inverse in $\mathcal{F}$ if and only if $\mathsf{ideal}_r(\{f\}) = \mathcal{F}$ since $f \star g - \mathbf{1} = o$ for some $g \in \mathcal{F}$ if and only if $\mathbf{1} \in \mathsf{ideal}_r(\{f\})$. So, in order to decide whether f has a right inverse in $\mathcal{F}$ one has to distinguish the following two cases provided we have a right Gröbner basis G_r of $\mathsf{ideal}_r(\{f\})$: If $\mathbf{1} \not\xrightarrow{*}{}^{\mathrm{r}}_{G_r} o$ then f has no right inverse. If $\mathbf{1} \xrightarrow{*}{}^{\mathrm{r}}_{G_r} o$ then we know $\mathbf{1} \in \mathsf{ideal}_r(\{f\})$, i.e. there exist $h \in \mathcal{F}$ such that $\mathbf{1} = f \star h$ and hence h is a right inverse of f in $\mathcal{F}$.

A symmetric argument holds for the case of left inverses.

Of course in case $\mathcal{F}$ is commutative, left inverses and right inverses coincide in case they exist and we can use the fact that $f \star g - \mathbf{1} = g \star f - \mathbf{1} = o$ if and only if $\mathbf{1} \in \mathsf{ideal}(\{f\})$.

Again, weak Gröbner bases are sufficient to solve the problem.

It is also possible to ask for the existence of left and right inverses for elements of the quotient rings described in the next section.

5.2 Quotient Rings

Let F be a subset of $\mathcal{F}$ generating an ideal $\mathfrak{i} = \mathsf{ideal}(F)$. The canonical homomorphism from $\mathcal{F}$ onto $\mathcal{F}/\mathfrak{i}$ is defined as

$$f \longmapsto [f]_{\mathfrak{i}}$$

with $[f]_{\mathfrak{i}} = f + \mathfrak{i}$ denoting the congruence class of f modulo $\mathfrak{i}$. The ring operations are given by

$$[f]_{\mathfrak{i}} + [g]_{\mathfrak{i}} = [f+g]_{\mathfrak{i}},$$

$$[f]_{\mathfrak{i}} * [g]_{\mathfrak{i}} = [f \star g]_{\mathfrak{i}}.$$

A natural question now is whether two elements of $\mathcal{F}$ are in fact in the same congruence class modulo $\mathfrak{i}$.

Congruence Problem

Given: A set $F \subseteq \mathcal{F}$ and two elements $f, g \in \mathcal{F}$.

Problem: $f = g$ in $\mathcal{F}/\mathsf{ideal}(F)$?

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}(F)$.
2. If $f - g \xrightarrow{*}_G o$, then $f = g$ in $\mathcal{F}/\mathsf{ideal}(F)$.

Hence if G is a Gröbner basis for which normal form computation is effective, the congruence problem is solvable.

Usually one element of the congruence class is identified as its representative and since normal forms with respect to Gröbner bases are unique, they can be chosen as such representatives.

Notice that for weak Gröbner bases unique representations for the quotient can no longer be determined by reduction (review Example 3.1.1).

Unique Representatives Problem

Given: A set $F \subseteq \mathcal{F}$ and an element $f \in \mathcal{F}$.

Problem: Determine a unique representative for f in $\mathcal{F}/\mathsf{ideal}(F)$.

Proceeding:
1. Let G be a respective Gröbner basis.
2. The normal form of f with respect to G is a unique representative.

Provided a Gröbner basis of $\mathfrak{i}$ together with an effective normal form algorithm we can specify unique representatives by

$$[f]_{\mathfrak{i}} := \text{normal\_form}(f, G),$$

and define addition and multiplication in the quotient by

$$[f]_{\mathfrak{i}} + [g]_{\mathfrak{i}} := \text{normal\_form}(f + g, G),$$

$$[f]_{\mathfrak{i}} * [g]_{\mathfrak{i}} := \text{normal\_form}(f \star g, G).$$

Similar to the case of polynomial rings for a function ring over a field $\mathbb{K}$ we can show that this structure is a $\mathbb{K}$-vector space with a special basis.

Lemma 5.2.1
For any ideal $\mathfrak{i} \subseteq \mathcal{F}_{\mathbb{K}}$ the following hold:

1. *$\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$ is a $\mathbb{K}$-vector space.*
2. *The set $B = \{[t]_{\mathfrak{i}} \mid t \in \mathcal{T}\}$ is a vector space basis and we can chose $[t]_{\mathfrak{i}} = \text{monic}(\text{normal\_form}(t, G))$ for G being a Gröbner basis of $\mathfrak{i}$.*

Proof :

1. We have to show that the following properties hold for $V = \mathcal{F}_{\mathbb{K}}/\mathfrak{i}$:

   (a) There exists a mapping $K \times V \longrightarrow V$, $(\alpha, [f]_{\mathfrak{i}}) \longmapsto \alpha \cdot [f]_{\mathfrak{i}}$ called multiplication with scalars.

   (b) $(\alpha \cdot \beta) \cdot [f]_{\mathfrak{i}} = \alpha \cdot (\beta \cdot [f]_{\mathfrak{i}})$ for all $\alpha, \beta \in \mathbb{K}$, $[f]_{\mathfrak{i}} \in V$.

   (c) $\alpha \cdot ([f]_{\mathfrak{i}} + [g]_{\mathfrak{i}}) = \alpha \cdot [f]_{\mathfrak{i}} + \alpha \cdot [g]_{\mathfrak{i}}$ for all $\alpha \in \mathbb{K}$, $[f]_{\mathfrak{i}}, [g]_{\mathfrak{i}} \in V$.

   (d) $(\alpha + \beta) \cdot [f]_{\mathfrak{i}} = \alpha \cdot [f]_{\mathfrak{i}} + \beta \cdot [f]_{\mathfrak{i}}$ for all $\alpha, \beta \in \mathbb{K}$, $[f]_{\mathfrak{i}} \in V$.

   (e) $\mathbf{1} \cdot [f]_{\mathfrak{i}} = [f]_{\mathfrak{i}}$ for all $[f]_{\mathfrak{i}} \in V$.

   It is easy to show that this follows from the natural definition

   $$\alpha \cdot [f]_{\mathfrak{i}} := [\alpha \cdot f]_{\mathfrak{i}}$$

   for $\alpha \in \mathbb{K}$, $[f]_{\mathfrak{i}} \in V$.

2. It follows immediately that B generates the quotient $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$. So it remains to show that this basis is free in the sense that o cannot be represented as a non-trivial linear combination of elements in B. Let G be a Gröbner basis of $\mathfrak{i}$. Then we can choose the elements of B as the normal forms of the elements in $\mathcal{T}$ with respect to G. Since for a polynomial in normal form all its terms are also in normal form we can conclude that these normal forms are elements of $\mathsf{M}(\mathcal{F}_{\mathbb{K}})$ and since $\mathbb{K}$ is a field we can make them monic. This leaves us with a basis $\{\tilde{t} = \text{monic}(\text{normal\_form}(t, G)) \mid t \in \mathcal{T}\}$. Now let us assume that B is not free, i.e. there exists $k \in \mathbb{N}$ minimal with $\alpha_i \in \mathbb{K}\backslash\{0\}$ and $[t_i]_{\mathfrak{i}} \in B$, $1 \leq i \leq k$ such that $\sum_i^k \alpha_i \cdot [t_i]_{\mathfrak{i}} = o$. Since then we also get $\text{normal\_form}(\sum_i^k \alpha_i \cdot \tilde{t}_i, G) = o$ and all $\tilde{t}_i$ are different and in normal form, all α_i must equal 0 contradicting our assumption.

q.e.d.

If we can compute normal forms for the quotient elements, we can give a multiplication table for the quotient in terms of the vector space basis by

$$[t_i]_{\mathfrak{i}} * [t_j]_{\mathfrak{i}} = [t_i \star t_j]_{\mathfrak{i}} = \text{normal\_form}(t_i \circ t_j, G).$$

Notice that for a function ring over a reduction ring the set $B = \{[t]_{\mathfrak{i}} \mid t \in \mathcal{T}\}$ also is a generating set where we can chose $[t]_{\mathfrak{i}} = \text{normal\_form}(t, G)$. But we can no longer choose the representatives to be a subset of $\mathcal{T}$. This is due to the fact that if a monomial $\alpha \cdot t$ is reducible by some polynomial g this does not imply that some other monomial $\beta \cdot t$ or even the term t is reducible by g. For example let $\mathsf{R} = \mathbb{Z}$, $\mathcal{T} = \{a, \lambda\}$ and $a \star a = 2 \cdot a$, $\lambda \star \lambda = \lambda$, $a \star \lambda = \lambda \star a = a$. Then $2 \cdot a$ is reducible by a while of course a isn't.

In case $\mathcal{F}_{\mathbb{K}}$ contains a unit say $\mathbf{1}$ we can ask whether an element of $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$ is invertible.

Definition 5.2.2
Let $f \in \mathcal{F}_{\mathbb{K}}$. An element $g \in \mathcal{F}_{\mathbb{K}}$ is called a **right inverse** of f in $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$ if $f \star g = \mathbf{1}$ mod $\mathfrak{i}$. Similarly g is called a **left inverse** of f in $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$ if $g \star f = \mathbf{1}$ mod $\mathfrak{i}$. $\diamond$

In case $\mathcal{F}_{\mathbb{K}}$ is commutative, right and left inverses coincide if they exist and we can tackle the problem by using the fact that f has an inverse in $\mathfrak{i}$ if and only if $f \star g - \mathbf{1} \in \mathfrak{i}$ if and only if $\mathbf{1} \in \mathfrak{i} + \mathsf{ideal}(\{f\})$. Hence, if we have a Gröbner basis G of the ideal $\mathfrak{i} + \mathsf{ideal}(\{f\})$ the existence of an inverse of f is equivalent to $\mathbf{1} \xrightarrow{*}_G o$.

Even, weak Gröbner bases are sufficient to solve the problem.

For the non-commutative case we introduce a new non-commuting tag variable z by lifting the multiplication $z \star z = z$, $z \star t = zt$ and $t \star z = tz$ for $t \in \mathcal{T}$ and extending $\mathcal{T}$ to $z\mathcal{T} = \{z^i t_1 z t_2 z \ldots z t_k z^j \mid k \in \mathbb{N}, i, j \in \{0,1\}, t_i \in \mathcal{T}\}$. The order on this enlarged set of terms is induced by combining a syllable ordering with respect to z with the original ordering on $\mathcal{T}$. By $\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}$ we denote the function ring over $z\mathcal{T}$.

This technique of using a tag variable now allows to study the right ideal generated by f in $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$, where $\mathfrak{i} = \mathsf{ideal}(F)$ for some set $F \subseteq \mathcal{F}_{\mathbb{K}}$, by studying the ideal generated by $F \cup \{z \star f\}$ in $\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}$ because of the following fact:

Lemma 5.2.3
Let $F \subseteq \mathcal{F}_{\mathbb{K}}$ and $f \in \mathcal{F}_{\mathbb{K}}$. Then $\mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F \cup \{z \star f\})$ has a Gröbner basis of the form $G \cup \{z \star p_i \mid i \in I, p_i \in \mathcal{F}_{\mathbb{K}}\}$ with $G \subseteq \mathcal{F}_{\mathbb{K}}$. In fact the set $\{p_i \mid i \in I\}$ then is a right Gröbner basis of $\mathsf{ideal}_r^{\mathcal{F}_{\mathbb{K}}/\mathfrak{i}}(\{f\})$.

Proof :
Let $G \subseteq \mathcal{F}_{\mathbb{K}}$ be a Gröbner basis of $\mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}}(F)$. Then obviously $\mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F \cup \{z \star f\}) = \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(G \cup \{z \star f\})$. Theorem 4.4.31 specifies a criterion to check whether a set is a Gröbner basis and gives rise to test sets for a completion procedure. Notice that due to the ordering on $z\mathcal{T}$ which uses the tag variable to induce syllables, we can state the following important result:

> If for a polynomial $q \in \mathcal{F}_{\mathbb{K}}$ the multiple $z \star q$ has a standard representation, then so has every multiple $u \star (z \star q) \star z \star v$ for $u, v \in z\mathcal{T}$.

Moreover, since G is already a Gröbner basis, no critical situation for polynomials in G have to be considered.
Then a completion of $G \cup \{z \star f\}$ can be obtained as follows:
In a first step only three kinds of critical situations have to be considered:

1. s-polynomials of the form $zu \star g \star v - z \star f \star w$ where $u, v, w \in \mathcal{T}$ such that $\mathsf{HT}(zu \star g \star v) = \mathsf{HT}(z \star f \star w)$,
2. s-polynomials of the form $z \star f \star u - z \star f \star v$ where $u, v \in \mathcal{T}$ such that $\mathsf{HT}(z \star f \star u) = \mathsf{HT}(z \star f \star v)$, and
3. polynomials of the form $z \star f \star u$ where $u \in \mathcal{T}$ such that $\mathsf{HT}(f \star u) \neq \mathsf{HT}(f) \star u$.

Since normal forms of polynomials of the form $z \star p$, $p \in \mathcal{F}_{\mathbb{K}}$, with respect to subsets of $\mathcal{F}_{\mathbb{K}} \cup z \star \mathcal{F}_{\mathbb{K}}$ are again elements of $z \star \mathcal{F}_{\mathbb{K}} \cup \{o\}$, we can assume that from then on we are completing a set $G \cup \{z \star q_i \mid q_i \in \mathcal{F}_{\mathbb{K}}\}$ and again three kinds of critical situations have to be considered:

1. s-polynomials of the form $zu \star g \star v - z \star q_i \star w$ where $u, v, w \in \mathcal{T}$ such that $\mathsf{HT}(zu \star g \star v) = \mathsf{HT}(z \star q_i \star w)$,
2. s-polynomials of the form $z \star q_i \star u - z \star q_j \star v$ where $u, v \in \mathcal{T}$ such that $\mathsf{HT}(z \star q_i \star u) = \mathsf{HT}(z \star q_j \star v)$, and
3. polynomials of the form $z \star p_i \star u$ where $u \in \mathcal{T}$ such that $\mathsf{HT}(p_i \star u) \neq \mathsf{HT}(p_i) \star u$.

Normal forms again are elements of $z \star \mathcal{F}_{\mathbb{K}} \cup \{o\}$. Hence a Gröbner basis of the form $G \cup \{z \star p_i \mid i \in I, p_i \in \mathcal{F}_{\mathbb{K}}\}$ with $G \subseteq \mathcal{F}_{\mathbb{K}}$ must exist.
It remains to show that the set $\{p_i \mid i \in I\}$ is in fact a right Gröbner basis of $\mathsf{ideal}_r^{\mathcal{F}_{\mathbb{K}}/\mathsf{i}}(\{f\})$. This follows immediately if we recall the history of the polynomials p_i. In the first step they arise as a normal form with respect to $G \cup \{z \star f\}$ of a polynomial either of the form $zu \star g \star v - z \star f \star w$, $z \star f \star u - z \star f \star v$ or $z \star f \star u$, hence belonging to $\mathsf{ideal}_r^{\mathcal{F}_{\mathbb{K}}/\mathsf{i}}(\{f\})$. In the iteration step, the new p_n arises as a normal form with respect to $G \cup \{z \star p_i \mid i \in I_{old}\}$ of a polynomial either of the form $zu \star g \star v - z \star p_i \star w$, $z \star p_i \star u - z \star p_j \star v$ or $z \star p_i \star u$, hence belonging to $\mathsf{ideal}_r^{\mathcal{F}_{\mathbb{K}}/\mathsf{i}}(\{p_i \mid i \in I_{old}\}) = \mathsf{ideal}_r^{\mathcal{F}_{\mathbb{K}}/\mathsf{i}}(\{f\})$. q.e.d.

Since we require $\mathcal{F}_{\mathbb{K}}$ to have a unit (otherwise looking for inverse elements makes no sense), $\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}$ then will contain z.

Inverse Element Problem

Given: An element $f \in \mathcal{F}_{\mathbb{K}}$ and a generating set F for $\mathfrak{i}$.

Problem: Does f have a right or left inverse in $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$?

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F \cup \{z \star f\})$.
2. If $z \xrightarrow{*}_G o$, then f has a right inverse.

1'. Let G be a Gröbner basis of $\mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F \cup \{f \star z\})$.

2'. If $z \xrightarrow{*}_G o$, then f has a left inverse.

To see that this is correct we give the following argument for the case of right inverses: It is clear that f has a right inverse in $\mathcal{F}_{\mathbb{K}}/\mathfrak{i}$ if and only if $f \star g - \mathbf{1} \in \mathfrak{i}$ for some $g \in \mathcal{F}_{\mathbb{K}}$. On the other hand we get $f \star g - \mathbf{1} \in \mathfrak{i}$ if and only if $z \star f \star g - z \in \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F) \cap z \star \mathcal{F}_{\mathbb{K}}$: $f \star g - \mathbf{1} \in \mathfrak{i}$ immediately implies $z \star (f \star g - \mathbf{1}) \in \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F) \cap z \star \mathcal{F}_{\mathbb{K}}$ as $\mathfrak{i} \subseteq \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F)$, $z \in z\mathcal{T} \subseteq \mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}$ and $z \star (f \star g - \mathbf{1}) \in z \star \mathcal{F}_{\mathbb{K}}$. On the other hand, if $z \star f \star g - z \in \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F) \cap z \star \mathcal{F}_{\mathbb{K}} \subseteq \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F)$, then we have a representation $z \star f \star g - z = \sum_{i=1}^{k} h_i \star f_i \star \tilde{h}_i$, $h_i, \tilde{h}_i \in \mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}$, $f_i \in F \subseteq \mathcal{F}_{\mathbb{K}}$. For a polynomial $p \in \mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}$ and some element $\alpha \in \mathbb{K}$ let $p[z = \alpha]$ be the polynomial which arises from p by substituting α for the variable z. Then by substituting $z = \mathbf{1}$ we get $f \star g - \mathbf{1} = \sum_{i=1}^{k} h_i[z = \mathbf{1}] \star f_i \star \tilde{h}_i[z = \mathbf{1}]$ with $h_i[z = \mathbf{1}], \tilde{h}_i[z = \mathbf{1}] \in \mathcal{F}_{\mathbb{K}}$ and are done.

Now, in order to decide whether f has a right inverse in $\mathfrak{i}$ one has to distinguish the following two cases provided we have a Gröbner basis G of $\mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F \cup \{z \star f\})$: If $z \not\xrightarrow{*}_G o$ then there exists no $g \in \mathcal{F}_{\mathbb{K}}$ such that $f \star g - \mathbf{1} \in \mathfrak{i}$ and hence f has no right inverse. If $z \xrightarrow{*}_G o$ then we know $z \in \mathsf{ideal}^{\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}}}(F \cup \{z \star f\})$, and even $z \in \mathsf{ideal}_r^{\mathcal{F}_{\mathbb{K}}/\mathfrak{i}}(\{z \star f\})$ Hence there exist $m_i, \tilde{m}_i, n_j \in \mathsf{M}(\mathcal{F}_{\mathbb{K}}^{z\mathcal{T}})$, $f_i \in F$ such that

$$z = \sum_{i=1}^{k} m_i \star f_i \star \tilde{m}_i + \sum_{j=1}^{l} z \star f \star n_j.$$

Now substituting $z = \mathbf{1}$ gives us that for $h = \sum_{j=1}^{l} n_j$ we have $f \star h = \mathbf{1} (\bmod \mathfrak{i})$ and we are done.

As before, weak Gröbner bases are sufficient to solve the problem.

5.3 Elimination Theory

In ordinary polynomial rings special term orderings called elimination orderings can be used to produce Gröbner bases with useful properties. Many problems, e.g. the ideal intersection problem or the subalgebra problem, can be solved using tag variables. The elimination orderings are then used to separate the ordinary variables from these additional tag variables. Something similar can be achieved for function rings.

Let $Z = \{z_i \mid i \in I\}$ be a set of new tag variables commuting with terms. The multiplication $\star$ can be extended by $z_i \star z_j = z_i z_j$, $z \star t = zt$ and $t \star z = zt$ for $z, z_i, z_j \in Z$ and $t \in \mathcal{T}$. The ordering $\succeq$ is lifted to $Z^*\mathcal{T} = \{wt \mid w \in Z^*, t \in \mathcal{T}\}$ by $w_1t_1 \succeq w_2t_2$ if and only if $w_1 \geq_{\text{lex}} w_2$ or ($w_1 = w_2$ and $t_1 \succeq t_2$) for all $w_1, w_2 \in Z^*$, $t_1, t_2 \in \mathcal{T}$. Moreover, we require $w \succ t$ for all $w \in Z^*$, $t \in \mathcal{T}$. This ordering is called an elimination ordering.

Up to now we have studied ideals in $\mathcal{F}^{\mathcal{T}}$. Now we can view $\mathcal{F}^{\mathcal{T}}$ as a subring of $\mathcal{F}^{Z^*\mathcal{T}}$ and study ideals in both rings. For a generating set $F \subset \mathcal{F}^{\mathcal{T}}$ we have $\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(F) \subseteq \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(F)$. This follows immediately since for every $f = \sum_{i=1}^{k} m_i \star f_i \star \tilde{m}_i$, $m_i, \tilde{m}_i \in \mathsf{M}(\mathcal{F}^{\mathcal{T}})$ this immediately implies $m_i, \tilde{m}_i \in \mathsf{M}(\mathcal{F}^{Z^*\mathcal{T}})$.

Lemma 5.3.1
Let G be a weak Gröbner basis of an ideal in $\mathcal{F}^{Z^*\mathcal{T}}$ with respect to an elimination ordering. Then the following hold:

1. $\mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G) \cap \mathcal{F}^{\mathcal{T}} = \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$.
2. *$G \cap \mathcal{F}^{\mathcal{T}}$ is a weak Gröbner basis for $\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$ with respect to $\succeq$.*
3. *If G is a Gröbner basis, then $G \cap \mathcal{F}^{\mathcal{T}}$ is a Gröbner basis for $\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$ with respect to $\succeq$.*

Proof :

1.
   - $\mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G) \cap \mathcal{F}^{\mathcal{T}} \subseteq \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$:
     Let $f \in \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G) \cap \mathcal{F}^{\mathcal{T}}$. By the elimination ordering property for $w \in Z^*$ and $t \in \mathcal{T}$ we have that $wt \succ w \succ t$ holds and we get that $\mathsf{HT}(f) \in \mathcal{T}$ if and only if $f \in \mathcal{F}^{\mathcal{T}}$. Since $f \in \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G)$ we know that $f \xrightarrow{*}_G o$ and as all monomials in f are also in $\mathcal{F}^{\mathcal{T}}$ for each $g \in G$ used in this reduction sequence we know $\mathsf{HT}(g) \in \mathcal{T}$ and hence $g \in \mathcal{F}^{\mathcal{T}}$. Moreover, the reduction sequence gives us a representation $f = \sum_{i=1}^{k} m_i \star f_i \star \tilde{m}_i$ with $f_i \in G \cap \mathcal{F}^{\mathcal{T}}$ and $m_i, \tilde{m}_i \in \mathsf{M}(\mathcal{F}^{\mathcal{T}})$, implying $f \in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$.
   - $\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}}) \subseteq \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G) \cap \mathcal{F}^{\mathcal{T}}$:
     Let $f \in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$. Then $f = \sum_{i=1}^{k} m_i \star f_i \star \tilde{m}_i$ with $f_i \in G \cap \mathcal{F}^{\mathcal{T}}$ and $m_i, \tilde{m}_i \in \mathsf{M}(\mathcal{F}^{\mathcal{T}})$. Hence $f \in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G) \subseteq \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G)$ and $f \in \mathcal{F}^{\mathcal{T}}$ imply $f \in \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G) \cap \mathcal{F}^{\mathcal{T}}$.

2. We show this by proving that for every $f \in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$ we have $f \xrightarrow{*}_{G\cap\mathcal{F}^{\mathcal{T}}} o$. Since G is a weak Gröbner basis of $\mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G)$ and $\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}}) \subseteq \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}}) \subseteq \mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G)$ we get $f \xrightarrow{*}_G o$. On the other hand, as every monomial in f is an element of $\mathcal{F}^{\mathcal{T}}$, only elements of $G \cap \mathcal{F}^{\mathcal{T}}$ are applicable for reduction.

3. Let G be a Gröbner basis with respect to some reduction relation $\longrightarrow$. To show that $G \cap \mathcal{F}^{\mathcal{T}}$ is a Gröbner basis of $\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G \cap \mathcal{F}^{\mathcal{T}})$ we proceed in two steps:

   (a) $\xleftrightarrow{*}_{G\cap\mathcal{F}^{\mathcal{T}}} \; = \; \equiv_{\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G\cap\mathcal{F}^{\mathcal{T}})}$:
   $\xleftrightarrow{*}_{G\cap\mathcal{F}^{\mathcal{T}}} \; \subseteq \; \equiv_{\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(G\cap\mathcal{F}^{\mathcal{T}})}$ trivially holds as because of Axiom (A2) reduction steps stay within the ideal congruence. To see the converse let $f \equiv_{\mathsf{ideal}(G\cap\mathcal{F}^{\mathcal{T}})} g$ for $f, g \in \mathcal{F}^{\mathcal{T}}$. Then, as G is a Gröbner basis and also $f \equiv_{\mathsf{ideal}^{\mathcal{F}^{Z^*\mathcal{T}}}(G)} g$ holds, we know $f \xleftrightarrow{*}_G g$ and as $\mathsf{HT}(f), \mathsf{HT}(g) \in \mathcal{F}^{\mathcal{T}}$, only elements from $G \cap \mathcal{F}^{\mathcal{T}}$ can be involved and we are done.

   (b) $\longrightarrow_{G\cap\mathcal{F}^{\mathcal{T}}}$ is confluent:
   Let $g, g_1, g_2 \in \mathcal{F}^{\mathcal{T}}$ such that $g \longrightarrow_{G\cap\mathcal{F}^{\mathcal{T}}} g_1$ and $g \longrightarrow_{G\cap\mathcal{F}^{\mathcal{T}}} g_2$. Then, as $\longrightarrow_G$ is confluent we know that there exists $f \in \mathcal{F}^{Z^*\mathcal{T}}$ such that $g_1 \xrightarrow{*}_G f$ and $g_2 \xrightarrow{*}_G f$. Now since $\mathsf{HT}(g) \in \mathcal{F}^{\mathcal{T}}$ we can conclude that $g_1, g_2, f \in \mathcal{F}^{\mathcal{T}}$ and hence all polynomials used for reduction in the reduction sequences lie in $G \cap \mathcal{F}^{\mathcal{T}}$ proving our claim.

q.e.d.

Given an ideal $\mathfrak{i} \subseteq \mathcal{F}^{Z^*\mathcal{T}}$ the set $\mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$ is again an ideal, now in $\mathcal{F}^{\mathcal{T}}$. This follows as

1. $o \in \mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$ since $o \in \mathfrak{i}$ and $o \in \mathcal{F}^{\mathcal{T}}$.

2. For $f, g \in \mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$ we have $f + g \in \mathfrak{i}$ as $f, g \in \mathfrak{i}$ and $f + g \in \mathcal{F}^{\mathcal{T}}$ as $f, g \in \mathcal{F}^{\mathcal{T}}$ yielding $f + g \in \mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$.

3. For $f \in \mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$ and $h \in \mathcal{F}^{\mathcal{T}}$ we have that $f \star h, h \star f \in \mathfrak{i}$ as $f \in \mathfrak{i}$ and $f \star h, h \star f \in \mathcal{F}^{\mathcal{T}}$ as $f, h \in \mathcal{F}^{\mathcal{T}}$ yielding $f \star h, h \star f \in \mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$.

The ideal $\mathfrak{i} \cap \mathcal{F}^{\mathcal{T}}$ is called the elimination ideal of $\mathfrak{i}$ with respect to Z since the occurrences of the tag variables Z are eliminated.

Definition 5.3.2
For an ideal $\mathfrak{i}$ in $\mathcal{F}$ the set

$$\sqrt{\mathfrak{i}} = \{f \in \mathcal{F} \mid \text{ there exists } m \in \mathbb{N} \text{ with } f^m \in \mathfrak{i}\}$$

is called the **radical** of $\mathfrak{i}$. $\diamond$

Obviously we always have $\mathfrak{i} \subseteq \sqrt{\mathfrak{i}}$. Moreover, if $\mathcal{F}$ is commutative the radical of an ideal is again an ideal. This follows as

1. $o \in \sqrt{\mathfrak{i}}$ since $o \in \mathfrak{i}$,

2. For $f, g \in \sqrt{\mathfrak{i}}$ we know $f^m, g^n \in \mathfrak{i}$ for some $m, n \in \mathbb{N}$. Now $f + g \in \sqrt{\mathfrak{i}}$ if we can show that $(f+g)^q \in \mathfrak{i}$ for some $q \in \mathbb{N}$. Remember that for $q = m+n-1$ every term in the binomial expansion of $(f+g)^q$ has a factor of the form $f^i \star g^j$ with $i + j = m + n - 1$. As either $i \geq m$ or $j \geq n$ we find $f^i \star g^j \in \mathfrak{i}$ yielding $(f+g)^q \in \mathfrak{i}$ and hence $f + g \in \sqrt{\mathfrak{i}}$. Notice that commutativity is essential in this setting.

3. For $f \in \sqrt{\mathfrak{i}}$ we know $f^m \in \mathfrak{i}$ for some $m \in \mathbb{N}$. Hence for $h \in \mathcal{F}^{\mathcal{T}}$ we get $(f \star h)^m = f^m \star h^m \in \mathfrak{i}$ yielding $f \star h \in \sqrt{\mathfrak{i}}$. Again commutativity is essential in the proof.

Unfortunately this no longer holds for non-commutative function rings. For example take $\mathcal{T} = \{a, b\}^*$ with concatenation as multiplication. Then for $\mathfrak{i} = \mathsf{ideal}(\{a^2\}) = \{\sum_{i=1}^{n} \alpha_i \cdot u_i a^2 v_i \mid n \in \mathbb{N}, \alpha_i \in \mathbb{Q}, u_i, v_i \in \mathcal{T}\}$ we get $a \in \sqrt{\mathfrak{i}}$. But for $b \in \mathcal{F}$ there exists no $m \in \mathbb{N}$ such that $(ab)^m \in \mathfrak{i}$ and hence $\sqrt{\mathfrak{i}}$ is no ideal.

In the commutative polynomial ring the question whether some polynomial f lies in the radical of some ideal generated by a set F can be answered by introducing a tag variable z and computing a Gröbner basis of the ideal generated by the set $F \cup \{fz - \mathbf{1}\}$. It can be shown that if a commutative function ring $\mathcal{F}$ contains a unit $\mathbf{1}$ we get a similar result.

Theorem 5.3.3
Let $F \subseteq \mathcal{F}$ and $f \in \mathcal{F}$ where $\mathcal{F}$ is a commutative function ring containing a unit $\mathbf{1}$. Then $f \in \sqrt{\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(F)}$ if and only if $\mathbf{1} \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$ for some new tag variable z.

Proof :
If $f \in \sqrt{\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(F)}$, then $f^m \in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(F) \subseteq \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$ for some $m \in \mathbb{N}$. But we also have that $z \star f - \mathbf{1} \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$. Remember that for the tag variable we have $t \star z = zt$ for all $t \in \mathcal{T}$ and hence $f \star z = z \star f$ yielding

$$\begin{aligned} \mathbf{1} &= z^m \star f^m - (z^m \star f^m - \mathbf{1}) \\ &= \underbrace{z^m \star f^m}_{\in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(F)} - \underbrace{(z \star f - \mathbf{1}) \star (\sum_{i=0}^{m-1} z^i \star f^i)}_{\mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})} \end{aligned}$$

and hence $\mathbf{1} \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$ and we are done.
On the other hand, $\mathbf{1} \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$ implies $\mathbf{1} = \sum_{i=1}^{k} m_i \star f_i \star \tilde{m}_i + \sum_{j=1}^{l} n_j \star (z \star f - \mathbf{1}) \star \tilde{n}_j$ with $m_i, \tilde{m}_i, n_j, \tilde{n}_j \in \mathsf{M}(\mathcal{F}^{\{z\}^*\mathcal{T}})$. Moreover, since for the tag variable we have $z \star t = t \star z = zt$ for all $t \in \mathcal{T}$ all terms occurring in $\sum_{i=1}^{k} g_i \star f_i \star h_i$ are of the form $z^j t$ for some $t \in \mathcal{T}$, $j \in \mathbb{N}$. Now, since $z \star f - \mathbf{1} \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$, we have $z^j t \star f^j = t \star z^j \star f^j = t$ as well as $f^j \star z^j \star t = z^j \star f^j \star t = t$. Hence, the occurrences of z in a term $z^j t$ with $t \in \mathcal{T}$ can be "cancelled" by multiplication with f^m, $m \geq j$. Therefore, by choosing $m \in \mathbb{N}$ sufficiently large to cancel *all* occurrences of z in the terms of $\sum_{i=1}^{k} m_i \star f_i \star \tilde{m}_i$, multiplying the equation with f^m from both sides yields

$$f^{2m} = \sum_{i=1}^{k} (f^m \star m_i) \star f_i \star (\tilde{m}_i \star f^m)$$

and $f^m \star m_i, \tilde{m}_i \star f^m \in \mathcal{F}^{\mathcal{T}}$. Hence $f^{2m} \in \mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}(F)$ and therefore $f \in \sqrt{\mathsf{ideal}^{\mathcal{F}^{\mathcal{T}}}}(F)$.

q.e.d.

This theorem now enables us to describe the membership problem for radicals of ideals in terms of Gröbner bases.

Radical Membership Problem

Given: A set $F \subseteq \mathcal{F}$ and an element $f \in \mathcal{F}$, $\mathcal{F}$ containing a unit $\mathbf{1}$.

Problem: $f \in \sqrt{\mathsf{ideal}}(F)$?

Proceeding:
1. Let G be a respective Gröbner basis of $\mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(F \cup \{z \star f - \mathbf{1}\})$ for some new tag variable z.
2. If $\mathbf{1} \xrightarrow{*}_G o$, then $f \in \sqrt{\mathsf{ideal}}(F)$.

If additionally the function ring is commutative, remember that then $\sqrt{\mathfrak{i}}$ is an ideal and we then describe the equality problem for radicals of ideals.

Notice that weak Gröbner bases are sufficient to solve the problem.

Radical Equality Problem

Given: Two sets $F_1, F_2 \subseteq \mathcal{F}$, $\mathcal{F}$ commutative containing a unit.

Problem: $\sqrt{\mathsf{ideal}}(F_1) = \sqrt{\mathsf{ideal}}(F_2)$?

Proceeding:
1. If for all $f \in F_1$ we have $f \in \sqrt{\mathsf{ideal}}(F_2)$, then $\sqrt{\mathsf{ideal}}(F_1) \subseteq \sqrt{\mathsf{ideal}}(F_2)$.
2. If for all $f \in F_2$ we have $f \in \sqrt{\mathsf{ideal}}(F_1)$, then $\sqrt{\mathsf{ideal}}(F_2) \subseteq \sqrt{\mathsf{ideal}}(F_1)$.
3. If 1. and 2. both hold, then $\sqrt{\mathsf{ideal}}(F_1) = \sqrt{\mathsf{ideal}}(F_2)$.

Correctness can be shown as follows: Let us assume that for all $f \in F_1$ we have $f \in \sqrt{\mathsf{ideal}(F_2)}$. Then, as $\mathcal{F}$ is commutative $\mathsf{ideal}(F_1) \subseteq \sqrt{\mathsf{ideal}(F_2)}$ holds. Now let $f \in \sqrt{\mathsf{ideal}(F_1)}$. Then for some $m \in \mathbb{N}$ we have $f^m \in \mathsf{ideal}(F_1) \subseteq \sqrt{\mathsf{ideal}(F_2)}$ and hence $\sqrt{\mathsf{ideal}(F_1)} \subseteq \sqrt{\mathsf{ideal}(F_2)}$.

If $\mathcal{F}$ is not commutative, $\mathsf{ideal}(F_1) \subseteq \sqrt{\mathsf{ideal}(F_2)}$ need not hold. Remember the function ring with $\mathcal{T} = \{a, b\}^*$. Take $F_1 = \{a\}$ and $F_2 = \{a^2\}$. Then $a \in \sqrt{\mathsf{ideal}(F_2)}$ since $a^2 \in \mathsf{ideal}(F_2)$. But while $ab \in \mathsf{ideal}(F_1)$ we have $ab \notin \sqrt{\mathsf{ideal}(F_2)}$.

Radicals of one-sided ideals can be defined as well and Theorem 5.3.3 is also valid in this setting and can be used to state the radical membership problem for one-sided ideals.

Another problem which can be handled using tag variables and elimination orderings in the commutative polynomial ring is that of ideal intersections. Something similar can be done for function rings containing a unit.

Theorem 5.3.4
Let $\mathfrak{i}$ and $\mathfrak{j}$ be two ideals in $\mathcal{F}$ and z a new tag variable. Then

$$\mathfrak{i} \cap \mathfrak{j} = \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(z \star \mathfrak{i} \cup (z - \mathbf{1}) \star \mathfrak{j}) \cap \mathcal{F}$$

where $z \star \mathfrak{i} = \{z \star f \mid f \in \mathfrak{i}\}$ and $(z - \mathbf{1}) \star \mathfrak{j} = \{(z - \mathbf{1}) \star f \mid f \in \mathfrak{j}\}$.

Proof :
Every polynomial $f \in \mathfrak{i} \cap \mathfrak{j}$ can be written as $f = z \star f - (z - \mathbf{1}) \star f$ and hence $f \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(z \star \mathfrak{i} \cup (z - \mathbf{1}) \star \mathfrak{j}) \cap \mathcal{F}$. On the other hand, $f \in \mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(z \star \mathfrak{i} \cup (z - \mathbf{1}) \star \mathfrak{j}) \cap \mathcal{F}$ implies $f = \sum_{i=1}^{k} m_i \star z \star f_i \star \tilde{m}_i + \sum_{j=1}^{l} n_j \star (z - \mathbf{1}) \star \tilde{f}_j \star \tilde{n}_j$ with $f_i \in \mathfrak{i}$, $\tilde{f}_j \in \mathfrak{j}$ and $m_i, \tilde{m}_i, n_j, \tilde{n}_j \in \mathsf{M}(\mathcal{F}^{\{z\}^*\mathcal{T}})$. Since $f \in \mathcal{F}^{\mathcal{T}}$, substituting $z = \mathbf{1}$ gives us $f \in \mathfrak{i}$ and $z = 0$ gives us $f \in \mathfrak{j}$ and hence $f \in \mathfrak{i} \cap \mathfrak{j}$.

q.e.d.

Moreover, combining this result with Lemma 5.3.1 gives us the means to characterize a Gröbner basis of the intersection ideal.

Intersection Problem

Given: Two sets $F_1, F_2 \subseteq \mathcal{F}$.

Problem: Determine a basis of $\mathsf{ideal}(F_1) \cap \mathsf{ideal}(F_2)$.

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}^{\mathcal{F}^{\{z\}^*\mathcal{T}}}(z \star \mathfrak{i} \cup (z - \mathbf{1}) \star \mathfrak{j})$ with respect to an elimination ordering with $z > \mathcal{T}$.
2. Then $G \cap \mathcal{F}$ is a Gröbner basis of $\mathsf{ideal}(F_1) \cap \mathsf{ideal}(F_2)$.

These ideas extend to one-sided ideals as well.

Again, weak Gröbner bases are sufficient to solve the problem.

Of course Theorem 5.3.4 can be generalized to intersections of more than two ideals.

The techniques can also be applied to treat quotients of ideals in case $\mathcal{F}_{\mathbb{K}}$ is commutative.

Definition 5.3.5
For two ideals $\mathfrak{i}$ and $\mathfrak{j}$ in a commutative function ring $\mathcal{F}_{\mathbb{K}}$ we define the quotient to be the set

$$\mathfrak{i}/\mathfrak{j} = \{g \mid g \in \mathcal{F}_{\mathbb{K}} \text{ with } g \star \mathfrak{j} \subseteq \mathfrak{i}\}$$

where $g \star \mathfrak{j} = \{g \star f \mid f \in \mathfrak{j}\}$. $\diamond$

Lemma 5.3.6
Let $\mathcal{F}_{\mathbb{K}}$ be a commutative function ring. Let $\mathfrak{i}$ and $\mathfrak{j} = \mathsf{ideal}(F)$ be two ideals in $\mathcal{F}_{\mathbb{K}}$. Then

$$\mathfrak{i}/\mathfrak{j} = \bigcap_{f \in F} (\mathfrak{i}/\mathsf{ideal}(\{f\}).$$

Proof : First let $g \in \mathfrak{i}/\mathfrak{j}$. Then $g \star \mathfrak{j} \subseteq \mathfrak{i}$. Since $\mathfrak{j} = \mathsf{ideal}(F)$ we get $g \star f \in \mathfrak{i}$ for all $f \in F$. As $\mathcal{F}_{\mathbb{K}}$ is commutative we can conclude $g \star \mathsf{ideal}(\{f\}) \subseteq \mathfrak{i}$ for all $f \in F$ and hence $g \in \mathfrak{i}/\mathsf{ideal}(\{f\})$ for all $f \in F$ yielding $g \in \bigcap_{f \in F}(\mathfrak{i}/\mathsf{ideal}(\{f\})$.
On the other hand, $g \in \bigcap_{f \in F}(\mathfrak{i}/\mathsf{ideal}(\{f\})$ implies $g \in \mathfrak{i}/\mathsf{ideal}(\{f\})$ for all $f \in F$ and hence $g \star \mathsf{ideal}(\{f\}) \subseteq \mathfrak{i}$ for all $f \in F$. Since $\mathfrak{j} = \mathsf{ideal}(F)$ then $g \star \mathfrak{j} \subseteq \mathfrak{i}$ and hence $g \in \mathfrak{i}/\mathfrak{j}$. q.e.d.

Hence we can describe quotients of ideals in terms of quotients of the special form $\mathfrak{i}/\mathsf{ideal}(\{f\})$. These special quotients now can be described using ideal intersection in case $\mathcal{F}_{\mathbb{K}}$ contains a unit element $\mathbf{1}$.

Lemma 5.3.7
Let $\mathcal{F}_{\mathbb{K}}$ be a commutative function ring. Let $\mathfrak{i}$ be an ideal and $f \neq o$ a polynomial in $\mathcal{F}_{\mathbb{K}}$. Then

$$\mathfrak{i}/\mathsf{ideal}(\{f\}) = (\mathfrak{i} \cap \mathsf{ideal}(\{f\})) \star f^{-1}$$

where f^{-1} is an element in $\mathcal{F}_{\mathbb{K}}$ such that $f \star f^{-1} = \mathbf{1}$.

Proof :
First let $g \in \mathfrak{i}/\mathsf{ideal}(\{f\})$. Then $g \star \mathsf{ideal}(\{f\}) \subseteq \mathfrak{i}$ and $g \star f \in \mathfrak{i}$, even $g \star f \in \mathfrak{i} \cap \mathsf{ideal}(\{f\})$. Hence $g \in (\mathfrak{i} \cap \mathsf{ideal}(\{f\})) \star f^{-1}$.
On the other hand let $g \in (\mathfrak{i} \cap \mathsf{ideal}(\{f\})) \star f^{-1}$. Then $g \star f \in \mathfrak{i} \cap \mathsf{ideal}(\{f\}) \subseteq \mathfrak{i}$. Since $\mathcal{F}_{\mathbb{K}}$ is commutative, this implies $g \star \mathsf{ideal}(\{f\}) \subseteq \mathfrak{i}$ and hence $g \in$

$\mathfrak{i}/\mathsf{ideal}(\{f\})$.

q.e.d.

Hence we can study the quotient of $\mathfrak{i}$ and $\mathfrak{j} = \mathsf{ideal}(F)$ by studying $(\mathfrak{i} \cap \mathsf{ideal}(\{f\})) \star f^{-1}$ for all $f \in F$.

5.4 Polynomial Mappings

In this section we are interested in $\mathbb{K}$-algebra homomorphisms between the non-commutative polynomial ring $\mathbb{K}[Z^*]$ where $Z = \{z_1, \ldots, z_n\}$, and $\mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$. Let

$$\phi : \mathbb{K}[Z^*] \longrightarrow \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$$

be a ring homomorphism which is determined by a linear mapping

$$\phi : z_i \longmapsto f_i$$

with $f_i \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$, $1 \leq i \leq n$. Then for a non-commutative polynomial $g \in \mathbb{K}[Z^*]$ with $g = \sum_{j=1}^{m} \alpha_j \cdot w_j$, $w_j \in Z^*$ we get $\phi(g) = \sum_{j=1}^{m} \alpha_j \cdot \phi(w_j)$ where $\phi(w_j) = w_j[z_1 \longmapsto f_1, \ldots, z_n \longmapsto f_n]$. The kernel of such a mapping is defined as

$$\mathsf{ker}(\phi) = \{g \in \mathbb{K}[Z^*] \mid \phi(g) = o\}$$

and the image is defined as

$$\mathsf{im}(\phi) = \{f \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}} \mid \text{ there exists } g \in \mathbb{K}[Z^*] \text{ such that } \phi(g) = f\}.$$

Note that $\mathsf{im}(\phi)$ is a subalgebra of $\mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$.

Lemma 5.4.1
Let $\phi : \mathbb{K}[Z^*] \longrightarrow \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ be a ring homomorphism. Then $\mathbb{K}[Z^*]/\mathsf{ker}(\phi) \cong \mathsf{im}(\phi)$.

Proof :
To see this inspect the mapping $\psi : \mathbb{K}[Z^*]/\mathsf{ker}(\phi) \longrightarrow \mathsf{im}(\phi)$ defined by $g + \mathsf{ker}(\phi) \mapsto \phi(g)$. Then ψ is an isomorphism.

1. $\psi(g + \mathsf{ker}(\phi)) = o$ for $g \in \mathsf{ker}(\phi)$ by the definition of $\mathsf{ker}(\phi)$.
2. $\psi((g_1 + \mathsf{ker}(\phi)) + (g_2 + \mathsf{ker}(\phi))) = \phi(g_1 + g_2) = \psi(g_1 + \mathsf{ker}(\phi)) + \psi(g_2 + \mathsf{ker}(\phi))$.
3. $\psi((g_1 + \mathsf{ker}(\phi)) \star (g_2 + \mathsf{ker}(\phi))) = \phi(g_1 \star g_2) = \psi(g_1 + \mathsf{ker}(\phi)) \star \psi(g_2 + \mathsf{ker}(\phi))$, as for $g \in \mathbb{K}[Z^*]$ and $h \in \mathsf{ker}(\phi)$ we have $\psi(g \star h) = \psi(h \star g) = o$.
4. ψ is onto as its image is the image of ϕ and by the definition of the latter for each $f \in \mathsf{im}(\phi) = \mathsf{im}(\psi)$ there exists $g \in \mathbb{K}[Z^*]$ such that $\phi(g) = f$. Since for all $h \in \mathsf{ker}(\phi)$ we have $\phi(h) = o$ then $\psi(g + \mathsf{ker}(\phi)) = \psi(g) = \phi(g)$.

5. Assume that for $g_1, g_2 \in \mathbb{K}[Z^*]$ we have $\psi(g_1 + \mathsf{ker}(\phi)) = \psi(g_2 + \mathsf{ker}(\phi))$. Then $\phi(g_1) = \phi(g_2)$ and this immediately implies that $g_1 - g_2 \in \mathsf{ker}(\phi)$ and hence ψ is also a monomorphism.

q.e.d.

Now the theory of elimination described in the previous section can be used to provide a Gröbner basis for $\mathsf{ker}(\phi)$. Remember that the tag variables commute with the elements on $\mathcal{T}$. Again we use the function ring $\mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ and the fact that $\mathbb{K}[Z^*] \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ by mapping the polynomials to the respective functions in $\mathcal{F}_{\mathbb{K}}^{Z^*} \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$.

Theorem 5.4.2
Let $\mathfrak{i} = \mathsf{ideal}(\{z_1 - f_1, \ldots, z_n - f_n\}) \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$. *Then* $\mathsf{ker}(\phi) = \mathfrak{i} \cap \mathbb{K}[Z^*]$.

Proof :
Let $g \in \mathfrak{i} \cap \mathbb{K}[Z^*]$. Then $g = \sum_{j=1}^{n} h_j \star s_j \star h'_j$ with $s_j \in \{z_1 - f_1, \ldots, z_n - f_n\}$, $h_j, h'_j \in \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$. As $\phi(z_j - f_j) = o$ for all $1 \leq j \leq n$ we get $\phi(g) = o$ and hence $g \in \mathsf{ker}(\phi)$.
To see the converse let $g \in \mathsf{ker}(\phi)$. Then $g \in \mathbb{K}[Z^*]$ and hence $g = \sum_{j=1}^{m} \alpha_j \cdot w_j$ where $w_j \in Z^*$, $1 \leq j \leq m$. On the other hand we know $\phi(g) = o$. Then

$$\begin{aligned} g &= g - \phi(g) \\ &= \sum_{j=1}^{m} \alpha_j \cdot w_j - \sum_{j=1}^{m} \alpha_j \cdot \phi(w_j) \\ &= \sum_{j=1}^{m} \alpha_j \cdot (w_j - \phi(w_j)) \end{aligned}$$

It remains to show that $w - \phi(w) \in \mathfrak{i}$ for all $w \in Z^*$ as this implies $g \in \mathfrak{i} \cap \mathbb{K}[Z^*]$. This will be done by induction on $k = |w|$. For $k = 1$ we get $w = z_i$ for some $1 \leq i \leq n$ and $w - \phi(w) = z_i - f_i \in \mathfrak{i}$. In the induction step let $w \equiv a_1 \ldots a_k$, $a_i \in Z$. Then we get

$$\begin{aligned} & a_1(a_2 \ldots a_k - \phi(a_2 \ldots a_k)) + (a_1 - \phi(a_1))\phi(a_2 \ldots a_k) \\ = \; & a_1 a_2 \ldots a_k - a_1\phi(a_2 \ldots a_k) + a_1\phi(a_2 \ldots a_k) - \phi(a_1)\phi(a_2 \ldots a_k) \\ = \; & a_1 a_2 \ldots a_k - \phi(a_1 \ldots a_k) \end{aligned}$$

Then, as $|a_2 \ldots a_k| = k-1$ the induction hypothesis yields $a_2 \ldots a_k - \phi(a_2 \ldots a_k) \in \mathfrak{i}$ and as of course $a_1 - \phi(a_1) \in \mathfrak{i}$ we find that $a_1 a_2 \ldots a_k - \phi(a_1 \ldots a_k) \in \mathfrak{i}$.

q.e.d.

Now if G is a (weak) Gröbner basis of $\mathfrak{i}$ in $\mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ with respect to an elimination ordering where the elements in Z^* are made smaller than those in $\mathcal{T}$, then $G \cap$

$\mathbb{K}[Z^*]$ is a (weak) Gröbner basis of the kernel of ϕ. Hence, in case finite such bases exist or bases allowing to solve the membership problem, they can be used to treat the following question.

Kernel of a Polynomial Mapping

Given: A set $F = \{z_1 - f_1, \ldots, z_n - f_n\} \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ encoding a mapping $\phi : \mathbb{K}[Z^*] \longrightarrow \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ and an element $f \in \mathbb{K}[Z^*]$.

Problem: $f \in \mathsf{ker}(\phi)$?

Proceeding:
1. Let G be a (weak) Gröbner basis of $\mathsf{ideal}(\{z_1 - f_1, \ldots, z_n - f_n\})$ with respect to an elimination ordering.
2. Let $G' = G \cap \mathbb{K}[Z^*]$.
3. If $f \xrightarrow{*}_{G'} o$, then $f \in \mathsf{ker}(\phi)$.

A similar question can be asked for the image of a polynomial mapping.

Image of a Polynomial Mapping

Given: A set $F = \{z_1 - f_1, \ldots, z_n - f_n\} \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ encoding a mapping $\phi : \mathbb{K}[Z^*] \longrightarrow \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ and an element $f \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$.

Problem: $f \in \mathsf{im}(\phi)$?

Proceeding:
1. Let G be a Gröbner basis of $\mathsf{ideal}(\{z_1 - f_1, \ldots, z_n - f_n\})$ with respect to an elimination ordering.
2. If $f \xrightarrow{*}_{G} h$, with $h \in \mathbb{K}[Z^*]$, then $f \in \mathsf{im}(\phi)$.

The basis for this solution is the following theorem.

Theorem 5.4.3
Let $\mathfrak{i} = \mathsf{ideal}(\{z_1 - f_1, \ldots, z_n - f_n\}) \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ and let G be a Gröbner basis of $\mathfrak{i}$ with respect to an elimination ordering where the elements in Z^* are smaller than those in $\mathcal{T}$. Then $f \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ lies in the image of ϕ if and only if there exists $h \in \mathbb{K}[Z^*]$ such that $f \xrightarrow{*}_{G} h$. Moreover, $f = \phi(h)$.

Proof :
Let $f \in \mathsf{im}(\phi)$, i.e., $f \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$. Then $f = \phi(g)$ for some $g \in \mathbb{K}[Z^*]$. Moreover, $f - g = \phi(g) - g$, and similar to the proof of Theorem 5.4.2 we can show $f - g \in \mathfrak{i}$. Hence, f and g must reduce to the same normal form h with respect to G. As $g \in \mathbb{K}[Z^*]$ this implies $h \in \mathbb{K}[Z^*]$ and we are done.
To see the converse, for $f \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ let $f \xrightarrow{*}_{G} h$ with $h \in \mathbb{K}[Z^*]$. Then $f - h \in \mathfrak{i}$ and hence $f - h = \sum_{j=1}^{k} g_j \star s_j \star g'_j$ with $s_j \in \{z_1 - f_1, \ldots, z_n - f_n\}$, $g_j, g'_j \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$. As $\phi(s_j) = o$ we get $f - \phi(h) = o$ and hence $f = \phi(h)$ is in the image of ϕ.

q.e.d.

Obviously the question of whether an element lies in the image of ϕ then can be answered in case we can compute a unique normal form of the element with respect to the Gröbner basis of $\mathfrak{i} = \mathsf{ideal}(\{z_1 - f_1, \ldots, z_n - f_n\})$.

Another question is whether the mapping $\phi : \mathbb{K}[Z^*] \longrightarrow \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ is onto. This is the case if for every $t \in \mathcal{T}$ we have $t \in \mathsf{im}(\phi)$. A simpler solution can be found in case $\mathcal{T} \subseteq \Sigma^*$ for some finite set of letters $\Sigma = \{a_1, \ldots, a_k\}$ and additionally $\mathcal{T}$ is subword closed as a subset of Σ^*.

Theorem 5.4.4
Let $\mathfrak{i} = \mathsf{ideal}(\{z_1 - f_1, \ldots, z_n - f_n\}) \subseteq \mathcal{F}_{\mathbb{K}}^{Z^*\mathcal{T}}$ and let G be a Gröbner basis of $\mathfrak{i}$ with respect to an elimination ordering where the elements in Z^* are smaller than those in $\mathcal{T}$. Then $f \in \mathcal{F}_{\mathbb{K}}^{\mathcal{T}}$ is onto if and only if for each $a_j \in \Sigma$, we have $a_j \xrightarrow{*}_G h_j$ where $h_j \in \mathbb{K}[Z^*]$. Moreover, $a_j = \phi(h_j)$.

Proof :
Remember that ϕ is onto if and only if $a_j \in \mathsf{im}(\phi)$ for $1 \leq j \leq k$.
Let us first assume that ϕ is onto, i.e., $a_1, \ldots, a_k \in \mathsf{im}(\phi)$. Then by Theorem 5.4.3 there exist $h_j \in \mathbb{K}[Z^*]$ such that $a_j \xrightarrow{*}_G h_j$, $1 \leq j \leq k$.
To see the converse, again, by Theorem 5.4.3 the existence of $h_j \in \mathbb{K}[Z^*]$ such that $a_j \xrightarrow{*}_G h_j$, $1 \leq j \leq k$ now implies $a_1, \ldots, a_k \in \mathsf{im}(\phi)$ and we are done.
q.e.d.

5.5 Systems of One-sided Linear Equations in Function Rings over the Integers

Let $\mathcal{F}_{\mathbb{Z}}$ be the function ring over the integers $\mathbb{Z}$ as specified in Section 4.2.3. Additionally we require that multiplying terms by terms results in terms, i.e., $\star : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$. Then a reduction relation can be defined for $\mathcal{F}_{\mathbb{Z}}$ as follows:

Definition 5.5.1
Let p, f be two non-zero polynomials in $\mathcal{F}_{\mathbb{Z}}$. We say f **reduces** p **to** q **at** $\alpha \cdot t$ **in one step**, i.e. $p \longrightarrow_g q$, if

(a) $t = \mathsf{HT}(f \star u) = \mathsf{HT}(f) \star u$ for some $u \in \mathcal{T}$.

(b) $\mathsf{HC}(f) > 0$ and $\alpha = \mathsf{HC}(f) \cdot \beta + \delta$ with $\beta, \delta \in \mathbb{Z}$, $\beta \neq 0$, and $0 \leq \delta < \mathsf{HC}(f)$.

(c) $q = p - f \star (\beta \cdot u)$.

The definition of s-polynomials can be derived from Definition 4.2.66.

Definition 5.5.2
Let p_1, p_2 be two polynomials in $\mathcal{F}_{\mathbb{Z}}$. If there are respective terms $t, u_1, u_2 \in \mathcal{T}$ such that $\mathsf{HT}(p_i) \star u_i = \mathsf{HT}(p_i \star u_i) = t \geq \mathsf{HT}(p_i)$ let $HC(p_i) = \gamma_i$.
Assuming $\gamma_1 \geq \gamma_2 > 0$[1], there are $\beta, \delta \in \mathbb{Z}$ such that $\gamma_1 = \gamma_2 \cdot \beta + \delta$ and $0 \leq \delta < \gamma_2$ and we get the following s-polynomial

$$\mathsf{spol}(p_1, p_2, t, u_1, u_2) = \beta \cdot p_2 \star u_2 - p_1 \star u_1.$$

The set $\mathsf{SPOL}(\{p_1, p_2\})$ then is the set of all such s-polynomials corresponding to p_1 and p_2. ◇

Notice that two polynomials can give rise to infinitely many s-polynomials. A subset C of these possible s-polynomials $\mathsf{SPOL}(p_1, p_2)$ is called a stable localization if for any possible s-polynomial $p \in \mathsf{SPOL}(p_1, p_2)$ there exists a special s-polynomial $h \in C$ such that $p \longrightarrow_h o$.

In the following let $f_1, \ldots, f_m \in \mathcal{F}_{\mathbb{Z}}$. We describe a generating set of solutions for the linear one-sided inhomogeneous equation $f_1 \star X_1 + \ldots + f_m \star X_m = f_0$ in the variables $X_1, \ldots, X_m$ provided a finite computable right Gröbner basis of the right ideal generated by $\{f_1, \ldots, f_m\}$ in $\mathcal{F}_{\mathbb{Z}}$ exists.

In order to find a generating set of solutions we have to find *one* solution of

$$f_1 \star X_1 + \ldots + f_m \star X_m \;=\; f_0 \tag{5.1}$$

and if possible a finite set of generators for the solutions of the homogeneous equation

$$f_1 \star X_1 + \ldots + f_m \star X_m \;=\; o. \tag{5.2}$$

We proceed as follows assuming that we have a *finite* right Gröbner basis of the right ideal generated by $\{f_1, \ldots, f_m\}$:

1. Let $G = \{g_1, \ldots, g_n\}$ be a right Gröbner basis of the right ideal generated by $\{f_1, \ldots, f_m\}$ in $\mathcal{F}_{\mathbb{Z}}$, and $\mathbf{f} = (f_1, \ldots, f_m)$, $\mathbf{g} = (g_1, \ldots, g_n)$ the corresponding vectors. There are two linear mappings given by matrices $P \in \mathsf{M}_{m \times n}(\mathcal{F}_{\mathbb{Z}})$, $Q \in \mathsf{M}_{n \times m}(\mathcal{F}_{\mathbb{Z}})$ such that $\mathbf{f} \cdot P = \mathbf{g}$ and $\mathbf{g} \cdot Q = \mathbf{f}$.

2. Equation 5.1 is solvable if and only if $f_0 \in \mathsf{ideal}_r(\{f_1, \ldots, f_m\})$. This is equivalent to $f_0 \overset{*}{\longrightarrow}{}^{\mathrm{r}}_G 0$ and the reduction sequence gives rise to a representation $f_0 = \sum_{i=1}^{n} g_i \star h_i = \mathbf{g} \cdot \mathbf{h}$ where $\mathbf{h} = (h_1, \ldots, h_n)$. Then, as $\mathbf{f} \cdot P = \mathbf{g}$, we get $\mathbf{g} \cdot \mathbf{h} = (\mathbf{f} \cdot P) \cdot \mathbf{h}$ and $P \cdot \mathbf{h}$ is such a solution of equation 5.1.

3. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_r\}$ be a generating set for the solutions of the homogeneous equation

$$g_1 \star X_1 + \ldots + g_n \star X_n \;=\; 0 \tag{5.3}$$

[1]Notice that $\gamma_i > 0$ can always be achieved by studying the situation for $-p_i$ in case we have $HC(p_i) < 0$.

and let I_m be the $m \times m$ identity matrix. Further let $\mathbf{w}_1, \ldots, \mathbf{w}_m$ be the columns of the matrix $P \cdot Q - I_m$. Since $\mathbf{f} \cdot (P \cdot Q - I_m) = \mathbf{f} \cdot P \cdot Q - \mathbf{f} \cdot I_m = \mathbf{g} \cdot Q - \mathbf{f} = 0$ these are solutions of equation 5.2. We can even show that the set $\{P \cdot \mathbf{z}_1, \ldots, P \cdot \mathbf{z}_r, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$ generates all solutions of equation 5.2: Let $\mathbf{q} = (q_1, \ldots, q_m)$ be an arbitrary solution of equation 5.2. Then $Q \cdot \mathbf{q}$ is a solution of equation 5.3 as $\mathbf{f} = \mathbf{g} \cdot Q$. Hence there are $h_1, \ldots, h_r \in \mathcal{F}_{\mathbb{Z}}$ such that $Q \cdot \mathbf{q} = \mathbf{z}_1 \cdot h_1 + \ldots \mathbf{z}_r \cdot h_r$. Further we find

$$\mathbf{q} = P \cdot Q \cdot \mathbf{q} - (P \cdot Q - I_m) \cdot \mathbf{q} = P \cdot \mathbf{z}_1 \cdot h_1 + \ldots P \cdot \mathbf{z}_r \cdot h_r + \mathbf{w}_1 \cdot q_1 + \ldots + \mathbf{w}_m \cdot q_m$$

and hence $\mathbf{q}$ is a right linear combination of elements in $\{P \cdot \mathbf{z}_1, \ldots, P \cdot \mathbf{z}_r, \mathbf{w}_1, \ldots, \mathbf{w}_m\}$.

Now the important part is to find a generating set for the solutions of the homogeneous equation 5.3. In commutative polynomial rings is was sufficient to look at special vectors arising from those situations causing s-polynomials. These situations are again important in our setting:

For every $g_i, g_j \in G$ not necessarily different such that the stable localization $C_{i,j} \subseteq \mathsf{SPOL}(g_i, g_j)$ for the s-polynomials is not empty and additionally we require these sets to be finite, we compute vectors $\mathbf{a}_{ij}^{\ell}$, $1 \leq \ell \leq |C|$ as follows:
Let $t = \mathsf{HT}(g_i \star u) = \mathsf{HT}(g_i) \star u = \mathsf{HT}(g_j) \star v = \mathsf{HT}(g_j \star v)$, $t \geq \mathsf{HT}(g_i)$, $t \geq \mathsf{HT}(g_j)$, be the overlapping term corresponding to $h_\ell \in C_{i,j}$. Further let $\mathsf{HC}(g_i) \geq \mathsf{HC}(g_j) > 0$ and $\mathsf{HC}(g_i) = \alpha \cdot \mathsf{HC}(g_j) + \beta$ for some $\alpha, \beta \in \mathbb{Z}$, $0 \leq \beta < \mathsf{HC}(g_j)$. Then

$$h_\ell = g_i \star u - g_j \star (\alpha \cdot v) = \sum_{l=1}^{n} g_l \star h_l,$$

where the polynomials $h_l \in \mathcal{F}_{\mathbb{Z}}$ are due to the reduction sequence $h_\ell \xrightarrow{*}{}^{\mathrm{r}}_{G} 0$.
Then $\mathbf{a}_{ij}^{\ell} = (a_1, \ldots, a_n)$, where

$$\begin{aligned} a_i &= h_i - u, \\ a_j &= h_j + \alpha \cdot v, \\ a_l &= h_l, \end{aligned}$$

$l \neq i, j$, is a solution of 5.3 as $\sum_{l=1}^{n} g_l \star h_l - g_i \star u + g_j \star \alpha \cdot v = 0$.

If all sets $\mathsf{SPOL}(g_i, g_j)$ are empty for $g_i, g_j \in G$, in the case of ordinary Gröbner bases in polynomial rings one could conclude that the homogeneous equation 5.3 had no solution. This is no longer true for arbitrary function rings.

Example 5.5.3
Let $\mathbb{Z}[\mathcal{M}]$ be a monoid ring where $\mathcal{M}$ is presented by the complete string rewriting system $\Sigma = \{a, b\}$, $T = \{ab \longrightarrow \lambda\}$. Then for the homogeneous equation

$$(a+1) \star X_1 + (b+1) \star X_2 = 0$$

we find that the set $\{a+1, b+1\}$ is a prefix Gröbner basis of the right ideal it generates. Moreover neither of the head terms of the polynomials in this basis is prefix of the other and hence no s-polynomials with respect to prefix reduction exist. Still the equation can be solved: $(b,-1)$ is a solution since $(a+1)\star b-(b+1)=b+1-(b+1)=0$.

Hence inspecting s-polynomials is not sufficient to describe all solutions. This phenomenon is due to the fact that as seen before in most function rings s-polynomials are not sufficient for a Gröbner basis test. Additionally the concept of saturation has to be incorporated. In Example 5.5.3 we know that $(a+1)\star b = 1+b$, i.e. $b+1 \in \mathsf{SAT}(a+1)$. Of course $(a+1)\star b \longrightarrow_{b+1} 0$ and hence $(a+1)\star b = b+1$ gives rise to a solution $(b,-1)$ as required above.

More general we can express these additional solutions as follows: For every $g_i \in G$ with $\mathsf{SAT}(g_i)$ a stable saturator for $\{g_i\}$ and again we additionally require it to be finte, we define vectors $\mathbf{b}_{i,\ell}=(b_1,\ldots,b_n)$ $1 \leq \ell \leq |\mathsf{SAT}(g_i)|$ as follows: For $g_i \star w_\ell \in \mathsf{SAT}(g_i)$ we know $g_i \star w_\ell = \sum_{l=1}^{n} g_l \star h_l$ as G is a Gröbner basis. Then $\mathbf{b}_{i,\ell}=(b_1,\ldots,b_n)$, where

$$\begin{aligned} b_i &= h_i - w_\ell, \\ b_l &= h_l, \end{aligned}$$

$l \neq i$, is a solution of equation 5.3 as $\sum_{l=1}^{n} g_l \star h_l - g_i \star w_\ell = 0$.

Lemma 5.5.4
Let $\{g_1,\ldots,g_n\}$ be a finite right Gröbner basis. For g_i, g_j let $C_{i,j}$ be a stable localization of $\mathsf{SPOL}(g_i,g_j)$. The finitely many vectors $\mathbf{a}_{i,j}^{\ell_1}, \mathbf{b}_{i,\ell_2}$, $1 \leq i,j \leq n$, $1 \leq \ell_1 \leq |C_{i,j}|$, $1 \leq \ell_2 \leq |\mathsf{SAT}(g_i)|$ form a right generating set for all solutions of equation 5.3.

Proof :
Let $\mathbf{p}=(p_1,\ldots,p_n)$ be an arbitrary (non-trivial) solution of equation 5.3, i.e., $\sum_{i=1}^{n} g_i \star p_i = 0$. Let $T_p = \max\{\mathsf{HT}(g_i \star t_j^{p_i}) \mid 1 \leq i \leq n, p_i = \sum_{j=1}^{n_i} \alpha_j^{p_i} \cdot t_j^{p_i}\}$, K_p the number of multiples $g_i \star t_j^{p_i}$ with $T_p = \mathsf{HT}(g_i \star t_j^{p_i}) \neq \mathsf{HT}(g_i) \star t_j^{p_i}$, and $M_p = \{\{\mathsf{HC}(g_i) \mid \mathsf{HT}(g_i \star t_j^{p_i}) = T_p\}\}$ a multiset in $\mathbb{Z}$. A solution $\mathbf{q}$ is called smaller than $\mathbf{p}$ if either $T_q \prec T_p$ or ($T_q = T_p$ and $K_q < K_p$) or ($T_q = T_p$ and $K_q = K_p$ and $M_q \ll M_p$). We will prove our claim by induction on T_p, K_p and M_p and have to distinguish two cases:

1. If there is $1 \leq i \leq n$, $1 \leq j \leq n_i$ such that $T_p = \mathsf{HT}(g_i \star t_j^{p_i}) \neq \mathsf{HT}(g_i) \star t_j^{p_i}$, then there exists $s_\ell \in \mathsf{SAT}(g_i)$ such that $g_i \star t_j^{p_i} = s_\ell \star v$ for some $v \in \mathcal{T}$, $\mathsf{HT}(s_\ell \star v) = \mathsf{HT}(s_\ell) \star v$ and $s_\ell = g_i \star w_\ell$, $w_\ell \in \mathcal{T}$. Then we can set $\mathbf{q} = \mathbf{p} + \alpha_j^{p_i} \cdot \mathbf{b}_{i,\ell} \star v$ with

$$\begin{aligned} q_i &= p_i + \alpha_j^{p_i} \cdot (h_i - w_\ell) \star v \\ q_l &= p_l + \alpha_j^{p_i} \cdot h_l \star v \text{ for } l \neq i \end{aligned}$$

which is again a solution of equation 5.3. It remains to show that it is a smaller one. To see this we have to examine the multiples $g_l \star t_j^{q_l}$ for all $1 \leq l \leq n$, $1 \leq j \leq m_l$ where $q_l = \sum_{j=1}^{m_l} \alpha_j^{q_l} \cdot t_j^{q_l}$. Remember that $\mathsf{HT}(s_\ell) \leq \mathsf{HT}(s_\ell \star v) = \mathsf{HT}(s_\ell) \star v = T_p$. Moreover, for all terms $w_j^{h_l}$ in $h_l = \sum_{j=1}^{m_l} \beta_j^{h_l} \cdot w_j^{h_l}$ we know $w_j^{h_l} \preceq \mathsf{HT}(s_\ell)$, as the h_l arise from the reduction sequence $g_i \star w_\ell \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$, and hence $\mathsf{HT}(w_j^{h_l} \star v) \preceq \mathsf{HT}(s_\ell \star v) = T_p$.

(a) For $l = i$ we get $g_i \star q_i = g_i \star (p_i + \alpha_j^{p_i} \cdot (h_i - w_\ell) \star v) = g_i \star p_i + \alpha_j^{p_i} \cdot g_i \star h_i \star v - \alpha_j^{p_i} \cdot g_i \star w_\ell \star v$ and as $\mathsf{HT}(g_i \star t_j^{p_i}) = \mathsf{HT}(g_i \star w_\ell \star v)$ and the resulting monomials add up to zero we get $\max\{\mathsf{HT}(g_i \star w_j^{h_i}) \mid 1 \leq j \leq m_i\} \leq T_p$.

(b) For $l \neq i$ we get $g_l \star q_l = g_l \star (p_l + \alpha_j^{p_i} \cdot h_l \star v) = g_l \star p_l + \alpha_j^{p_i} \cdot g_l \star h_l \star v$ and $\max\{\mathsf{HT}(g_i \star w_j^{h_l}) \mid 1 \leq j \leq m_l\} \preceq T_p$ as well as $\max\{\mathsf{HT}(g_i \star w_j^{h_l}) \mid 1 \leq j \leq m_l\} \preceq T_p$.

Hence while still in one of the cases we must have $T_q = T_p$, the element $g_i \star t_j^{p_i}$ is replaced by the sum $\sum_{l=1}^{n} g_l \star h_l \star v$ where the h_l arise from the reduction sequence $s_\ell \xrightarrow{*}_G 0$. Let $h_l = \sum_{j=1}^{k_l} \alpha_j^{h_l} \cdot t_j^{h_l}$. Since s_ℓ is stable, for all elements $g_l \star t_j^{h_l}$ involved in the reduction of the head term of s_ℓ we know $\mathsf{HT}(g_l \star t_j^{h_l} \star v) = \mathsf{HT}(g_l) \star t_j^{h_l} \star v = T_p$ and no other elements result in this term. Hence $K_q < K_p$ and $\mathbf{q}$ is smaller than $\mathbf{p}$.

2. Let us now assume there are $1 \leq i_1, i_2 \leq n$, $1 \leq j_1 \leq n_{i_1}$, $1 \leq j_2 \leq n_{i_2}$ such that $\mathsf{HT}(g_{i_1} \star t_{j_1}^{p_{i_1}}) = \mathsf{HT}(g_{i_1}) \star t_{j_1}^{p_{i_1}} = T_p = \mathsf{HT}(g_{i_2}) \star t_{j_2}^{p_{i_2}} = \mathsf{HT}(g_{i_2} \star t_{j_2}^{p_{i_2}})$. Moreover, we assume $\mathsf{HC}(g_{i_1}) \geq \mathsf{HC}(g_{i_2}) > 0$ and $\mathsf{HC}(g_{i_1}) = \alpha \cdot \mathsf{HC}(g_{i_2}) + \beta$, $\alpha, \beta \in \mathbb{Z}$, $0 \leq \beta < \mathsf{HC}(g_{i_2})$. Let $h_{\ell_2} \in C_{i_1,i_2}$ such that for the corresponding s-polynomial $p = g_{i_1} \star t_{j_1}^{p_{i_1}} - \alpha \cdot g_{i_2} \star t_{j_2}^{p_{i_2}}$ we have $p = h_{\ell_2} \star v$ and $h_{\ell_2} = g_{i_1} \star u_1 - g_{i_2} \star (\alpha \cdot u_2)$. Since we have a vector $\mathbf{a}_{i_1,i_2}^{\ell_2}$ corresponding to h_{ℓ_2}, we can define a new solution $\mathbf{q} = \mathbf{p} + \alpha_{j_1}^{p_{i_1}} \cdot \mathbf{a}_{i_1,i_2} \star v$ with

$$\begin{aligned} q_{i_1} &= p_{i_1} + \alpha_{j_1}^{p_{i_1}} \cdot (h_{i_1} - u_1) \star v \\ q_{i_2} &= p_{i_2} + \alpha_{j_1}^{p_{i_1}} \cdot (h_{i_2} + \alpha \cdot u_2) \star v \\ q_l &= p_l + \alpha_{j_1}^{p_{i_1}} \cdot h_l \star v \text{ for } l \neq i, j. \end{aligned}$$

It remains to show that this solution indeed is smaller. To do this we examine the multiples $g_l \star t_j^{q_l}$ for all $1 \leq l \leq n$, $1 \leq j \leq m_l$ where $q_l = \sum_{j=1}^{m_l} \alpha_j^{q_l} \cdot t_j^{q_l}$. Let $h_l = \sum_{j=1}^{k_l} \alpha_j^{h_l} \cdot t_j^{h_l}$. Since the elements $g_l \star t_j^{h_l}$ arise from the reduction sequence $h_{\ell_2} \xrightarrow{*}_G 0$ and the s-polynomial is stable we have additional information on how these elements affect the size of the new solution $\mathbf{q}$. Since $\mathsf{HT}(g_l \star t_j^{h_l}) = \mathsf{HT}(g_l) \star t_j^{h_l} \leq \mathsf{HT}(h_{\ell_2})$ we can conclude $\mathsf{HT}(g_l \star t_j^{q_l}) \leq \mathsf{HT}(h_{\ell_2}) \star v \preceq T_p$ and we get the following boundaries:

(a) For $l \neq i_1, i_2$ we get $g_l \star q_l = g_l \star p_l + \alpha_{j_1}^{p_{i_1}} \cdot g_l \star h_l \star v$. This implies $\max\{\mathsf{HT}(g_l \star t_j^{q_l}) \mid 1 \leq j \leq m_l\} \preceq T_p$.

(b) For $l = i_1$ we get $g_{i_1} \star q_{i_1} = g_{i_1} \star p_{i_1} + \alpha^{p_{i_1}}_{j_1} \cdot g_{i_1} \star h_{i_1} \star v - \alpha^{p_{i_1}}_{j_1} \cdot g_{i_1} \star u_1 \star v$. Since $\alpha^{p_{i_1}}_{j_1} \cdot \mathsf{HM}(g_{i_1}) \star t^{p_{i_1}}_{j_1} = \alpha^{p_{i_1}}_{j_1} \cdot \mathsf{HM}(g_{i_1}) \star u_1 \star v$ we get $\max\{\{\mathsf{HT}(g_{i_1} \star t^{q_{i_1}}_j) \mid 1 \leq j \leq m_{i_1}\} \backslash \{\mathsf{HT}(g_{i_1}) \star t^{p_{i_1}}_{j_1}, \mathsf{HT}(g_{i_1}) \star u_1 \star v\}\} \preceq T_p$.

(c) For $l = i_2$ we get $g_{i_2} \star q_{i_2} = g_{i_2} \star p_{i_2} + \alpha^{p_{i_1}}_{j_1} \cdot g_{i_2} \star h_{i_2} \star v + \alpha^{p_{i_1}}_{j_1} \cdot g_{i_2} \star \alpha \star u_2 \star v$. Again $\max\{\mathsf{HT}(g_{i_1} \star t^{q_{i_1}}_j) \mid 1 \leq j \leq m_{i_1}\} \preceq T_p$.

Now in case $\beta = 0$ we know that the equations are strict as then $\mathsf{HT}(h_{\ell_2}) \star v \prec T_p$ holds. Then either $T_q \prec T_p$ or ($T_q = T_p$ and $K_q < K_p$). If $\beta \neq 0$ we have to be more carefull and have to show that then $M_q \ll M_p$. For the elements $g_l \star t^{h_l}_j$ arising from reducing the head of the s-polynomial we know that $g_l \star t^{h_l}_j \star v$ again has the same head coefficient as $g_l \star t^{h_l}_j$. Now as $\mathsf{HC}(h_{\ell_2}) = \beta$, by the definition of our reduction relation we know that only g_l with $\mathsf{HC}(g_l) \leq \beta$ are applicable. Hence while two elements $\mathsf{HC}(g_{i_1}), \mathsf{HC}(g_{i_2})$ are removed from the multiset M_p only ones less equal to $\beta < \mathsf{HC}(g_{i_2}) \leq \mathsf{HC}(g_{i_1})$ are added and hence the multiset becomes smaller.

Hence we find that in all cases above either $T_q \prec T_p$ or ($T_q = T_p$ and $K_q < K_p$) or ($T_q = T_p$, $K_q = K_p$ and $M_q \ll M_p$). Therefore, in all cases, we can reach a smaller solution and since our ordering on solutions is well-founded, or claim holds.

q.e.d.

Corollary 5.5.5
Let $\{g_1, \ldots, g_n\}$ be a finite right Gröbner basis. For not necessarily finite localizations $C_{i,j} \subseteq \mathsf{SPOL}(g_i, g_j)$ and $\mathsf{SAT}(g_i)$ the not necessarily finite set of vectors $\mathbf{a}^{\ell_1}_{i,j}, \mathbf{b}_{i,\ell_2}$, $1 \leq i, j \leq n$, $h_{\ell_1} \in C_{i,j}$, $s_{\ell_2} \in \mathsf{SAT}(g_i)$ forms a right generating set for all solutions of equation 5.3.

The approach extends to systems of linear equations by using Gröbner bases in right modules. A study of the situation for one-sided equations in integer monid and group rings can be found in [Rei00].

Chapter 6

Conclusions

The aim of this work was to give a guide for introducing reduction relations and Gröbner basis theory to algebraic structures. We chose function rings as they allow a representation of their elements by formal sums. This gives a natural link to those algebraic structures known in the literature where the Gröbner basis method works. At the same time function rings provide enough flexibility to subsume these algebraic structures.

In the general setting of function rings we introduced the algebraic terms which are vital in Gröbner basis theory: head monomials, head terms, standard representations, standard bases, reduction relations and of course (weak) Gröbner bases. Incorporating the technique of saturation we could give characterizations of Gröbner bases in terms of critical situations similar to the original approach.

We have established the theory first for right ideals in function rings over fields as this is the easiest setting. This has been generalized to function rings over reduction rings - a very general setting. Then in order to show how more knowledge on the reduction relation can be used to get deeper results on characterizing Gröbner bases, we have studied the special reduction ring $\mathbb{Z}$, which is of interest in the literature. The same approach has been applied to two-sided ideals in function rings with of course weaker results but still providing characterizations of Gröbner bases.

Important algebraic structures where the Gröbner basis method has been successfully applied in the literature have been outlined in the setting of function rings. It has also been shown how special applications from Gröbner basis theory in polynomial rings can be lifted to function rings.

What remains to be done is to find out if this approach can be extended to function rings allowing infinite formal sums as elements. Such an extension would allow to subsume the work of Mora et. al. on power series which resulted in the tangent cone algorithm. These rings are covered by graded structures as defined by Apel in his habilitation ([Ape98]), by monomial structures as defined by Pesch in his PhD Thesis ([Pes97]) and by Mora in “The Eigth variation” (on Gröbner bases). However, these approaches require admissible orderings and hence do not cover general monoid rings.

Bibliography

[AL88] J. Apel and W. Lassner. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *Journal of Symbolic Computation*, 6:361–370, 1988.

[AL94] W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. Graduate Studies in Mathematics, AMS, Providence, 1994.

[Ape88] J. Apel. *Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung*. PhD thesis, Universität Leipzig, 1988.

[Ape98] J. Apel. *Zu Berechenbarkeitsfragen der Idealtheorie*. Habilitationsschrift, Universität Leipzig, 1998.

[BO93] R. Book and F. Otto. *String Rewriting Systems*. Springer, 1993.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, 1965.

[Buc70] B. Buchberger. Ein algorithmisches kriterium für die lösbarkeit eines algebraischen gleichungssystems. *Aequ. Math. 4/3*, 1970.

[Buc83] B. Buchberger. A critical-pair completion algorithm for finitely generated ideals in rings. In *Proc. Logic and Machines: Decision Problems and Complexity*, LNCS 171, pages 137–161. Springer, 1983.

[Buc85] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Multidimensional Systems Theory*, chapter 6, pages 184–232. Reidel, Dordrecht, 1985.

[Buc87] B. Buchberger. Applications of Gröbner bases in non-linear computational geometry. In R. Janßen, editor, *Trends in Computer Algebra*, LNCS 296, pages 52–80. Springer, 1987.

[BW92] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer, 1992.

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer, 1992.

[FCF93] D. Farkas and E. Green C. Feustel. Synergy in the theories of Gröbner bases and path algebras. *Canadian Journal of Mathematics*, 45(4):727–739, 1993.

[Hir64] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. *Annals of Mathematics*, 79:109–326, 1964.

[Hue80] G. Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, 1980.

[Hue81] G. Huet. A complete proof of correctness of the Knuth-Bendix completion algorithm. *Journal of Computer and System Science*, 23(1):11–21, 1981.

[Kel98] B. J. Keller. Alternatives in implementing noncommutative Gröbner basis systems. In *Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995*, pages 127–180. Birkhäuser, 1998.

[KM89] D. Kapur and K. Madlener. A completion procedure for computing a canonical basis for a k-subalgebra. In *Computers and Mathematics*, pages 1–11. Springer, 1989.

[KN85] D. Kapur and P. Narendran. A finite thue system with decidable word problem and without equivalent finite canonical system. *Theoretical Computer Science*, 35:337–344, 1985.

[Kre93] H. Kredel. *Solvable Polynomial Rings.* Verlag Shaker, Aachen, 1993.

[KRK84] A. Kandri-Rody and D. Kapur. An algorithm for computing the Gröbner basis of a polynomial ideal over an Euclidean ring. Technical report, General Electric Company Corporate Research and Development, Schenectady, NY 12345, December 1984.

[KRK88] A. Kandri-Rody and D. Kapur. Computing a Gröbner basis of a polynomial ideal over an Euclidean domain. *Journal of Symbolic Computation*, 6:37–57, 1988.

[KRW90] A. Kandri-Rody and V. Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. *Journal of Symbolic Computation*, 9:1–26, 1990.

[Las85] W. Lassner. Symbol representations of noncommutative algebras. In *EUROCAL'85*, LNCS 204, pages 99–115. Springer, 1985.

[Lau76] M. Lauer. Kanonische Repräsentanten für die Restklassen nach einem Polynomideal. Master's thesis, Universität Kaiserslautern, 1976.

[Lo96] E. Lo. *A Polycyclic Quotient Algorithm.* PhD thesis, Rutgers, New Brunswick, New Jersey, 1996.

[Lo98] E. Lo. A polycyclic quotient algorithm. *Journal of Symbolic Computation*, 25(1), 1998.

[Mad86] K. Madlener. Existence and construction of Gröbner bases for ideals in reduction rings. Universität Kaiserslautern, 1986.

[Mor85] F. Mora. Gröbner bases for non-commutative polynomial rings. In *Proc. AAECC-3*, LNCS 229, pages 353–362. Springer, 1985.

[Mor87] T. Mora. Gröbner bases and the word problem. Genova, 1987.

[Mor89] T. Mora. Gröbner bases for non-commutative algebras. In *Proc. of ISSAC'88*, LNCS 358, pages 150–161, 1989.

[Mor94] T. Mora. An introduction to commutative and non-commutative Gröbner bases. *Theoretical Computer Science*, 134:131–173, 1994.

[MR93a] K. Madlener and B. Reinert. Computing Gröbner bases in monoid and group rings. In M. Bronstein, editor, *Proc. ISSAC'93*, pages 254–263. ACM, 1993.

[MR93b] K. Madlener and B. Reinert. On Gröbner bases in monoid and group rings. SEKI Report SR-93-08, Universität Kaiserslautern, 1993.

[MR97a] K. Madlener and B. Reinert. A generalization of Gröbner bases algorithms to nilpotent group rings. *Applicable Algebra in Engineering, Communication and Computing*, 8(2):103–123, 1997.

[MR97b] K. Madlener and B. Reinert. String rewriting and Gröbner bases – a general approach to monoid and group rings. Reports on Computer Algebra 16, Centre of Computer Algebra, Universität Kaiserslautern, Universität Kaiserslautern, 1997. Online available at http://www.mathematik.uni-kl.de/˜zca.

[MR98a] K. Madlener and B. Reinert. A generalization of Gröbner basis algorithms to polycyclic group rings. *Journal of Symbolic Computation*, 25(1):23–45, 1998.

[MR98b] 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*, pages 408–420. Cambridge University Press, 1998.

[MR98c] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. *Theoretical Computer Science*, 208:3–31, 1998.

[MR98d] K. Madlener and B. Reinert. String rewriting and Gröbner bases – a general approach to monoid and group rings. In M. Bronstein, J. Grabmeier, and V. Weispfenning, editors, *Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995*, volume 15 of *Progress in Computer Science and Applied Logic*, pages 127–180. Birkhäuser, 1998.

[Pan85] L. Pan. On the Gröbner bases of ideals in polynomial rings over a prinicipal ideal domain. Technical report, Department of Mathematics, University of California, Santa Barbara, 1985.

[Pes97] M. Pesch. *Gröbner Bases in Skew Polynomial Rings*. PhD thesis, Universität Passau, 1997.

[Pes98] M. Pesch. Two-sided gröbner bases in iterated ore extensions. In M. Bronstein, J. Grabmeier, and V. Weispfenning, editors, *Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995*, volume 15 of *Progress in Computer Science and Applied Logic*. Birkhäuser, 1998.

[Rei95] B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* PhD thesis, Universität Kaiserslautern, 1995.

[Rei96] B. Reinert. Introducing reduction to polycyclic group rings - a comparison of methods. Reports on Computer Algebra 9, Centre of Computer Algebra, Universität Kaiserslautern, 1996. Online available at http://www.mathematik.uni-kl.de/˜zca.

[Rei00] B. Reinert. Solving systems of linear one-sided equations in integer monoid and group rings. In C. Traverso, editor, *Proc. ISSAC'00*, pages 281–287. ACM, 2000.

[Ros93] A. Rosenmann. An algorithm for constructing Gröbner and free Schreier bases in free group algebras. *Journal of Symbolic Computation*, 16:523–549, 1993.

[Sti87] S. Stifter. A generalization of reduction rings. *Journal of Symbolic Computation*, 4:351–364, 1987.

[Sto90] T. Stokes. Gröbner bases in exterior algebras. *Journal of Automated Reasoning*, 6:233–250, 1990.

[Tri78] W. Trinks. Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *Journal of Number Theory*, 10(4):475–488, 1978.

[Wei87a] V. Weispfenning. Finite Gröbner bases in non-noetherian skew polynomial rings. In P. Wang, editor, *Proc. ISSAC'92*, pages 329–334. ACM, 1987.

[Wei87b] V. Weispfenning. Gröbner basis for polynomial ideals over commutative regular rings. In *Proc. EUROCAL'87*, LNCS 378, pages 336–347. Springer, 1987.

[Zac78] G. Zacharias. Generalized Gröbner bases in commutative polynomial rings. Master's thesis, M. I. T., Dept. of Comp. Sci., 1978.