American Journal of Applied Mathematics
2021; 9(4): 123-140
http://www.sciencepublishinggroup.com/j/ajam
doi: 10.11648/j.ajam.20210904.14
ISSN: 2330-0043 (Print); ISSN: 2330-006X (Online)

SciencePG
Science Publishing Group

An Axiomatic Approach to Gröbner Basis Theory by Examining Several Reduction Principles

Günter Landsmann*, **Christoph Fürst**

Research Institute for Symbolic Computation – RISC Linz, Johannes Kepler University, Linz, Austria

Email address:
landsmann@risc.jku.at (G. Landsmann), Christoph.Fuerst@risc.jku.at (C. Fürst)
*Corresponding author

To cite this article:
Günter Landsmann, Christoph Fürst. An Axiomatic Approach to Gröbner Basis Theory by Examining Several Reduction Principles. *American Journal of Applied Mathematics*. Vol. 9, No. 4, 2021, pp. 123-140. doi: 10.11648/j.ajam.20210904.14

Received: May 28, 2021; **Accepted:** June 26, 2021; **Published:** August 2, 2021

Abstract: Several variants of the classical theory of Gröbner bases can be found in the literature. They come, depending on the structure they operate on, with their own specific peculiarity. Setting up an expedient reduction concept depends on the arithmetic equipment that is provided by the structure in question. Often it is necessary to introduce a term order that can be used for determining the orientation of the reduction, the choice of which might be a delicate task. But there are other situations where a different type of structure might give the appropriate basis for formulating adequate rewrite rules. In this paper we have tried to find a unified concept for dealing with such situations. We develop a global theory of Gröbner bases for modules over a large class of rings. The method is axiomatic in that we demand properties that should be satisfied by a reduction process. Reduction concepts obeying the principles formulated in the axioms are then guaranteed to terminate. The class of rings we consider is large enough to subsume interesting candidates. Among others this class contains rings of differential operators, Ore-algebras and rings of difference-differential operators. The theory is general enough to embrace the well-known classical Gröbner basis concepts of commutative algebra as well as several modern approaches for modules over relevant noncommutative rings. We start with introducing the appropriate axioms step by step, derive consequences from them and end up with the Buchberger Algorithm, that makes it possible to compute a Gröbner basis. At the end of the paper we provide a few examples to illustrate the abstract concepts in concrete situations.

Keywords: Gröbner Bases, Reduction Relations, Rings of Differential Operators, Differential Algebra

1. Introduction

The principal reason for studying Gröbner bases is their utility when dealing with computational questions regarding submodules and quotient modules. As a paradigma we may consider the membership problem for submodules:

> Given modules M, N with $N \subset M$. Decide whether a given element of M belongs to N.

The solution strategy provided by Gröbner basis theory for solving this problem is to set up a family of *reduction steps* $u \longrightarrow v$. The decision process consists in repeatedly applying these reduction steps to an element $u \in M$ until an element v is reached which does not allow further reduction. The nature of this v gives the answer to the question.

In order to satisfy its demands the set ρ of all permitted reduction steps has to obey certain regulations.

1. Being a member of ρ must be effectively decidable.
2. ρ should allow no infinite sequences of reduction steps i.e., every such sequence has to have finite length.
3. The relation ρ has to be designed in such a way that admitted reduction steps do not leave the congruence classes mod N.
4. When $m = u_0 \longrightarrow u_1 \longrightarrow \cdots \longrightarrow u_r = v$ is a maximally exhausted sequence then its terminal node v being irreducible (w.r.t. ρ) is called a *normal form* of u. The demand is now that we must know all possible normal forms contained within N.

These requirements are enough to solve the membership problem for N: To decide whether a given element u is a member of N, simply reduce u until an irreducible v is reached; if $v \in N$ then u is in N, otherwise not.

It is common and useful to request additional properties for ρ. The first is that normal forms be unique. This draft is then described by the two conditions 'Noetherian' and 'Church-Rosser'. Details on confluence of reduction processes are described in the fundamental paper [3]. The second property we want is additivity of irreducibles, i.e., the set I_ρ of normal forms of all elements of M has to be an additive group. Necessarily, this group has to have a decidable membership problem.

The entire conception results in a direct sum decomposition $M = N \oplus I$ - at least as abelian groups. Obviously then the sequence $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ must split. This splitting capability of the module pair $N \subset M$ is the ultimate limit beyond which the concept is meaningless. In addition to the amenity of invertible coefficients, this is the reason why we will focus on modules over rings R that contain a field K. All R-modules are then K-vector spaces and the mentioned limitation vanishes.

Starting in 1965 with his dissertation, Buchberger developed the theory of Gröbner bases into an indispensible tool for algorithmic algebra [5]. The scope of problems that can be solved by means of this tool is vast. Among others, the computation of Hilbert functions and their differential variants (Dimension polynomials) has been a central point of interest.

Already in 1964 Kolchin formulated a fundamental theorem on univariate differential dimension polynomials [20], and [21] (Sect. II.12. Thm. 6).

Levin extended the originally univariate and bivariate dimension polynomials to the multivariate case by using serveral term orders [25-28].

In 2006, Winkler and Zhou introduced Gröbner bases in difference-differential modules using a generalized term order that uses a cover of the group $\mathbb{Z}^n$ by finitely many copies of $\mathbb{N}^n$ (orthant decomposition) [35].

In 2008, Winkler and Zhou extended their 2006-approach to the notion of relative Gröbner bases and applied it to the computation of difference-differential dimension polynomials Splitting the set of derivations and the set of automorphisms, they provided algorithms for the univariate and the bivariate case [36, 37].

In his 2013 paper, C. Dönch pointed out that the algorithm which generates a relative Gröbner basis out of a finite set of generators might not terminate [12]. See also [11]. In the meantime this has been fixed (cf. [18]).

Different viewpoints on the computation and applications of dimension polynomials are presented in [24]. For results on extending a presentation of a base algebra A to the free differential algebra on A see [38].

At the ISSAC 2015 conference, the authors have introduced the notion of Gröbner reduction, a general concept that covers the reduction part of several Gröbner basis techniques appearing in the literature. There, the principal intention has been to provide a scheme that makes it possible to compare such constructions. In particular, the Gröbner basis concepts developed in the papers of Levin, Pauer, Winkler, Zhou for rings of differential operators, Ore algebras etc. have been shown to be subordinate to this scheme. It has then be proved that reduction concepts which obey the axioms of Gröbner reduction allow the derivation of the dimension polynomial of finitely generated modules [15]. Later it has been shown that concepts like reduction relative to several term orders or relative reduction can be expressed in terms of Gröbner reductions [16].

Since its starting point with Buchbergers dissertation the theory has developed in several directions. Gröbner bases of particular types of ideals are treated in [33]. The evolution of the theory towards integro-differential algebras can be seen in [17]. Gröbner bases for operads is developed in [13]. Performing adjoint functor constructions for operated algebras is done in [39]. For Gröbner bases whose element have specific properties see e.g. [4].

In this paper we leave the tight environment that was dictated by the conception of [15]. The notion of reduction relation in a module is analyzed with regard to maximizing the scope of its models. This results in the formulation of four properties that are central for all such relations.

It turns out that the reduction is steered by two parameters: a binary predicate P, and a unary one, i.e., a set X. Accordingly, we are concerned with three items that have to be varied: P, X and the ground ring R. It is not surprising that the nature of R occupies central attentiveness.

Interestingly, the predicate P can be discussed in full generality, ignoring the particular nature of R. This is owed to the fact that the principal task of P is a restrictive one. The reduction has to terminate, and it does so because the predicate P forces this by importing some external structure to the ring. As a consequence, the choice of P has impact on the method of reduction rather than its actual power.

In contrast to the significance of the binary predicate, the unary predicate X is subordinate to the nature of the ring, and it is this nature that has greatest influence on the strength of reduction.

We are interested in rings R that contain a field K as a subring. R is then a free K-module and we assume a fixed K-basis $\Lambda \subset R$ that is considered as part of the structure – we call this a *ring with basis*. There is then a plethora of concepts that allow developing the facets of the theory, in particular when a well-order on the basis Λ is imposed. The nature of R is then discerned by the two *basic structure formulae*, answering the following questions:

Given $c \in K$, $\lambda, \mu \in \Lambda$, what is $\lambda \cdot c$ and $\lambda \cdot \mu$, both expressed in terms of the basis Λ? If $\lambda \cdot c = c\lambda$, then K is central and consequently R is an algebra over K. If, in addition, $1 \in \Lambda$ and $\lambda \cdot \mu \in \Lambda$, then R is the monoid ring $K[\Lambda]$. These cases are discussed in the literature.

In this paper we develop the theory of reductions for rings with basis without assuming such restrictions. As the theory evolves, the unary predicate X, playing the active part in determining the strength of the reduction, is subject to increasing bondage. First, we assume that X is closed under multiplication by scalars. Later we will consider elements of X as being built from two components, one coming from the ground ring, the other from the module. It is this second component which then is called a Gröbner basis, provided that all conditions are satisfied. Under the validity of an appropriate ascending chain condition, by stepwise enlarging X, it is possible to increase the strength of the resulting reduction until all axioms of a Gröbner reduction are satisfied.

The structure of the paper is the following: First we present our four properties axiomatically and derive some elementary consequences. Then we take care of construction principles that eventually result in models of the axioms.

According to the logical conception of the paper, the setup is organized in decreasing generality. We start with the seemingly most comprehensive concepts, and subject them to a process of increasing specialization.

In the last section we consider applications of the concepts to particular rings. The first three examples discuss briefly cases of finite dimension. As Gröbner bases in these can be treated by linear methods, the concepts are of little computational value. Nethertheless we include them here because we feel that they reflect the ideas in a particularly simple way.

Concerning performance, the concepts are suited to turn into algorithmic procedures when specialized to particular situations. For aspects of complexity and computation see e.g. [32] or [23]. Further strengthening of computational power by combining Gröbner bases with characteristic pairs is performed in [31].

In any concrete instance the spezialized concepts will incorporate the computational advantages that come from the specific equipment.

2. Notation

A ring is always an associative ring with a unit element 1 which is preserved by ring homomorphisms. Modules are assumed to be left and unitary. $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Z}^+$ denote the sets of non-negative integers, integers and integers > 0. Most often we consider the additive monoid $\mathbb{N}^p$ equipped with the product partial order $\leq_\pi$ given by

$$a \leq_\pi b \iff \forall_{1 \leq j \leq p}\, a_j \leq b_j.$$

Throughout, R will be a ring, M an arbitrary module over R and K a field. If X is a subset of M then $\mathbb{Z}X$ and RX stand for the abelian group resp. the R-submodule of M generated by X. If $S \subset R$ is a set without additive structure then $SX = \{sx \mid s \in S,\, x \in X\}$. This applies in particular to the group of units $K^\times$ of K in case that $K \subseteq R$.

If not locally introduced otherwise, F denotes a free module over R. The letters X, Y and W are chosen to designate an unspecified set, most often W will be equipped with some kind of (partial) order. $\mathcal{P}(X)$ denotes the set of all subsets of the set X and $\mathcal{P}_{\text{fin}}(X)$ is the subset of all finite subsets. $X + Y = X \setminus Y \cup Y \setminus X$ denotes symmetric difference of sets. A binary relation $\rho \subseteq M \times M$ is considered as a reduction and we write $f \xrightarrow[\rho]{} h$ to indicate that $(f, h) \in \rho$. $f \xrightarrow[\rho]{k} h$ stands for $(f, h) \in \rho^k$, $f \xrightarrow[\rho]{\star} h$ means that there is a finite chain $f = m_0 \xrightarrow[\rho]{} m_1 \xrightarrow[\rho]{} \cdots \xrightarrow[\rho]{} m_r = h$ $(r \geq 0)$ and $f \xrightarrow[\rho]{+} h$ claims that this chain has positive length. Thus, $\rho^+ = \bullet \xrightarrow[\rho]{+} \bullet$ is the transitive closure whereas $\rho^\star = \bullet \xrightarrow[\rho]{\star} \bullet$ denotes the reflexive and transitive closure of ρ. We write $\mathrm{I}_\rho = \{f \in M \mid \nexists h \text{ such that } f \xrightarrow[\rho]{} h\}$ for the set of *ρ-irreducible* elements and $\mathrm{Z}_\rho = (\rho^\star)^{-1}(0)$ for the set of elements f with the property $f \xrightarrow[\rho]{\star} 0$. Using these notions we will omit reference to ρ when the situation under discussion is unambiguous.

The relation ρ is *Noetherian* if it does not allow an infinite sequence $f_1 \longrightarrow f_2 \longrightarrow \cdots$. The equivalence relation generated by ρ is written $\langle\rho\rangle$ or, on occasion, $\xleftrightarrow[\rho]{\star}$. A subset $Y \subseteq M$ is called stable w.r.t. ρ (or ρ-stable) iff $f \longrightarrow h \wedge f \in Y \Rightarrow h \in Y$. A family (V_j) of subsets of M is called ρ-stable iff each V_j is ρ-stable.

3. The General Theory

Let $N \subseteq M$ be an additive subgroup and $\rho \subseteq M \times M$ an arbitrary relation. Consider the following requirements on ρ:

Axiom 1: ρ is Noetherian;

Axiom 2: ρ is congruence preserving, i.e.,

$f \longrightarrow h \Rightarrow f \equiv h \mod N$;

Axiom 3: I is an additive group;

Axiom 4: $I \cap N = 0$

Definition 3.1.

1. ρ is a *reduction for* N iff it satisfies Axioms 1 and 2.
2. ρ is *additive* iff it satisfies Axiom 3.
3. ρ is *a Gröbner reduction for* N iff it satisfies Axioms 1,2,3,4.

The following example demonstrates that the system of Axioms 1 to 4 is trivially consistent.

Example 3.1 (The irrelevant reduction). The empty relation $\emptyset \subset M \times M$ is an additive reduction for arbitrary subgroups $N \subseteq M$. Plainly, $I = M$ and $\emptyset$ is a Gröbner reduction for $N = 0$.

Proposition 3.1. Let $\rho \subseteq M \times M$ be a reduction for $N \subseteq M$. Then:

1. $f \xrightarrow[\rho]{} h \Rightarrow \exists_{n \in N}\, h = f - n$;
2. $M = I + N$;
3. $I \cap N = 0 \iff N = Z$.

If, in addition, ρ is a Gröbner reduction for N then

4. $M = I \oplus N$;
5. ρ is confluent;
6. the sequence $0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$ splits over $\mathbb{Z}$.

Proof. 1. is an equivalent form of Axiom 2. Take $f \in M$ and reduce it to an irreducible $f \xrightarrow{\star} i$. Then $f \equiv i \mod N$ hence $f \in I + N$. Plainly $Z \subseteq N$. If $I \cap N = 0$

and $n \in N$ then $n \xrightarrow{\star} i$ with $i \in I$. Thus $i \in I \cap N = 0$ i.e., $n \in Z$. If, conversely, $N = Z$ then an $i \in I \cap N$ must eventually reduce to 0; as i is irreducible, this reduction is improper, that is, $i = 0$. It remains to show that the RHS implies irreducibility of 0. But if 0 would reduce to some h, this h must be in N and, by assumption, $h \xrightarrow{\star} 0$. This would produce a chain of reductions $0 \longrightarrow h \xrightarrow{\star} 0$ which contradicts the Noetherian property. 4. is a consequence of Proposition 3.1. Assume that $h_1 \longleftarrow f \longrightarrow h_2$. Reduce both h_1, h_2 till irreducibles i_1, i_2 are reached. Then $i_1 \equiv i_2 \mod N$ and therefore $i_1 - i_2 \in I \cap N = 0$ which proves 5. Point 6. is obvious.

Thus, in case of a Gröbner reduction, given an additive section $s\colon M/N \longrightarrow M$ to π, the endomorphism $s \circ \pi$ provides the *normal form* $\mathrm{NF}(f) = (s \circ \pi)(f)$ of elements $f \in M$. Moreover $\mathrm{im}(s \circ \pi) = I$ and each $f \in M$ has a unique representation $f = f_N + \mathrm{NF}(f)$ with $f_N \in N$.

Corollary 3.1. Let ρ be a Gröbner reduction for $N \subseteq M$. Then $\langle \rho \rangle$ equals the congruence modulo N.

Proof. Plainly $\langle \rho \rangle \subseteq \equiv_N$. Conversely, suppose that $f \equiv_N h$. Then $f - h = f_N + \mathrm{NF}(f) - h_N - \mathrm{NF}(h) \in N$. It follows that $\mathrm{NF}(f) - \mathrm{NF}(h) \in N \cap I = 0$. Consequently $f \xrightarrow{\star} \mathrm{NF}(f) = \mathrm{NF}(h) \xleftarrow{\star} h$ witnessing that $(f, h) \in \langle \rho \rangle$.

Lemma 3.1. Let $M' \subseteq M$ be modules, $0 \longrightarrow \ker \varphi \longrightarrow F \xrightarrow{\varphi} M \longrightarrow 0$ a free presentation and ρ a Gröbner reduction for $N = \varphi^{-1}(M')$. Let

$$\begin{aligned} \varphi_\rho : = \{(u, v) \in M \times M \mid \exists_{f \in F}(\varphi(f) \\ = u \wedge v = \varphi(\mathrm{NF}_\rho(f)))\}. \end{aligned}$$

Then $\varphi_\rho \setminus 1_M$ is a Gröbner reduction for M'. In fact, φ_ρ is the projection $M \longrightarrow M$ onto a direct complement of M'.

Proof. The splitting exact sequence induced by ρ extends to a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d] & F \arrow[r, "\pi"] \arrow[d, "\varphi"] & F/N \arrow[r] \arrow[d, "\widetilde{\varphi}"] \arrow[l, bend right, "s"'] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r, "p"] & M/M' \arrow[r] & 0
\end{tikzcd}$$

Evidently, $\widetilde{\varphi}$ is an isomorphism. Let $s' = \varphi s \widetilde{\varphi}^{-1}$. Then

$$ps'\widetilde{\varphi} = p\varphi s \widetilde{\varphi}^{-1}\widetilde{\varphi} = p\varphi s = \widetilde{\varphi}\pi s = \widetilde{\varphi}.$$

Thus, $ps' = 1_{M/M'}$ i.e., $M = M' \oplus \mathrm{im}\, s'$. If $(u, v) \in \varphi_\rho$ then $u = \varphi(f)$ and $v = \varphi(\mathrm{NF}_\rho(f)) = \varphi s \pi(f) = s'\widetilde{\varphi}\pi(f) = s'p\varphi(f) = s'p(u)$. Conversely, $(u, s'p(u)) = (\varphi(f), s'p\varphi(f)) = (\varphi(f), \varphi s \pi(f)) = (\varphi(f), \varphi(\mathrm{NF}_\rho(f)))$ i.e., $(u, s'p(u)) \in \varphi_\rho$.

In the next sections we shall focus on accomplishing the environment for constructing relations that satisfy the Axioms 1 to 4.

4. Construction of Reduction Relations

Because the general complexion of a reduction $\rho \subset M \times M$ for a subgroup $N \subseteq M$ is determined by it, we start discussing Axiom 2.

4.1. Axiom 2

Let d denote subtraction in the module M. That a relation $\rho \subseteq M \times M$ satisfies Axiom 2 can be expressed by the commutativity of the diagram

$$\begin{tikzcd}
M \times M \arrow[r, "d"] & M \\
\rho \arrow[u] \arrow[r, "d'"] & N \arrow[u]
\end{tikzcd}$$

where $d' = d|\rho$ and the upwardly directed arrows denote inclusion. If we let P denote the relation ρ written as a binary predicate and set $X = d(\rho)$ then we obtain

$$f \underset{\rho}{\longrightarrow} h \iff P(f, h) \wedge f - h \in X. \tag{1}$$

If, conversely, $X \subseteq N$ and $P(f, h)$ is an arbitrary predicate then (1) read as a definition for its LHS results in a relation that satisfies Axiom 2. We will therefore constrain reduction relations to this formula. So (1) is the primary scheme subsuming all relations that will emerge in this paper. It is then clear that Axiom 2 is always fulfilled. Moreover

$$f \in I \iff \forall_{x \in X} \neg P(f, f - x). \tag{2}$$

As X and P are the involved parameters we will denote the relation (1) by the symbol $\rho_{(X,P)}$.

Proposition 4.1. Consider a subgroup $N \subseteq M$, a set $X \subseteq N$ and a binary predicate P. If $\rho_{(X,P)}$ is a Gröbner reduction for N then $N = \mathbb{Z}X$.

Proof. $\mathbb{Z}X \subseteq N$ and $I + \mathbb{Z}X \subseteq M$. Take $f \in M$ and reduce it to an irreducible

$$f \longrightarrow h_1 \longrightarrow \cdots \longrightarrow h_r = i \in I$$

Then there are $x_j \in X$ with $i = f - \sum_{j=1}^r x_j$, hence $f = i + \sum_{j=1}^r x_j \in I + \mathbb{Z}X$. Therefore $I + \mathbb{Z}X = M$. Moreover $I \cap \mathbb{Z}X \subseteq I \cap N = 0$. Altogether

$$\mathbb{Z}X \subseteq N \wedge I + \mathbb{Z}X = I + N \wedge I \cap \mathbb{Z}X = I \cap N$$

which proves that $\mathbb{Z}X = N$.

Proposition 4.2. Let X, Y be sets and let P, Q denote predicates. Assume that $Y \subseteq X$ and $Q \subseteq P$. If $\rho_{(X,P)}$ is Noetherian then $\rho_{(Y,Q)}$ is a reduction for $\mathbb{Z}Y$.

4.2. Axiom 1

We will modulate the parameters present in Formula (1) in order to come along with the remaining axioms. This depends on the situation, that is, on the equipment provided by the actual candidates for R, M and N.

In order to warrant Axiom 1 we need to import a Noetherian structure from some well-founded set.

Definition 4.1. Let $(W, \leq)$ be a partially ordered set, $v\colon M \longrightarrow W$ and $V\colon W \longrightarrow \mathcal{P}(M)$ functions and $X \subseteq M$ a set. We consider the following relations.

1) $\rho_{(X,v)}\colon f \longrightarrow h \iff f - h \in X \wedge v(h) < v(f).$

2) $\rho_{(X,V)}\colon f \longrightarrow h \iff f - h \in X$
$\wedge \forall_{w \in W} \big(f \in V(w) \Rightarrow \exists_{z<w}\, h \in V(z)\big).$

Evidently $\rho_{(X,v)}$ and $\rho_{(X,V)}$ are of type (1) for the obvious predicates P. We will refer to a function $v\colon M \longrightarrow W$ as a *rank* for M with values in W.

The function $V\colon W \longrightarrow \mathcal{P}(M)$ is called monotone and exhaustive when

$$w_1 \leq w_2 \Rightarrow V(w_1) \subseteq V(w_2) \text{ and } \bigcup_{w \in W} V(w) = M.$$

Proposition 4.3. Let $(W, \leq)$ be well-founded, $v\colon M \longrightarrow W$ a rank, and $V\colon W \longrightarrow \mathcal{P}(M)$ monotone and exhaustive. Then

1. $\rho_{(X,v)}$ is a reduction for $\mathbb{Z}X$. If, moreover, $(W, \leq)$ is a well-order then
$$I = \{f \mid \forall_{x \in X}\, v(f) \leq v(f - x)\}.$$
2. $\rho_{(X,V)}$ is a reduction for $\mathbb{Z}X$ with irreducibles
$$I = \Big\{f \mid \forall_{x \in X}\, \exists_{w \in W}\, \big(f \in V(w) \wedge \neg \exists_{z<w}\, f - x \in V(z)\big)\Big\}.$$
Moreover, V is stable w.r.t. $\rho_{(X,V)}$.

Proof. Both relations are congruence preserving w.r.t. $\mathbb{Z}X$. Since W is well-founded $\rho_{(X,v)}$ satisfies Axiom 1. As to the second relation, consider a sequence of $\rho_{(X,V)}$-steps

$$f \longrightarrow f_1 \longrightarrow f_2 \longrightarrow \cdots \tag{3}$$

Choose $w \in W$ with $f \in V(w)$. Then there exists $z_1 < w$ with $f_1 \in V(z_1)$. To the same effect there is an $z_2 < z_1$ with $f_2 \in V(z_2)$. Iteration produces a sequence in W, descending w.r.t. $<$. Since this sequence must terminate after finitely many steps so does (3), thus $\rho_{(X,V)}$ is Noetherian. From its definition it is clear that the family $(V(w))_{w \in W}$ is $\rho_{(X,V)}$-stable.

4.3. Axiom 3

Fixing the predicate P, the only tool for influencing the behavior of the irreducibles is scaling the generating set X. This will be elaborated in the sequel by adjusting X due to the configuration available in the type of ring under consideration.

4.4. Axiom 4

In general when constructing a reduction for N Axiom 4 will not hold. In this case we will try to achieve it by extending the set X. This is what the classical Buchberger algorithm does. Also here a general instruction is beyond our control.

Example 4.1. Consider $M = \mathbb{R}^2$ as a vector space over $\mathbb{R}$, $N = 0 \times \mathbb{R}$, $X \subseteq N$. Let the rank function $\operatorname{rk}\colon M \longrightarrow \mathbb{N}$, be given as $\operatorname{rk}(f_1, f_2) = \lfloor |f_2| \rfloor$, and consider the reduction $\rho_{(X,\operatorname{rk})}$. Because $\operatorname{rk}(f) = 0\ \forall f \in \mathbb{R} \times (-1, 1)$ it follows that $\mathbb{R} \times (-1, 1) \subseteq I$ and therefore $I \cap N \supseteq 0 \times (-1, 1)$ no matter how $X \subseteq N$ is chosen.

This example shows that, in this generality, we cannot expect to construct a Gröbner reduction by simply enlarging X. The reason is, that the group N contains elements $f \neq 0$ of minimal rank. To achieve Axiom 4 this has to be prevented.

Proposition 4.4. Let $N \subseteq M$ be a subgroup and assume that the rank function $\operatorname{rk}\colon M \longrightarrow W$ satisfies $\operatorname{rk}(0) < \operatorname{rk}(f)$ $\forall f \neq 0$. Then any $X \subseteq N$ can be extended to a set $Y \supseteq X$ such that $\rho_{(Y,\operatorname{rk})}$ satisfies Axiom 4.

Proof. As a witness choose $Y = N$ and take $f \in N \setminus 0$. Then $f - 0 \in Y$ and $\operatorname{rk}(0) < \operatorname{rk}(f)$, that means, $f \longrightarrow 0$. Consequently $I \cap N = 0$.

5. Well-founded Orders

Throughout this chapter we assumme that $(W, \leq)$ is a well-founded partially ordered set. Regarding Axiom 1., the importance of such a set is evident. Later we will consider the case where $(W, \leq)$ is even a well-order.

Definition 5.1. Let $V\colon W \longrightarrow \mathcal{P}M$ be a mapping. The difference function of V is the map $V'\colon W \longrightarrow \mathcal{P}M$,
$V'(x) = V(x) \setminus \bigcup_{y<x} V(y)$.

We consider the following requirements on the function V:

1. $x < y \iff V(x) \subset V(y)$;
2. V' provides a partition on M;

Proposition 5.1. Let $\mathcal{F}(W, M)$ be the set of all mappings $W \longrightarrow \mathcal{P}(M)$ that satisfy conditions 1. 2., and $\mathcal{E}(M, W)$ the set of surjections $M \longrightarrow W$. We set

$$F(v) = \Big\{\big(x, \bigcup_{y \leq x} v^{-1}(y)\big) \mid x \in W\Big\}$$

and

$$E(V) = \big\{(m, x) \mid x \in W \wedge m \in V'(x)\big\}.$$

Then $\mathcal{E}(M, W) \underset{E}{\overset{F}{\rightleftarrows}} \mathcal{F}(W, M)$ are bijections inverse to each other.

Proof. $m \in F(v)(x) \iff v(m) \leq x$ and $F(v)'(x) = v^{-1}(x)$, hence $\{F(v)'(x) \mid x \in W\}$ is a partition of M and $F(v)(x) = \bigcup_{y \leq x} F(v)'(y)$. Plainly

$$x < y \iff F(v)(x) \subset F(v)(y).$$

Thus F takes values in $\mathcal{F}(W, M)$. Conversely, for each $V \in \mathcal{F}(W, M)$, $E(V)\colon M \longrightarrow W$ is surjective.

Let $\omega := E(V)$. Plainly $\omega(m) = x \iff m \in V'(x)$, therefore $m \in V'(\omega(m))$.

$$F(\omega)(x) = \bigcup_{y \leq x} \omega^{-1}(y),$$

and

$$m \in F(\omega)(x) \iff \omega(m) \le x.$$

Thus, when $m \in F(\omega)(x)$ then $\omega(m) \le x$ and so $m \in V'(\omega(m)) \subseteq V(\omega(m)) \subseteq V(x)$ by monotonicity of V. This shows that $F(\omega)(x) \subseteq V(x)$. Conversely, assume that $m \in V(x)$. Let y be a minimal member of $\{z \le x \mid m \in V(z)\}$. Then $y \le x$ and $m \in V'(y)$. Since also $m \in V'(\omega(m))$ it follows that $\omega(m) \le x$ whence $m \in F(\omega)(x)$. Consequently $F \circ E = \mathrm{id}$.

For the second equation take a surjection $v\colon M \longrightarrow W$. The set of sets $F(v)'(x) = v^{-1}(x)$ is precisely the partition of W where v is constant on each of its constituents. Comparison with the definition of $E \circ F(v)$ convinces us that also $E \circ F = \mathrm{id}$.

The proposition says that surjective rank-functions are one-one associated with certain monotone exhaustive functions, we call them the corresponding *monotone exhaustive families*. The next proposition says that their associated reduction relations coincide.

Corollary 5.1. Let $\mathrm{rk}\colon M \longrightarrow W$ be surjective and $V\colon M \longrightarrow \mathcal{P}M$ the corresponding monotone exhaustive family. Then, for arbitrary set $X \subseteq M$, we have that $\rho_{(X,\mathrm{rk})} = \rho_{(X,V)}$.

Proof. Take $(f,h) \in \rho_{(X,\mathrm{rk})}$ and $f \in V(w)$. Then $\mathrm{rk}(f) \le w$, and so $\mathrm{rk}(h) < \mathrm{rk}(f) \le w$. Therefore $\exists y < w$ with $h \in \mathrm{rk}^{-1}(y) \subseteq V(y)$. Consequently $(f,h) \in \rho_{(X,V)}$. Conversely, assume that $(f,h) \in \rho_{(X,V)}$. Let $w := \mathrm{rk}(f)$. Then $f \in \mathrm{rk}^{-1}(w) \subseteq V(w)$. So there $\exists y < w$ with $h \in V(y) = \bigcup_{z \le y} \mathrm{rk}^{-1}(z)$. Thus, $\exists z \le y$ s.t. $h \in \mathrm{rk}^{-1}(z)$. Therefore $\mathrm{rk}(h) = z \le y < w = \mathrm{rk}(f)$. We conclude that $(f,h) \in \rho_{(X,\mathrm{rk})}$.

Plainly we may always assume that a rank function is surjective. By violating some of the properties 1. 2., Proposition 5.1 shows that the set of monotonous and exhaustive functions $W \longrightarrow M$ is richer than the set $\mathcal{E}(M,W)$.

A particularly important class of monotone and exhaustive families of subsets of M is the class of $\mathbb{N}^p$-indexed filtrations.

Definition 5.2. By a p-fold filtration on R we mean a family of additive subgroups $R_k \subseteq R$, indexed by $k \in \mathbb{N}^p$, such that

1. $R_k \cdot R_l \subseteq R_{k+l}$;
2. $k \le_\pi l \Rightarrow R_k \subseteq R_l$;
3. $R = \bigcup_{k\in\mathbb{N}^p} R_k$.

R together with such a filtration is called a *(p-fold) filtered ring*.

Definition 5.3. Let $R = \bigcup_{k\in\mathbb{N}^p} R_k$ be a filtered ring and M an R-module. A filtration of M w.r.t. the filtered ring R is a family of additive subgroups $\mathcal{F}_k(M) \subseteq M$ ($k \in \mathbb{N}^p$) with the properties

1. $R_k \cdot \mathcal{F}_l(M) \subseteq \mathcal{F}_{k+l}(M)$;
2. $k \le_\pi l \Rightarrow \mathcal{F}_k(M) \subseteq \mathcal{F}_l(M)$;
3. $M = \bigcup_{k\in\mathbb{N}^p} \mathcal{F}_k(M)$.

M together with a filtration is called a *filtered module* over the filtered ring R.

From its axioms a filtration is a monotone and exhaustive function on the well-founded set $(\mathbb{N}^p, \le_\pi)$. Proposition 4.3 yields

Corollary 5.2. Let $\mathcal{F}$ be a filtration on M and $X \subseteq M$. The relation $\rho_{(X,\mathcal{F})}$ is a reduction for $\mathbb{Z}X$ and the filtration $\mathcal{F}$ is stable w.r.t. $\rho_{(X,\mathcal{F})}$.

Proposition 5.2 (Properties of $\rho_{(X,\mathcal{F})}$).

1. $\mathcal{F}_0(M) \subseteq I \wedge X \setminus \mathcal{F}_0(M) \subseteq Z$;
2. $f \in I \iff \forall_{x\in X}\, \exists_{k\in\mathbb{N}^p} \big(f \in \mathcal{F}_k(M) \wedge \not\exists_{l<_\pi k}\, f - x \in \mathcal{F}_l(M)\big)$.

Proof. If $f \in \mathcal{F}_0(M)$ were reducible there should be an $l \in \mathbb{N}^p$ being smaller than 0, which is impossible. Take $f \in X \setminus \mathcal{F}_0(M)$. Then $f - 0 \in X$ and $f \in \mathcal{F}_k(M)$ implies that $k \ne 0$. Therefore $0 <_\pi k \wedge 0 \in \mathcal{F}_0(M)$ which shows that $f \longrightarrow 0$. Consequently $0 \in Z$. The characterization of the irreducibles is obvious.

Plainly, well-ordered sets are optimal for the values of a rank function. Often we will use them in an extended version.

Definition 5.4. Let W be a linearly ordered set. For $A, B \in \mathcal{P}_{\mathrm{fin}}(W)$ we set

$$A < B \iff \max(A + B) \in B. \tag{4}$$

Proposition 5.3. Let W be linearly ordered, $A, B \in \mathcal{P}_{\mathrm{fin}}(W)$ and $x, y \in W$.

1. (4) is a linear order on $\mathcal{P}_{\mathrm{fin}}(W)$.
2. $A < B \iff \max(A + B) = \max(B \setminus A)$;
3. $A \subset B \Rightarrow A < B$;
4. $\{x\} < \{y\} \iff x < y$.
5. If W is well-ordered then (4) is a well-order on $\mathcal{P}_{\mathrm{fin}}(W)$;

Thus, the well-order (4) extends both, inclusion and a given well-order on W.

6. Rings and Modules with Basis

Assume that the field K is a subring of R. We fix a K-basis $\Lambda \subset R$, so that $R = K^{(\Lambda)}$. Let $F = R^{(E)}$ be the free R-module on the set E. Then $F = K^{(\Lambda E)}$ and each element $f \in F$ has a unique representation

$$f = \sum_{t\in\Lambda E} f_t t \quad (f_t \in K).$$

For $f \in F$ its set of *terms* is $\mathrm{T}(f) = \{t \in \Lambda E \mid f_t \ne 0\}$. In particular, for ring elements $r \in R$, $\mathrm{T}(r) = \{\lambda \in \Lambda \mid r_\lambda \ne 0\}$.

The K-bases Λ and ΛE will be considered as part of the structure and R (F) is called a ring (module) with K-basis. We write $\pi_t(f) = f_t$ for the projection function $\pi_t\colon F \longrightarrow K$ ($t \in \Lambda E$). For a term $s = \lambda e \in \Lambda E$ ($\lambda \in \Lambda$, $e \in E$) we set $\pi^1(s) = \lambda$, $\pi^2(s) = e$. This gives the projection functions $\pi^1\colon \Lambda E \longrightarrow \Lambda$, $\pi^2\colon \Lambda E \longrightarrow E$. We say that the term s involves the basis element e (cf. [14]). This notation will stay in force for the remainder of the paper.

For the product of $a, b \in R$ we obtain

$$a \cdot b = \sum_{\lambda\in\Lambda} a_\lambda \lambda \cdot \sum_{\mu\in\Lambda} b_\mu \mu = \sum_{\lambda,\mu,\nu,\xi\in\Lambda} a_\lambda (\lambda \cdot b_\mu)_\nu (\nu \cdot \mu)_\xi \xi \tag{5}$$

The two expressions $\lambda \cdot b_u$ and $\nu \cdot \mu$ are responsible for the behaviour of multiplication in R and scalar operation in R-modules. When explicitly exposed these two expressions provide the *basic structure formulae* of R.

In concrete instances the monomials $\lambda \in R$ often carry additional structure. The basic structure formulae simplify then by expressing them in terms of the structural components of the monomials.

We call a submodule $V \subseteq F$ *monomial* when it is generated as an R-module by a subset of ΛE. The submodule V is called *homogeneous* when it is generated over K by such a subset.

Lemma 6.1. Let $V \subseteq F$ be an R-submodule.

1. V is homogeneous $\iff \forall_{f \in V}\, \mathrm{T}(f) \subseteq V$.
2. V homogeneous $\Rightarrow V$ monomial.
3. Let $\Lambda \cdot \Lambda \subseteq \Lambda$. Then V is homogeneous iff it is monomial.

Proof.

1. If $V = KX$ with $X \subseteq \Lambda E$ then $\forall_{f \in V}\, \mathrm{T}(f) \subseteq X \subseteq V$. Conversely, if $\mathrm{T}(f) \subseteq V\ \forall f \in V$ then $X := \bigcup_{f \in V} \mathrm{T}(f) \subseteq V \cap \Lambda E$ and $KX = V$.
2. if $V = KX$ with $X \subseteq \Lambda E$ then $V = KX \subseteq RX \subseteq V$.
3. Let $\Lambda \cdot \Lambda \subseteq \Lambda$ and $V = RX$ with $X \subseteq \Lambda E$. Then $Y := \Lambda X \subseteq \Lambda \cdot \Lambda E \subseteq \Lambda E$ and $KY \subseteq V$. For arbitrary $f \in V$ we obtain

$$f = \sum_{x \in X} r_x x = \sum_{x \in X} \sum_{\lambda \in \Lambda} r^x_\lambda \lambda x = \sum_{y \in Y} \sum_{\lambda x = y} r^x_\lambda y \in KY.$$

6.1. Term Orders

Now assume that $< \subset \Lambda E \times \Lambda E$ is a well-order on the set ΛE. Each non-zero $f \in F$ has then a *leading term* $\mathrm{LT}(f) = \max \mathrm{T}(f)$. The *leading coefficient* of f is the coefficient $\mathrm{LC}(f) = f_{\mathrm{LT(f)}} \in K$. If $X \subseteq F$, we write $\mathrm{LT}(X)$ and $\mathrm{LC}(X)$ for the sets $\{\mathrm{LT}(x) \mid x \in X\}$ and $\{\mathrm{LC}(x) \mid x \in X\}$ respectively.

Let us agree that $\mathrm{LT}(0) = 0$ and $\mathrm{LC}(0) = 1$. We formally enhance an element $f \in F$ to a function $f \colon \Lambda E \cup \{0\} \longrightarrow K$ by setting $f_0 = \mathrm{LC}(f)$. Then for arbitrary $f \in F$ we have that $f_0 \neq 0$. In particular $0_0 = \mathrm{LC}(0) = 1$. We write $F_0 = \{f \in F \mid \mathrm{LC}(f) = 1\}$ for the set of monic elements of F. Note that $0 \in F_0$.

We extend the well-order $<$ on ΛE in several ways.

1. to $\Lambda E \cup \{0\}$ by stipulating $0 < t\, \forall t \in \Lambda E$;
2. to $\mathcal{P}_{\mathrm{fin}}(\Lambda E)$ according to (4). This defines a well-order on $\{\mathrm{T}(f) \mid f \in F\}$;
3. to the module F:

$$\begin{aligned} f \prec g &\iff \mathrm{LT}(f) < \mathrm{LT}(g) \text{ and} \\ f \preceq g &\iff \mathrm{LT}(f) \leq \mathrm{LT}(g). \end{aligned} \tag{6}$$

Then $\preceq$ is a well-founded quasi-order on F.

Proposition 6.1. Let $f, g, h \in F$.

1. $\mathrm{T}(f) + \mathrm{T}(g) \subseteq \mathrm{T}(f+g) \subseteq \mathrm{T}(f) \cup \mathrm{T}(g)$;
2. $\mathrm{T}(f) < \mathrm{T}(g) \iff \max(\mathrm{T}(f) + \mathrm{T}(g)) = \max(\mathrm{T}(g) \setminus \mathrm{T}(f))$;
3. $f \prec g \Rightarrow \mathrm{T}(f) < \mathrm{T}(g)$ and $\mathrm{T}(f) < \mathrm{T}(g) \Rightarrow f \preceq g$;
4. $f \prec g \vee g \prec f \vee \mathrm{LT}(f) = \mathrm{LT}(g)$.

Note that the relation $\prec$ is not the strict version of $\preceq$.

6.2. Reduction in a Module with Basis

We proceed assuming presence of a well-order $<$ on ΛE. Let $X \subseteq F$. We consider three types of reduction relations

$$\begin{aligned} \rho_{\mathrm{LT}}(X)\colon\ f \xrightarrow[\mathrm{LT}]{} h &\iff f - h \in X \wedge h \prec f; \\ \rho_{\mathrm{T}}(X)\colon\ f \xrightarrow[\mathrm{T}]{} h &\iff f - h \in X \wedge T(h) < T(f); \\ \rho_{\mathrm{CR}}(X)\colon\ f \xrightarrow[\mathrm{CR}]{} h &\iff f - h \in X \wedge h_{\mathrm{LT}(f-h)} = 0. \end{aligned} \tag{7}$$

We call $\rho_{\mathrm{LT}}(X)$ *leading term reduction*, $\rho_{\mathrm{T}}(X)$ *T-reduction* and $\rho_{\mathrm{CR}}(X)$ *classical reduction*.

$\rho_{\mathrm{LT}}(X)$ uses the leading term $\mathrm{LT}\colon F \longrightarrow \Lambda E \cup \{0\}$ as a rank. The extended well-order on $\mathcal{P}_{\mathrm{fin}}(\Lambda E)$ provides the map $T\colon F \longrightarrow \mathcal{P}_{\mathrm{fin}}(\Lambda E)$ as a rank function for $\rho_{\mathrm{T}}(X)$. So these are relations of the type considered in Definition 4.1 and therefore both are reductions for $\mathbb{Z}X$. That also $\rho_{\mathrm{CR}}(X)$ is a reduction for $\mathbb{Z}X$ is a consequence of the next proposition. To reduce clumsy notation we shall on occasion suppress the letter ρ writing $\mathrm{CR}(X)$ instead of $\rho_{\mathrm{CR}(X)}$. We even may omit the 'X' when it is obvious from context. A similar convention will be used for the other reduction relations. From (2) we derive immediately

$$\begin{aligned} f \in I_{\mathrm{LT}(X)} &\iff \neg\exists_{x \in X}\, f - x \prec f; \\ f \in I_{\mathrm{T}(X)} &\iff \neg\exists_{x \in X}\, \mathrm{T}(f - x) < \mathrm{T}(f); \\ f \in I_{\mathrm{CR}(X)} &\iff \neg\exists_{x \in X}\, f_{\mathrm{LT}(x)} = \mathrm{LC}(x). \end{aligned}$$

Proposition 6.2. $\rho_{\mathrm{LT}}(X) \subseteq \rho_{\mathrm{CR}}(X) \subseteq \rho_{\mathrm{T}}(X)$.

Proof. Let $f \xrightarrow[\mathrm{LT}]{} h$, that is, $h = f - x \wedge \mathrm{LT}(h) < \mathrm{LT}(f)$. Then $f \neq 0$ and $0 = h_{\mathrm{LT}(f)} = f_{\mathrm{LT}(f)} - x_{\mathrm{LT}(f)}$. Thus $x_{\mathrm{LT}(f)} = \mathrm{LC}(f) \neq 0$, hence $\mathrm{LT}(x) \geq \mathrm{LT}(f) > \mathrm{LT}(h)$ and so $h_{\mathrm{LT}(x)} = 0$. This means that $f \xrightarrow[\mathrm{CR}]{} h$.

Now assume that $f \xrightarrow[\mathrm{CR}]{} h$ with $h = f - x$, $h_{\mathrm{LT}(x)} = 0$. Then $x \neq 0$ since otherwise $0 = h_0 \neq 0$. $f_{\mathrm{LT}(x)} = x_{\mathrm{LT}(x)} = \mathrm{LC}(x) \neq 0$ and $\mathrm{LT}(x) \in \mathrm{T}(f) \setminus \mathrm{T}(h)$. If $f_s = h_s$ then $s \notin \mathrm{T}(f) + \mathrm{T}(h)$. In contraposition, when $s \in \mathrm{T}(f) + \mathrm{T}(h)$ then $f_s \neq h_s$, meaning that $s \in \mathrm{T}(x)$, hence $s \leq \mathrm{LT}(x)$. Therefore $\mathrm{LT}(x) = \max(\mathrm{T}(f) + \mathrm{T}(h)) \in \mathrm{T}(f)$ whence $\mathrm{T}(h) < \mathrm{T}(f)$.

It is plain that these inclusions may be strict.

Lemma 6.2. Let ρ be one of $\rho_{\mathrm{LT}}(X)$, $\rho_{\mathrm{T}}(X)$, $\rho_{\mathrm{CR}}(X)$. Consider a chain of ρ-reductions $f \longrightarrow f_1 \longrightarrow \cdots \longrightarrow f_r$.

Then $\exists\, x_1, \ldots, x_r \in X$ with

$$f = \sum_{k=1}^{r} x_k + f_r \wedge \forall_{1 \leq k \leq r}\, x_k \preceq f.$$

In particular, $f \xrightarrow[\rho]{\star} h \Rightarrow f \equiv h \mod \mathbb{Z}X$.

Proof. For $r = 1$ we obtain that $f_1 = f - x_1 \wedge \mathrm{T}(f_1) < \mathrm{T}(f)$. Thus $f_1 \preceq f$ and $x_1 = f - f_1$, $\mathrm{LT}(x_1) \leq$

$\max\{\mathrm{LT}(f), \mathrm{LT}(f_1)\} = \mathrm{LT}(f)$. Therefore $f = x_1 + f_1 \wedge x_1 \preceq f$.

Assuming that the assertion holds for $r \geq 1$, let $f \xrightarrow{\star} f_{r+1}$ be a reduction chain of length $r+1$. Then

$$\begin{aligned} f &= \sum_{k=1}^{r} x_k + f_r \wedge \forall_{1\leq k\leq r}\, x_k \preceq f \wedge f_{r+1} \\ &= f_r - x_{r+1} \wedge \mathrm{T}(f_{r+1}) < \mathrm{T}(f_r). \end{aligned}$$

$f_{r+1} \preceq f_r$ and $\mathrm{LT}(x_{r+1}) \leq \max\{\mathrm{LT}(f_r), \mathrm{LT}(f_{r+1})\} = \mathrm{LT}(f_r)$ hence $x_{r+1} \preceq f_r \preceq f$. Thus $f = \sum_{k=1}^{r+1} x_k + f_{r+1} \wedge \forall_{1\leq k\leq r+1}\, x_k \preceq f$.

Corollary 6.1. $X \subseteq F$. Then

$$X \subseteq Z_{\mathrm{LT}(X)} \subseteq Z_{\mathrm{CR}(X)} \subseteq Z_{\mathrm{T}(X)} \subseteq \mathbb{Z}X.$$

Proof. Take $f \in X$. If $f = 0$ then $f \xrightarrow{\star} 0$ hence $f \in Z_{\mathrm{LT}(X)}$. Let $f \neq 0$. Then $0 = f - f \wedge \mathrm{LT}(0) = 0 < \mathrm{LT}(f)$ which shows that $f \xrightarrow[\mathrm{LT}]{} 0$, again $f \in Z_{\mathrm{LT}(X)}$. The remaining inclusions are consequences of Proposition 6.2 and Lemma 6.2.

In the sequel we need to impose conditions on the set $X \subseteq F$. This is necessary in order to derive more specific properties of the relation $\rho_{(X,P)}$. A quite strong condition is to request that $X = N$.

Corollary 6.2. Let $N \subseteq F$ be an additive subgroup and ρ one of $\rho_{\mathrm{LT}}(N)$, $\rho_{\mathrm{T}}(N)$, $\rho_{\mathrm{CR}}(N)$. Then $I_\rho \cap N = 0$.

Proof. Specializing $X = N$ in Corollary 6.1 yields $N \subseteq Z_\rho \subseteq \mathbb{Z}N = N$. Proposition 3.1 gives the result.

Of course, the statement of this corollary is of little value. More moderate is it to require that $K^\times X = X$, a condition that we will meet on several occasions. Later we will presume that $X = AG$ for certain sets $A \subseteq R$ and $G \subseteq F$. Note that the condition $K^\times X = X$ implies that $\mathbb{Z}X = KX$; Axiom 2 is then talking about the congruence modulo a vector space.

Proposition 6.3. Let ρ be one of $\rho_{\mathrm{LT}}(X)$, $\rho_{\mathrm{CR}}(X)$, $\rho_{\mathrm{T}}(X)$ where $K^\times X = X$. If $f \xrightarrow[\rho]{} h$ then $\forall_{c\in K^\times}\ cf \xrightarrow[\rho]{} ch$.

6.3. Leading Term Reduction

The function $\mathrm{LT}\colon F \longrightarrow \Lambda E \cup \{0\}$ is a surjection. The corresponding monotone exhaustive family is

$$\mathcal{F}_t = \bigcup_{s\leq t} \mathrm{LT}^{-1}(s) = \{f \in F \mid \mathrm{LT}(f) \leq t\} \quad (t \in \Lambda E).$$

Corollary 5.1 provides that $\rho_{\mathrm{LT}}(X) = \rho_{(X,\mathcal{F})}$ for arbitrary $X \subseteq F$.

6.4. Classical Reduction

Lemma 6.3. Assume $K^\times X = X$. If $u - v \xrightarrow[\mathrm{CR}]{} h'$ then $\exists u', v'$ such that $u \xrightarrow[\mathrm{CR}]{\star} u'$ and $v \xrightarrow[\mathrm{CR}]{\star} v'$ and $u' - v' = h'$.

Proof. Let $h = u - v$, $h' = h - x$ with $h'_{\mathrm{LT}(x)} = 0$. Let $t = \mathrm{LT}(x)$, thus $h_t = x_t = \mathrm{LC}(x)$. Set

$$u' = u - \frac{u_t}{\mathrm{LC}(x)}x \quad v' = v - \frac{v_t}{\mathrm{LC}(x)}x$$

If $u_t = 0$ then $u \xrightarrow{0} u'$. So let $u_t \neq 0$. Then

$$\mathrm{LT}\left(\frac{u_t}{\mathrm{LC}(x)}x\right) = \mathrm{LT}(x) = t$$

and $u'_t = u_t - \frac{u_t}{\mathrm{LC}(x)}x_t = 0$, this means, $u \longrightarrow u'$. In any case $u \xrightarrow{\star} u'$. The same happens to v, i.e. $v \xrightarrow{\star} v'$. Now we get

$$\begin{aligned} u' - v' &= u - \frac{u_t}{\mathrm{LC}(x)}x - v + \frac{v_t}{\mathrm{LC}(x)}x = h + \frac{v_t - u_t}{\mathrm{LC}(x)}x \\ &= h - \frac{u_t - v_t}{\mathrm{LC}(x)}x = h - \frac{h_t}{\mathrm{LC}(x)}x = h' \end{aligned}$$

Proposition 6.4 (Transition). Let $K^\times X = X$. If $u - v = h \xrightarrow[\mathrm{CR}]{\star} h'$ then $\exists u', v'$ such that the below diagram can be augmented by the dotted arrows.

$$\begin{tikzcd} u \arrow[d, dotted, "\mathrm{CR}"', "\star"] & - & v \arrow[d, dotted, "\mathrm{CR}"', "\star"] & = & h \arrow[d, "\mathrm{CR}"', "\star"] \\ u' & - & v' & = & h' \end{tikzcd}$$

Proof. Let $A(k)$ be the formula

$$\begin{aligned} &A(k) \iff \\ &\forall_{h'}\Big(h \xrightarrow[\mathrm{CR}]{k} h' \Rightarrow \exists_{u',v'}\ u \xrightarrow[\mathrm{CR}]{\star} u' \wedge v \xrightarrow[\mathrm{CR}]{\star} v' \\ &\qquad \wedge u' - v' = h'\Big) \end{aligned}$$

If $h \xrightarrow[\mathrm{CR}]{0} h'$ then $h' = h$, hence $u \xrightarrow[\mathrm{CR}]{\star} u$ and $v \xrightarrow[\mathrm{CR}]{\star} v$ and $u - v = h$. Assume $A(k)$ and let $h \xrightarrow[\mathrm{CR}]{k+1} h'$. Then $h \xrightarrow[\mathrm{CT}]{k} h^1 \xrightarrow[\mathrm{CR}]{} h'$. By induction hypothesis

$$\exists_{u^1,v^1}\big(u \xrightarrow[\mathrm{CR}]{\star} u^1 \wedge v \xrightarrow[\mathrm{CR}]{\star} v^1 \wedge u^1 - v^1 = h^1\big)$$

Invoking Lemma 6.3 provides u', v' such that

$$\begin{tikzcd} u \arrow[d, dotted, "\mathrm{CR}"', "\star"] & - & v \arrow[d, dotted, "\mathrm{CR}"', "\star"] & = & h \arrow[d, "\mathrm{CR}"', "k"] \\ u^1 \arrow[d, "\mathrm{CR}"', "\star"] & - & v^1 \arrow[d, "\mathrm{CR}"', "\star"] & = & h^1 \arrow[d, "\mathrm{CR}"', "1"] \\ u' & - & v' & = & h' \end{tikzcd}$$

Generalizing over h^1 yields $A(k+1)$. Consequently $\forall_k A(k)$.

Corollary 6.3. Assume $K^\times X = X$ and let $u - v \xrightarrow[\mathrm{CR}]{\star} 0$. Then $u \xleftrightarrow[\mathrm{CR}]{\star} v$

Proof. Proposition 6.4 yields that

$$\exists_{u^1,v^1} \left(u \xrightarrow[\mathrm{CR}]{\star} u^1 \ \wedge \ v \xrightarrow[\mathrm{CR}]{\star} v^1 \ \wedge u^1 - v^1 = 0 \right).$$

Corollary 6.4. Let $K^\times X = X$. Then $\xleftrightarrow[\mathrm{CR}]{\star} = \xleftrightarrow[\mathrm{T}]{\star} = \ \equiv_{\mathbb{Z}X}$.

Proof. From Proposition 6.2 and the fact that $\rho_{\mathrm{T}}(X)$ is congruence preserving w.r.t. $\mathbb{Z}X$ it is clear that $\xleftrightarrow[\mathrm{CR}]{\star} \ \subseteq \ \xleftrightarrow[\mathrm{T}]{\star} \ \subseteq \ \equiv_{\mathbb{Z}X}$. We show that $\equiv_{\mathbb{Z}X} \subseteq \ \xleftrightarrow[\mathrm{CR}]{\star}$ by induction on the predicate

$$A(k) \iff \forall_{u,v} \left(\exists_{x \in X^{\{1,\dots,k\}}} \, u - v = \sum_{i=1}^{k} x_i \Rightarrow \ u \xleftrightarrow[\mathrm{CR}]{\star} v \right).$$

$A(0)$ is reflexivity of the equivalence relation. Let $u - v = \sum_{i=1}^{k+1} x_i$. Then $u-(v+x_{k+1}) = \sum_{i=1}^{k} x_i$ and from induction hypothesis we obtain $u \xleftrightarrow[\mathrm{CR}]{\star} v + x_{k+1}$. Set $h := v + x_{k+1}$. Then $h - v = \ x_{k+1} \xrightarrow[\mathrm{CR}]{\star} 0$. Proposition 6.4 provides h', v' such that

$$\begin{tikzcd}
h \arrow[d, dotted, "\mathrm{CR}"', "\star"] & - & v \arrow[d, dotted, "\mathrm{CR}"', "\star"] & = & x_{k+1} \arrow[d, "\mathrm{CR}"', "\star"] \\
h' & - & v' & = & 0
\end{tikzcd}$$

which shows that $v + x_{k+1} \ = \ h \xleftrightarrow[\mathrm{CR}]{\star} v$. Consequently $u \xleftrightarrow[\mathrm{CR}]{\star} v$.

6.5. T-Reduction

The rank-function $T \colon F \longrightarrow \mathcal{P}_{\mathrm{fin}}(\Lambda E)$ is a surjection. According to Corollary 5.1 we obtain $\rho_{\mathrm{T}}(X) = \rho_{(X,\tau)}$ ($X \subseteq F$ arbitrary), where

$$\tau_Y = \bigcup_{Z \leq Y} \mathrm{T}^{-1}(Z) = \{f \in F \mid \mathrm{T}(f) \leq Y\}$$

is the corresponding monotone exhaustive family.

Lemma 6.4. Let $X \subseteq F$ be an arbitrary set, $f \in F$, $x \in X$.

1. $f \xrightarrow[\mathrm{T}]{} f - x \ \Rightarrow \mathrm{LT}(x) \in \mathrm{T}(f)$;
2. $f \xrightarrow[\mathrm{T}]{} h = f - x \ \Rightarrow \max\big(\mathrm{T}(f) + \mathrm{T}(h)\big) \leq \mathrm{LT}(x) \leq \mathrm{LT}(f)$.

Proof.

1. Let $f \xrightarrow[\mathrm{T}]{} f - x = h$, $t = \max(\mathrm{T}(f) + \mathrm{T}(h)) = \max(\mathrm{T}(f) \setminus \mathrm{T}(h))$ and $v = \mathrm{LT}(x)$. If $s > v$ then $h_s = f_s$ whence $s \notin \mathrm{T}(f) + \mathrm{T}(h)$. This means $\forall s \, (s \in \mathrm{T}(f) + \mathrm{T}(h) \Rightarrow s \leq v)$ In particular $t \leq v$. Assume for contradiction that $v \notin \mathrm{T}(f)$. Then $h_v = -x_v \neq 0$, that is, $v \in \mathrm{T}(h) \setminus \mathrm{T}(f) \subseteq \mathrm{T}(f) + \mathrm{T}(h)$ and therefore $v \leq t$. Thus $t = v$, a contradiction.

2. $m := \max\big(\mathrm{T}(f) + \mathrm{T}(h)\big) \in \mathrm{T}(f)$ and $\mathrm{LT}(x) \in \mathrm{T}(f)$ hence $\mathrm{LT}(x) \leq \mathrm{LT}(f)$. $m \in \mathrm{T}(f) \setminus \mathrm{T}(h)$, $0 = h_m = f_m - x_m$, $x_m = f_m \neq 0$, $m \in \mathrm{T}(x)$, $m \leq \mathrm{LT}(x)$.

Corollary 6.5. Assume that $K^\times X = X$.

1. $\mathrm{LT}(x) \in \mathrm{T}(f) \Rightarrow \exists_{c \in K^\times} \ f \xrightarrow[\mathrm{CR}]{} f - cx$;
2. $I_{\mathrm{CR}(X)} = I_{\mathrm{T}(X)} = \{f \in F \mid \mathrm{T}(f) \cap \mathrm{LT}(X) = \emptyset\}$.

Proof.

1. $s := \mathrm{LT}(x) \in \mathrm{T}(f)$. Since $s \in \mathrm{T}(f)$ it is clear that $x \neq 0$. Set $c = \frac{f_s}{\mathrm{LC}(x)}$, $y = cx$ and $h = f - y$. Then $y \in X$, $\mathrm{LT}(y) = s$ and $h_s = f_s - cx_s = 0$, this means, $f \xrightarrow[\mathrm{CR}]{} h$.

2. If f is $\mathrm{T}(X)$-reducible then $\exists_{x \in X}$ s.t. $f \xrightarrow[\mathrm{T}]{} f - x$. Lemma 6.4 guarantees then that $\mathrm{LT}(x) \in \mathrm{T}(f)$. Therefore

$$\{f \in F \mid \neg\exists_{x \in X} \, \mathrm{LT}(x) \in \mathrm{T}(f)\} \subseteq I_{\mathrm{T}(X)} \subseteq I_{\mathrm{CR}(X)}.$$

The second point of the same Lemma yields that

$$I_{\mathrm{CR}(X)} \subseteq \{f \in F \mid \neg\exists_{x \in X} \, \mathrm{LT}(x) \in \mathrm{T}(f)\}.$$

Corollary 6.6. Let $X \subseteq F \setminus \{0\}$. Then

1) f is $\mathrm{LT}(X)$-reducible iff $\exists_{x \in X} \big(\mathrm{LT}(x) = \mathrm{LT}(f) \wedge \mathrm{LC}(x) = \mathrm{LC}(f)\big)$;

2) f is $\mathrm{CR}(X)$-reducible iff $\exists_{x \in X} \, f_{\mathrm{LT}(x)} = \mathrm{LC}(x)$.

If $K^\times X = X \setminus \{0\}$ then

3) f is $\mathrm{LT}(X)$-reducible iff $\mathrm{LT}(f) \in \mathrm{LT}(X)$;

4) f is $\mathrm{CR}(X)$-reducible iff $\mathrm{T}(f) \cap \mathrm{LT}(X) \neq \emptyset$.

Corollary 6.7. Assume that $K^\times X = X$ and let ρ be one of $\rho_{\mathrm{CR}}(X)$, $\rho_{\mathrm{T}}(X)$. Then I_ρ is an additive homogeneous subgroup of F.

Proof. This follows immediately from Corollary 6.5.

Note that Corollary 6.7 does not hold for leading-term reduction; that is, in general the irreducibles of $\rho_{\mathrm{LT}}(X)$ neither form a group nor is a term of an irreducible element necessarily irreducible.

We realize that under the assumtions of Corollary 6.7, which is a requirement on the set X, relations $\rho_{\mathrm{CR}(X)}$ and $\rho_{\mathrm{T}(X)}$ both are models of Axioms 1,2,3. Then Corollary 6.2 claims that at least for the case $X = N$, where N is a submodule of F, they provide Gröbner reductions.

These are of course not very useful. We need to specify a set X which is recursively accessible.

Proposition 6.5. Consider two sets $X, Y \subseteq N \subseteq F$ with property $K^\times X = X$, $K^\times Y = Y$. Let ρ_X stand for one of $\rho_{\mathrm{CR}}(X)$, $\rho_{\mathrm{T}}(X)$, and similar for ρ_Y. Assume that ρ_X and ρ_Y are both Gröbner reductions for N. If $X \subseteq Y$ then $I_X = I_Y$.

Proof. From $X \subseteq Y$ we obtain $I_Y \subseteq I_X$ and Corollary 6.7 yields that I_X and I_Y are both groups. Moreover

$$I_X + N = I_Y + N = M \wedge I_X \cap N = I_Y \cap N = 0.$$

Consequently $I_X = I_Y$.

6.6. Reduction for Finitely Generated Submodules

Assume that $N \subseteq F$ is generated by a finite set $G = \{g_1, \dots, g_q\} \subset N$. Let $X \subseteq F$ with $K^\times X = X$ and ρ one of $\mathrm{CR}(X)$, $\mathrm{T}(X)$. The kernel of the corresponding presentation $\Phi\colon R^q \longrightarrow N$ is $\ker(\Phi) = \bigcap_{t \in \Lambda E} \ker(\pi_t \circ \Phi)$ and we obtain that

$$\Phi^{-1}(I \cap N) = \bigcap_{s \in \mathrm{LT}(X)} \ker(\pi_s \circ \Phi).$$

Corollary 6.8. Let $G = \{g_1, \dots, g_q\} \subseteq N$, $\Phi\colon R^q \longrightarrow N$, $X = K^\times X \subseteq N = RG$ and ρ one of $\mathrm{CR}(X)$, $\mathrm{T}(X)$. Then

$$\begin{aligned} &\rho \text{ is a Gröbner reduction for } N \iff \\ &\ker(\Phi) = \bigcap_{s \in \mathrm{LT}(X)} \ker(\pi_s \circ \Phi). \end{aligned} \tag{8}$$

Proof. ρ is a Gröbner reduction for N iff $I \cap N = 0$. This is equivalent to $\Phi^{-1}(I \cap N) = \ker(\Phi)$.

Definition 6.1. Consider an R-submodule $N \subseteq F$. Let $A \subseteq R$ and $G = \{g_1, \dots, g_q\} \subseteq F$ be sets, $X = AG$ and ρ one of $\rho_{\mathrm{LT}}(X)$, $\rho_{\mathrm{CR}}(X)$, $\rho_{\mathrm{T}}(X)$. Then (A, G) is a *ρ-Gröbner basis* for N iff ρ is a Gröbner reduction for N.

Under ideal conditions statement (8) can be used to compute a Gröbner basis:

Consider $r = (r_1, \dots, r_q) \in R^q$ and write

$$r_j = \sum_{\lambda \in \Lambda} r^j_\lambda \lambda \text{ and } g_j = \sum_{t \in \Lambda E} g^j_t t \quad (1 \leq j \leq q). \tag{9}$$

Assume we can solve the system of equations

$$\sum_{j=1}^{q} \sum_{\lambda \in \Lambda} \sum_{\xi \in \Lambda} \sum_{t \in \Lambda E} r^j_\lambda (\lambda \cdot g^j_t)_\xi (\xi \cdot t)_s = 0 \quad (s \in \mathrm{LT}(X)) \tag{10}$$

for the indeterminants r^j_λ and select a solution r with $\Phi(r) \neq 0$. Then we may use $\Phi(r)$ to enlarge the set X, e.g., by setting $G' = G \cup \{\Phi(r)\}$ and defining X' accordingly (such that $K^\times X' = X'$, ρ' is defined by X' and $\mathrm{LT}(X') \supset \mathrm{LT}(X)$). If iterated replication of this process terminates, it will eventually result in a Gröbner reduction for N. Simple examples will follow in Section 7.

In general the system (10) will not be satisfactorily accessible. Then we need more sophisticated concepts which will defined next.

6.7. S-polynomials

To construct Gröbner bases in a finitary way we need an appropriate concept describing S-polynomials.

Definition 6.2. A *quotient function* for F is a map

$$q\colon (\Lambda E \cup 0) \times (\Lambda E \cup 0) \longrightarrow R \times R$$

such that for arbitrary $\lambda, \mu \in \Lambda$, $s, t \in \Lambda E$

1) $q(s, s) = (1, 1)$;

2) $\lambda s = \mu t \Rightarrow \exists_{\omega \in \Lambda}\, \omega \cdot q(s, t) = (\lambda, \mu)$.

We will address the function q in terms of its components, i.e., $q = (q^1, q^2)$.

Example 6.1. Consider $R = K[x_1, \dots, x_n]$, $F = R^{(E)}$. The least common multiple in Λ extends to ΛE via

$$\mathrm{LCM}(\alpha e, \beta e') = \begin{cases} \mathrm{LCM}(\alpha, \beta) e & \dots\ e = e' \\ 0 & \dots \text{ else} \end{cases} \tag{11}$$

($\alpha, \beta \in \Lambda$, $e, e' \in E$). Then

$$q(s, t) = \left(\frac{\mathrm{LCM}(s, t)}{s}, \frac{\mathrm{LCM}(s, t)}{t} \right)$$

is a quotient function.

This example generalizes to situations where $\Lambda \subset R$ admits a least common (left) multiple. Precisely, assume that Λ is a multiplicative monoid which satisfies the cancellation rule $\lambda\nu = \mu\nu \Rightarrow \lambda = \mu$. Assume further that any two elements of Λ have a least common left multiple. Let LCM be a function $\Lambda \times \Lambda \longrightarrow \Lambda$ which picks a least common left multiple for all pairs (λ, μ) and such that $\mathrm{LCM}(\lambda, \lambda) = \lambda$. As in (11) this function extends to $\mathrm{LCM}\colon \Lambda E \times \Lambda E \longrightarrow R \times R$

$$\mathrm{LCM}(s, t) = \begin{cases} \mathrm{LCM}(\pi^1(s), \pi^1(t)) \cdot \pi^2(s) & \pi^2(s) = \pi^2(t) \\ 0 & \text{else.} \end{cases} \tag{12}$$

Then there are functions q^1, q^2 defined implicitly by means of the equations

$$q^1(s, t) \cdot s = \mathrm{LCM}(s, t) = q^2(s, t) \cdot t \quad (s, t \in \Lambda E). \tag{13}$$

We may set $q^1(s, t) = q^2(s, t) = 0$ in case that $\pi^2(s) \neq \pi^2(t)$. When at least one argument is 0, the values of q^1 and q^2 are irrelevant.

Proposition 6.6. $q = (q^1, q^2)$ is a quotient function for F.

Proof. Let $s = \alpha e$, $t = \beta e'$. Because $\mathrm{LCM}(s, s) = \mathrm{LCM}(\alpha, \alpha) e = \alpha e = s$, we obtain from (13) that $q^1(s, s) \cdot s = s = q^2(s, s) \cdot s$. The cancellation rule provides that $q^1(s, s) = 1 = q^2(s, s)$.

Suppose that $\lambda s = \mu t$. This means $\lambda \alpha e = \mu \beta e'$. Since $0 \notin \Lambda$ (Λ is a K-basis of R), we derive that $e = e'$ and $\lambda\alpha = \mu\beta$. In particular $\pi^2(s) = \pi^2(t)$ hence $\mathrm{LCM}(s, t) = \mathrm{LCM}(\alpha, \beta) e$. Since $\lambda\alpha$ is a left multiple of both α and β, there exists a unique $\omega \in \Lambda$ s.t. $\omega \cdot \mathrm{LCM}(\alpha, \beta) = \lambda\alpha$. From (13) we obtain that

$$\begin{aligned} \omega \cdot q^1(s, t) \cdot s &= \omega \cdot \mathrm{LCM}(s, t) = \omega \cdot \mathrm{LCM}(\alpha, \beta) e \\ &= \lambda \alpha e = \lambda s \\ \omega \cdot q^2(s, t) \cdot t &= \omega \cdot \mathrm{LCM}(s, t) = \omega \cdot \mathrm{LCM}(\alpha, \beta) e \\ &= \mu \beta e' = \mu t. \end{aligned}$$

Consequently $\omega \cdot q^1(s, t) = \lambda \wedge \omega \cdot q^2(s, t) = \mu$, shortly $\omega \cdot q(s, t) = (\lambda, \mu)$.

In particular there is a quotient function for F when $\Lambda \cdot \Lambda \subseteq \Lambda \cong \mathbb{N}^n$.

Definition 6.3. An *S-polynomial* is a function

$$S \in \prod_{(f, g) \in F \times F} R \cdot \{f, g\}$$

subject to the following properties.

1. $\forall_{f,g\in F_0}\big(\mathrm{LT}(f)=\mathrm{LT}(g)\Rightarrow S(f,g)=f-g\big)$;
2. $\forall_{f,g\in F_0}\forall_{\lambda,\mu\in\Lambda}\big(\mathrm{LT}(\lambda f)=\mathrm{LT}(\mu g)$
 $\Rightarrow\exists_{\omega\in\Lambda}\, S(\lambda f,\mu g)=\omega\cdot S(f,g)\big)$.

Taking into account condition 1. of this definition one is tempted to write $\lambda f-\mu g$ for $S(\lambda f,\mu g)$ in the second condition. But we have to be careful, since the first condition is required only for $f,g\in F_0$ and it is not guaranteed that $\lambda f\in F_0$ even when $f\in F_0$.

Proposition 6.7. Suppose that $\Lambda\cdot\Lambda\subseteq R\setminus 0$ and $\mathrm{LT}(\lambda f)=\lambda\,\mathrm{LT}(f)\;\forall_{\lambda\in\Lambda}\forall_{f\in F_0}$. If q is a quotient function for F then

$$S(f,g)=q^1(\mathrm{LT}(f),\mathrm{LT}(g))f-q^2(\mathrm{LT}(f),\mathrm{LT}(g))g \quad (14)$$

is an S-polyomial in F.

Proof. Take $f,g\in F_0$. If $\mathrm{LT}(f)=\mathrm{LT}(g)=0$ then $f=g=0$. $S(f,g)=q^1(0,0)0-q^2(0,0)0=0=f-g$. If $\mathrm{LT}(f)=\mathrm{LT}(g)\neq 0$ then $S(f,g)=1\cdot f-1\cdot g$.

Assume that $\mathrm{LT}(\lambda f)=\mathrm{LT}(\mu g)=0$. Then $\lambda\cdot\mathrm{LT}(f)=\mu\cdot\mathrm{LT}(g)=0$. If $\mathrm{LT}(f)$ were different from 0, then $\exists_{\alpha\in\Lambda}\exists_{e\in E}\,\mathrm{LT}(f)=\alpha e$, whence $\lambda\alpha e=0$. But then $\lambda\alpha=0$ contradicting that $0\notin\Lambda\Lambda$. Therefore $\mathrm{LT}(f)=0$ and thus $f=0$. Similarly $g=0$. Therefore $S(f,g)=q^1(0,0)\cdot 0-q^2(0,0)\cdot 0=0$ and $S(\lambda f,\mu g)=S(0,0)=0$. Trivially than $\exists_{\omega\in\Lambda}\,S(\lambda f,\mu g)=\omega S(f,g)$.

Now assume that $\mathrm{LT}(\lambda f)=\mathrm{LT}(\mu g)\neq 0$. Then $\lambda\cdot\mathrm{LT}(f)=\mu\cdot\mathrm{LT}(g)\neq 0$, i.e., $\mathrm{LT}(f),\mathrm{LT}(g)\in\Lambda E$. Therefore $\exists_{\omega\in\Lambda}\,\omega\cdot q(\mathrm{LT}(f),\mathrm{LT}(g))=(\lambda,\mu)$. Consequently

$$\begin{aligned}\omega\,S(f,g)&=\omega\,q^1(\mathrm{LT}(f),\mathrm{LT}(g))f-\omega\,q^2(\mathrm{LT}(f),\mathrm{LT}(g))g\\&=\lambda f-\mu g\\&=q^1(\mathrm{LT}(\lambda f),\mathrm{LT}(\mu g))\lambda f-q^2(\mathrm{LT}(\lambda f),\mathrm{LT}(\mu g))\mu g\\&=S(\lambda f,\mu g).\end{aligned}$$

Lemma 6.5. Let $S\colon F\times F\longrightarrow F$ be an S-polynomial and $f_1,\dots,f_q\in F_0$ with $\mathrm{LT}(f_j)=t\;\forall j=1,\dots,q$. Then

$$K\cdot\{S(f_i,f_q)\mid 1\le i<q\}=\{h\in K\cdot\{f_1,\dots,f_q\}\mid h\prec t\}.$$

Proof. $S(f_i,f_q)_t=(f_i)_t-(f_q)_t=1-1=0$ hence LHS $\subseteq$ RHS. Let $h\in$ RHS, $h=\sum_{j=1}^q c_jf_j$. Then $0=h_t=\sum_{j=1}^q c_j(f_j)_t=\sum_{j=1}^q c_j$. Therefore

$$\sum_{i=1}^{q-1}c_i\cdot S(f_i,f_q)=\sum_{i=1}^{q-1}c_i(f_i-f_q)=\sum_{i=1}^{q-1}c_if_i+c_qf_q=h.$$

6.8. TO-pairs and Syzygies

In most sitations the well-order on ΛE is accompanied by a well-order on Λ.

Definition 6.4. Let $<_R$ be a well-order on Λ and $<_F$ one on ΛE. Extend both according to (6). Then $(<_R,<_F)$ is a TO-pair (a pair of term orders) provided that

1. $\lambda<_R\mu\Rightarrow\lambda f\prec_F\mu f$ $(\lambda,\mu\in\Lambda,\,f\in F_0)$;
2. $\mathrm{LT}(r)f\preceq_F rf$ $(r\in R,\,f\in F_0)$;
3. $f\preceq_F g\Rightarrow\lambda f\preceq_F\lambda g$ $(\lambda\in\Lambda,\,f,g\in F)$.

We will omit subscripts in these relations writing them both as $\prec$ resp. $\preceq$.

Proposition 6.8. Assume $\Lambda\Lambda\subseteq\Lambda$ and a TO-pair with additional properties

1) $\forall_{\lambda\in\Lambda}\forall_{c\in K}\,\lambda\cdot c\preceq\lambda$;

2) $\forall_{\lambda\in\Lambda}\forall_{s,t\in\Lambda E}\,(s<t\Rightarrow\lambda s<\lambda t)$.

Let $\Lambda\subseteq A\subseteq R$, $G\subseteq F_0$, $X=AG$, $\rho=\rho_{\mathrm{T}}(X)$. Then $I\cap\Lambda E\cap R\cdot\mathrm{LT}(G)=\emptyset$.

Proof. Suppose for contradiction that $t\in I\cap\Lambda E\cap R\cdot\{\mathrm{LT}(g)\mid g\in G\}$. Then there are finite subsets $\{g_1,\dots,g_q\}\subseteq G$ and $\{r_1,\dots,r_q\}\subseteq R$ s.t.

$$t=\sum_{j=1}^q r_j\cdot\mathrm{LT}(g_j)=\sum_{j=1}^q\sum_{\lambda\in\Lambda}r^j_\lambda\lambda\cdot\mathrm{LT}(g_j).$$

Since $\Lambda\Lambda\subseteq\Lambda$, this sum must collapse: $\exists_j\exists_\lambda\,t=\lambda\cdot\mathrm{LT}(g_j)$. Consider $h:=t-\lambda g_j$.

$$\begin{aligned}h&=t-\lambda\Big(\mathrm{LT}(g_j)+\sum_{s\prec g_j}g^j_ss\Big)\\&=t-\lambda\cdot\mathrm{LT}(g_j)-\sum_{s\prec g_j}\lambda g^j_ss\\&=-\sum_{s\prec g_j}\sum_{\mu\le\lambda}c_\mu\mu s\end{aligned}$$

where we express λg^j_s as the sum $\sum_{\mu\le\lambda}c_\mu\mu$ justified by the additional property. Each summand is smaller than t, because $s\prec g_j$ and $\mu\le\lambda$ has as a consequence that

$$\mu s<\mu\cdot\mathrm{LT}(g_j)\le\lambda\cdot\mathrm{LT}(g_j)=t.$$

Therefore $\mathrm{T}(h)<t$, and this means that $t\longrightarrow h$ which is impossible.

In order to use reduction relations for performing computations we have to impose finiteness conditions.

Let $N\subseteq F$ be finitely generated by the set $G=\{g_1,\dots,g_q\}$. We consider the associated representation $\Phi\colon R^q\longrightarrow N$, $\phi(r)=\sum_{j=1}^q r_jg_j$ together with the map

$$\delta\colon R^q\longrightarrow\Lambda E,\;\delta(r)=\max_{j=1}^q\mathrm{LT}(r_jg_j).$$

For $t\in\Lambda E$ we set $R_{<t}=\delta^{-1}[0,t)$, i.e., $R_{<t}=\{r\in R^q\mid\delta(r)<t\}$.

Then $\phi(r)\preceq\delta(r)\;\forall r\in R^q$ and $R_{<t}$ is a module over the ring K^q i.e.,

$$r,s\in R_{<t}\wedge c\in K^q\Rightarrow r+s\in R_{<t}\wedge(c_1r_1,\dots,c_qr_q)\in R_{<t}.$$

Moreover we have that

$$r\in R_{<t}\Rightarrow\phi(r)\prec t. \quad (15)$$

We proceed assuming available a TO-pair.

Theorem 6.1. Assume that $\forall_{\lambda\in\Lambda}\forall_{f\in F_0}\,\lambda f\in F_0$ and that F admits an S-polynomial $S\colon F\times F\longrightarrow F$. Let $A\subseteq R$ be such that $\Lambda \subseteq A = K^\times A$, $G = \{g_1, \ldots, g_q\} \subseteq F_0$, $X = AG$ and ρ one of $\rho_{\mathrm{CR}}(X)$, $\rho_{\mathrm{T}}(X)$. If for all $1 \leq i \neq j \leq q$: $S(g_i, g_j) \xrightarrow[\rho]{\star} 0$ then (A, G) is a ρ-Gröbner basis for RG.

Proof. Because $\mathbb{Z}X \subseteq RG$, ρ is a reduction for RG. Since $K^\times X = K^\times AG = AG = X$ we obtain from Corollary 6.7 that ρ satisfies also Axiom 3. It remains to show that $RG \cap I_\rho = 0$.

Assume this is false. Then $\exists f \in RG \cap I \setminus 0$. Take $r \in \phi^{-1}(f)$. We show that $\exists_{s \in \phi^{-1}(f)}\, \delta(s) < \delta(r)$. This produces an infinite descending chain in ΛE contradicting the Noetherian property.

Obviously $\delta(r) > 0$. For arbitrary $1 \leq j \leq q$ we write

$$r_j = c_j \lambda_j + \sum_{\nu < \lambda_j} r^j_\nu \nu, \quad g_j = t_j + \sum_{s < t_j} g^j_s s$$

with $c_j, r^j_\nu, g^j_s \in K$, $\lambda_j = \mathrm{LT}(r_j) \in \Lambda \cup \{0\}$, $c_j = \mathrm{LC}(r_j)$, $t_j = \mathrm{LT}(g_j)$. Then

$$f = \phi(r) \preceq \delta(r) \text{ and } r_j g_j = c_j \lambda_j g_j + \sum_{\nu < \lambda_j} r^j_\nu \nu g_j$$

Definition 6.4 yields $\lambda_j g_j = \mathrm{LT}(r_j) g_j \preceq r_j g_j \preceq \delta(r)$ $(1 \leq j \leq q)$. Let

$$J = \{i \in \{1, \ldots, q\} \mid \mathrm{LT}(\lambda_i g_i) = \delta(r)\}.$$

WLOG $J = \{1, \ldots, k\} \subseteq \{1, \ldots, k, k+1, \ldots, q\}$ with $0 \leq k \leq q$.

$$\begin{aligned} f &= \sum_{j=1}^q c_j \lambda_j g_j + \sum_{j=1}^q \sum_{\nu < \lambda_j} r^j_\nu \nu g_j \\ &= \underbrace{\sum_{i \in J} c_i \lambda_i g_i}_{f^0} + \underbrace{\sum_{i \notin J} c_i \lambda_i g_i}_{f^1} + \underbrace{\sum_{j=1}^q \sum_{\nu < \lambda_j} r^j_\nu \nu g_j}_{f^2} \end{aligned}$$

For $i \notin J$ we obtain $\lambda_i g_i \prec \delta(r)$. Thus $(0, \ldots, 0, \lambda_{k+1}, \ldots, \lambda_q) \in R_{<\delta(r)}$, hence $(0, \ldots, 0, c_{k+1}\lambda_{k+1}, \ldots, c_q \lambda_q) \in R_{<\delta(r)}$. Consequently

$$f^1 = \phi(0, \ldots, 0, c_{k+1}\lambda_{k+1}, \ldots, c_q \lambda_q) \in \phi\big(R_{<\delta(r)}\big)$$

and

$$f^1 \prec \delta(r).$$

For $1 \leq j \leq q$ and $\nu < \lambda_j$ we get from Definition 6.4 that

$$\nu g_j \prec \lambda_j g_j = \mathrm{LT}(r_j) g_j \preceq r_j g_j \preceq \delta(r).$$

Therefore

$$\sum_{\nu < \lambda_j} r^j_\nu \nu g_j \preceq \max_{\nu < \lambda_j} \mathrm{LT}(\nu g_j) \prec \delta(r) \; (j = 1, \ldots, q).$$

Thus

$$\big(\sum_{\nu < \lambda_1} r^1_\nu \nu, \ldots, \sum_{\nu < \lambda_q} r^q_\nu \nu \big) \in R_{<\delta(r)}$$

and so

$$f^2 = \phi\Big(\sum_{\nu < \lambda_1} r^1_\nu \nu, \ldots, \sum_{\nu < \lambda_q} r^q_\nu \nu \Big) \in \phi(R_{<\delta(r)})$$

and

$$f^2 \prec \delta(r).$$

It follows that $f^1 + f^2 \in \phi(R_{<\delta(r)})$. We will show that also $f^0 \in \phi(R_{<\delta(r)})$.

If $J = \emptyset$ (i.e. $k = 0$) then $f^0 = 0$ whence $f^0 \in \phi(R_{<\delta(r)})$. So assume that $J \neq \emptyset$. From Corollary 6.5, $\delta(r) = \mathrm{LT}(\lambda_1 g_1) \notin \mathrm{T}(f)$. Thus

$$0 = f_{\delta(r)} = f^0_{\delta(r)} + f^1_{\delta(r)} + f^2_{\delta(r)} = f^0_{\delta(r)} + 0 + 0.$$

Therefore

$$f^0 = \sum_{i \in J} c_i \lambda_i g_i \wedge \forall_{i \in J} \mathrm{LT}(\lambda_i g_i) = \delta(r) \wedge f^0 \prec \delta(r).$$

If $J = \{1\}$ $(k = 1)$ then $f^0 = c_1 \lambda_1 g_1 \wedge \mathrm{LT}(\lambda_1 g_1) = \delta(r) \wedge f^0 \prec \delta(r)$. Since K is a field, this cannot be.

Therefore $k \geq 2$. Because $\lambda_i g_i \in F_0$ $(1 \leq i \leq k)$, we derive from Lemma 6.5 that

$$\exists_{e \in K^{k-1}}\, f^0 = \sum_{i=1}^{k-1} e_i S(\lambda_i g_i, \lambda_k g_k).$$

From the axioms on S-polynomials we obtain

$$\forall_{i=1,\ldots,k-1} \exists_{\eta_i \in \Lambda}\, S(\lambda_i g_i, \lambda_k g_k) = \eta_i S(g_i, g_k)$$

thus $f^0 = \sum_{i=1}^{k-1} e_i \eta_i S(g_i, g_k)$. Since $S(g_i, g_k) \xrightarrow{\star} 0$ we obtain from Lemma 6.2 that

$$\begin{gathered} \exists_{m \in \mathbb{N}} \exists_{a^i_\bullet \in A^{\{1,\ldots,m\}}} \exists_{g_\bullet \in G^{\{1,\ldots,m\}}} \forall_l \\ a^i_l g_l \preceq S(g_i, g_k) = \sum_{l=1}^m a^i_l g_l \quad (1 \leq i \leq k-1). \end{gathered}$$

Collecting like terms gives

$$\exists_{a^i_\bullet \in (\mathbb{Z}A)^{\{1,\ldots,q\}}} \forall_j\, a^i_j g_j \preceq S(g_i, g_k) = \sum_{j=1}^q a^i_j g_j \; (1 \leq i \leq k-1).$$

$$f^0 = \sum_{i=1}^{k-1} e_i \eta_i S(g_i, g_k) = \sum_{j=1}^q \sum_{i=1}^{k-1} e_i \eta_i a^i_j g_j$$

Because $a^i_j g_j \preceq S(g_i, g_k) = \sum_{j=1}^q a^i_j g_j$ $\forall_i \forall_j$ using Definition 6.4 we get

$$\eta_i a^i_j g_j \preceq \eta_i S(g_i, g_k) = S(\lambda_i g_i, \lambda_k g_k).$$

Because $\lambda_i g_i$ and $\lambda_k g_k$ are in F_0 and $\mathrm{LT}(\lambda_i g_i) = \mathrm{LT}(\lambda_k g_k) = \delta(r)$ we obtain that $S(\lambda_i g_i, \lambda_k g_k) = \lambda_i g_i - \lambda_k g_k \prec \delta(r)$ $\forall_{i=1,\ldots,k-1}$. Thus

$$\eta_i a^i_j g_j \preceq S(\lambda_i g_i, \lambda_k g_k) \prec \delta(r) \; \forall_{i=1,\ldots,k-1},\; \forall_{j=1,\ldots,q}$$

$$\mathrm{LT}\Big(\sum_{i=1}^{k-1} e_i\eta_i a_j^i g_j\Big) \leq \max_{i=1}^{k-1} \mathrm{LT}(\eta_i a_j^i g_j) < \delta(r)\ \forall_{j=1,\dots,q}$$

$$\Rightarrow \delta\big(\sum_{i=1}^{k-1} e_i\eta_i \cdot a_1^i, \dots, \sum_{i=1}^{k-1} e_i\eta_i \cdot a_q^i\big) < \delta(r).\text{ This means}$$

$$\Big(\sum_{i=1}^{k-1} e_i\eta_i \cdot a_1^i, \dots, \sum_{i=1}^{k-1} e_i\eta_i \cdot a_q^i\Big) \in R_{<\delta(r)}\text{ and thus}$$

$$f^0 = \phi\Big(\sum_{i=1}^{k-1} e_i\eta_i \cdot a_1^i, \dots, \sum_{i=1}^{k-1} e_i\eta_i \cdot a_q^i\Big) \in \phi(R_{<\delta(r)}).$$

Consequently

$$f = f^0 + f^1 + f^2 \in \phi(R_{<\delta(r)}).$$

It follows that $\exists s \in R_{<\delta(r)}$ with $\phi(s) = f$ and therefore

$$s \in \phi^{-1}(f) \wedge \delta(s) < \delta(r).$$

This proof when spezializing the Ring R to $K[x_1, \dots, x_n]$ corresponds to the one found in [1]. For other proofs of the polynomial case see [2], [7], [34] and the literature listed in [8].

6.9. The Buchberger Algorithm

As in the classical theory Theorem 6.1 allows the construction of Gröbner bases provided that the groundring R has a Noetherian structure.

Thus, supposing that an S-polynomial $S\colon F \times F \longrightarrow F$ is available, we fix a set $A \subseteq R$ such that $\Lambda \subseteq A = K^\times A$.

Buchberger Algorithm

```
In: $G = \{g_1, \dots, g_q\} \subseteq F_0$;
$G_{\text{-}} := G$;
Pick $\gamma \in G_{\text{-}}$;
while $\exists_{g \in G_{\text{-}} \setminus \{\gamma\}}$ with $\neg\ S(g,\gamma) \xrightarrow[\rho_{\mathrm{T}}(AG_{\text{-}})]{\star} 0$ do
        Choose such a $g$;
        $G_{\text{-}} := G_{\text{-}} \cup \{\frac{\mathrm{NF}(S(g,\gamma))}{\mathrm{LC}(\mathrm{NF}(S(g,\gamma)))}\}$;
endwhile;
RETURN $G_{\text{-}}$;
```

Theorem 6.2. Suppose that $R = K^{(\Lambda)}$ is left Noetherian ring, $F = R^{(E)}$ with a finite set E. Moreover assume that

1. $\Lambda\Lambda \subseteq \Lambda$,
2. $(<_R, <_F)$ a TO-pair;
3. $\forall_{\lambda\in\Lambda}\,\forall_{c\in K}\,\lambda c \preceq \lambda$;
4. $\forall_{\lambda\in\Lambda}\,\forall_{s,t\in\Lambda E}\,(s < t \Rightarrow \lambda s < \lambda t)$;
5. $\forall_{\lambda\in\Lambda}\,\forall_{f\in F_0}\,\lambda f \in F_0$;
6. $S\colon F \times F \longrightarrow F$ is an S-polynomial;
7. $A \subseteq R$ s.t. $\Lambda \subseteq A = K^\times A$;
8. $G = \{g_1, \dots, g_q\} \subseteq F_0$;
9. $X = AG$;
10. $\rho = \rho_{\mathrm{CR}}(X) \vee \rho = \rho_{\mathrm{T}}(X)$;

Then the Buchberger algorithm terminates on input G.

Proof. In the while-loop consider the set $G_{\text{-}} = \{g_1, \dots, g_p\}$ and assume that $g_j \in G_{\text{-}} \setminus \{\gamma\}$ is a chosen element. Denote the updated set $G_{\text{-}}$ with G_1. Thus G_1 is the old set $G_{\text{-}}$ augmented with $h := \frac{\mathrm{NF}(S(g_j,\gamma))}{\mathrm{LC}(\mathrm{NF}(S(g_j,\gamma)))}\}$. Then $h \neq 0$ and h is irreducible (w.r.t the old $G_{\text{-}}$). From Corollary 6.7 we obtain that $\mathrm{T}(h) \subseteq I$. Let $t := \mathrm{LT}(h)$. Then $t \in I \cap \Lambda E$. Proposition 6.8 guarantees that $t \notin R \cdot \mathrm{LT}(G_{\text{-}})$. Because $t \in \mathrm{LT}(G_1)$ we conclude that $R \cdot \mathrm{LT}(G_{\text{-}}) \subset R \cdot \mathrm{LT}(G_1)$. Because F is a Noetherian R-module the chain of these submodules is finite. Consequently the process must stop.

7. Specialization to Particular Rings

As mentioned in Section 6.6, when $\dim_K R$ as well as $\operatorname{rank} F$ are both finite, it may happen that a Gröbner basis for $N \subseteq F$ can be computed without invoking the machinery of S-polynomials.

Consider $R = K^{(\Lambda)}$, $F = R^{(E)} = K^{(\Lambda E)}$ where Λ and E are both finite sets. Moreover let $G = \{g_1, \dots, g_q\} \subset F$, $N = RG$, $X = K^\times \Lambda G$. By linearly ordering the set ΛE arbitrarily we may apply classical reduction w.r.t. X

$$\rho\colon\ f \longrightarrow h \iff f - h \in X \wedge h_{\mathrm{LT}(f-h)} = 0.$$

If ρ is not a Gröbner reduction for N there must be an irreducible $n \in N \setminus 0$. Therefore, the linear system

$$\pi_s\Big(\sum_{l=1}^{q}\sum_{\lambda\in\Lambda} r_\lambda^l \lambda g_l\Big) = 0 \quad (s \in \mathrm{LT}(X)) \tag{16}$$

must have a non-zero solution $(r_\lambda^l) \in K^{\{1,\dots,q\}\times\Lambda}$ which is so that

$$\exists t \in \Lambda E \setminus \mathrm{LT}(X)$$

with

$$\pi_t\Big(\sum_{l=1}^{q}\sum_{\lambda\in\Lambda} r_\lambda^l \lambda g_l\Big) \neq 0.$$

Consequently

$$n = \sum_{l=1}^{q}\sum_{\lambda\in\Lambda} r_\lambda^l \lambda g_l \neq 0.$$

Assume we can compute such a solution (r_λ^l), set $G' = G \cup \{n\}$ and $X' = K^\times \Lambda G'$. If then $\mathrm{LT}(X')$ is strictly containing $\mathrm{LT}(X)$, iteration of this procedure must terminate due to the finiteness of ΛE.

7.1. Vector Spaces

The most simple situation occurs when $K = R$. Then $\Lambda = \{1\}$, and if $E = \{e_1, \dots, e_n\}$, the module $F = R^{(E)}$ is just a finite dimensional vector space over the field K. $\Lambda E = E$ and the structure formulae are $1 \cdot c = c \quad (c \in K)$ and $1 \cdot 1 = 1$.

We put E in order $e_1 < \cdots < e_n$. Given a subspace $N = RG \subseteq F$ with $G = \{g_1, \dots, g_q\}$, the system of equations (10) collapses to

$$\sum_{j=1}^{q} r_j g_e^j = 0 \quad (e \in \mathrm{LT}(X)).$$

Of course this is solvable, and we can produce a Gröbner reduction as described in Section 6.6.

In particular we obtain a Gröbner basis when X is defined as $X = K^\times G$ and we proceed by extending it to $X' = K^\times(G \cup \{\Phi(r)\})$ with a solution $r \notin \ker(\Phi)$.

Alternatively, we may take $S(f, g) = f - g$ as an S-polynomial and compute a Gröbner basis using the Buchberger algorithm.

7.2. Monoid Rings

Assume that Λ is a finite monoid, $R = K[\Lambda]$ the associated monoid ring, and $F = R^E$ with finite set E. We order ΛE arbitrarily. The linear system (16) associated to $G = \{g_1, \ldots, g_q\} \subseteq F$ amounts to

$$\sum_{l=1}^{q} \sum_{\lambda s = t} g_s^l r_\lambda^l = 0 \quad (t \in \mathrm{LT}(X)).$$

Having determined a solution matrix $(r_\lambda^l) \in K^{q \times \Lambda}$ such that the corresponding element

$$n = \sum_{t \in \Lambda E} \sum_{\lambda s = t} \sum_{l=1}^{q} r_\lambda^l g_s^l t \neq 0$$

we can set $G' = G \cup \{n\}$, $X' = K^\times \Lambda G$. Since $1 \in \Lambda$ it is clear that $n \in X'$ and $\mathrm{LT}(n) \in \mathrm{T}(n) \subseteq \Lambda E \backslash \mathrm{LT}(X)$. Therefore the set X' properly contains X, and since ΛE is finite, iteration of this process must terminate and yields a Gröbner basis for RG.

7.3. Matrixrings

Let $R = K^{n \times n}$ be the ring of square $n \times n$-matrices over K. This ring has a natural K-basis Λ consisting of all matrices λ_i^j $(1 \leq i, j \leq n)$ where λ_i^j is the matrix with 1 in position (j, i) and 0 else. Thus

$$(\lambda_i^j)_l^k = \begin{cases} 1 & \ldots\ k = j \wedge l = i \\ 0 & \ldots\ \text{else.} \end{cases}$$

The basic structure formulae in this setting are then

$$\lambda_i^j \cdot c = c\lambda_i^j \text{ and } \lambda_i^j \cdot \lambda_k^l = \begin{cases} \lambda_k^j & \ldots\ i = l \\ 0 & \ldots\ \mathrm{e}lse \end{cases}$$

and so, for $a \in R$ and arbitrary indices i, j, k, l

$$(\lambda_i^j a)_k^l = \sum_{r=1}^{n} (\lambda_i^j)_r^l a_k^r = \begin{cases} a_k^i & \ldots\ j = l \\ 0 & \ldots\ j \neq l. \end{cases}$$

Let $F = R^E$ with finite set E be a free module and order ΛE arbitrarily. Consider a submodule $N \subseteq F$. Since R is simple Artinian, it is clear that F is Noetherian and therefore N is generated by a finite set $G = \{g_1, \ldots, g_q\} \subseteq F$. Set $X = K^\times \Lambda G$. With notation as before we get

$$\Phi(r) = \sum_{e \in E} \sum_{u=1}^{n} \sum_{j=1}^{n} \sum_{l=1}^{q} \sum_{i=1}^{n} (r_l)_i^j (g_l^e)_u^i \lambda_u^j e$$

So we have to compute the general solution of the system

$$\sum_{l=1}^{q} \sum_{i=1}^{n} (g_l^e)_u^i (r_l)_i^j = 0 \quad (\lambda_u^j e \in \mathrm{LT}(X))$$

and check if it is possible to single out a particular instance such that the corresponding element n is not zero. If this is the case we can proceed in the usual way: set $X' = K^\times \Lambda \cdot (G \cup \{n\})$. Although $n \notin X'$ it is obvious that $\mathrm{LT}(X') \supset \mathrm{LT}(X)$ whence the process terminates.

7.4. The Ring of Ore Polynomials

Given an endomorphism $\sigma\colon K \longrightarrow K$, a σ-skew derivation is an additive map $\delta\colon K \longrightarrow K$ satisfying

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b, \quad (a, b \in K).$$

An Ore-variable over K is a pair $\partial = (\sigma, \delta)$ where σ is an endomorphism and δ is a σ-skew derivation.

Let $\partial_i = (\sigma_i, \delta_i)$ be Ore-variables $(1 \leq i \leq n)$ such that all mappings σ_i, δ_j commute with each other. Then the Ore algebra $\mathbb{O}$ defined by $X = (\partial_1, \ldots, \partial_n)$ is the free K-module on the set of formal expressions $\partial^k = \partial_1^{k_1} \cdots \partial_n^{k_n}$ $(k \in \mathbb{N}^n)$ with multiplication determined by the rules

$$\partial_i \cdot \partial_j = \partial_j \cdot \partial_i \text{ and } \partial_i \cdot x = \sigma_i(x)\partial_i + \delta_i(x) \quad (x \in K). \quad (17)$$

For the set of monomials we use $\Lambda = \{\partial^k \colon k \in \mathbb{N}^n\}$. With the notation

$$x_k^l = (\delta^l \circ \sigma^k)(x) \quad (k, l \in \mathbb{N}^n,\ x \in K) \qquad (18)$$

and the binomial coefficient

$$\binom{l}{v} = \binom{l_1}{v_1} \cdots \binom{l_n}{v_n} \qquad (l, v \in \mathbb{N}^n)$$

the product in $\mathbb{O}$ may be written explicitly

$$\begin{aligned} x\partial^k \cdot y\partial^l &= \sum_{v \in \mathbb{N}^n} \binom{k}{v} x y_v^{k-v} \partial^{l+v} \\ &= \sum_{v \leq_\pi k} \binom{k}{v} x y_{k-v}^v \partial^{k+l-v} \end{aligned} \qquad (19)$$

where $x, y \in K$ and $k, l \in \mathbb{N}^n$. Inparticular the two basic structure formulae are

$$\partial^k \cdot y = \sum_{v \leq_\pi k} \binom{k}{v} y_{k-v}^v \partial^{k-v} \text{ and } \partial^k \cdot \partial^l = \partial^{k+l}.$$

It is customary to denote $\mathbb{D}$ by the symbol $K\{\partial_1, \dots, \partial_n\}$. The particular instance $x\partial^0 \cdot y\partial^0 = xy\partial^0$ demonstrates that K is naturally a subring of $\mathbb{D}$ whilst substituting unit vectors for l and q reveals the formal expression ∂^k as a concrete product $\partial_1^{k_1} \cdots \partial_n^{k_n}$. Consequently we have that $\Lambda \cong \mathbb{N}^n$.

As before we consider the free $\mathbb{D}$-module $F = \mathbb{D}^{(E)}$.

Definition 7.1. Let $<\subset \Lambda \times \Lambda$ be a classical term-order and let the K-basis E be linearly ordered (cf. [2]). Then we define the order $<_F$ on ΛE lexicographically

$$\lambda e <_F \mu e' \iff \lambda < \mu \vee (\lambda = \mu \wedge e < e').$$

Proposition 7.1. Let $\lambda, \mu \in \lambda$, $e \in E$, $s, t \in \Lambda E$, $x, y \in K^\times$, $r \in R$, $f, g \in F$;

1. $\mathrm{LT}(x\partial^k \cdot y\partial^l e) = \partial^{k+l}e \wedge \mathrm{LC}(x\partial^k \cdot y\partial^l e) = xy_k$;
2. $\mathrm{LT}(rf) = \mathrm{LT}(r)\mathrm{LT}(f)$;
3. $\mathrm{LT}(\lambda f) = \lambda\,\mathrm{LT}(f)$;
4. $\lambda < \mu \Rightarrow \lambda s < \mu s$;
5. $s < t \Rightarrow \lambda s < \lambda t$;
6. $\lambda < \mu \Rightarrow \lambda f \prec \mu f$;
7. $\mathrm{LT}(r) f \preceq rf$;
8. $f \preceq g \Rightarrow \lambda f \preceq \lambda g$;
9. $(<, <_F)$ is a TO-pair.

Proof. Let

$$\lambda = \partial^k, \mu = \partial^l, s = \partial^u e, t = \partial^v e',$$
$$r = r_0\partial^{m_0} + \sum_{\partial^m < \partial^{m_0}} r_m \partial^m,$$
$$f = f_0 \partial^{n_0} e_0 + \sum_{\partial^n e < \partial^{n_0} e_0} f_{n,e}\partial^n e.$$

1. From $v = k$ in the first formula of (19) we obtain the summand $xy_k^0\partial^{k+l}e$ which is diffenet from 0 whence $\partial^{k+l}e \in \mathrm{T}(x\partial^k \cdot y\partial^l e)$. If $t \in \mathrm{T}(x\partial^k \cdot y\partial^l e) \setminus \{\partial^{k+l}e\}$ then $\exists_{v <_\pi k}\, t = \partial^{l+v}e$. Thus $\partial^{l+v} < \partial^{k+l}$ hence $t = \partial^{l+v}e < \partial^{k+l}e$. One more inspection of formula (19) provides that $\mathrm{LC}(x\partial^k \cdot y\partial^l e) = xy_k$.
2. $\mathrm{LT}(rf) \leq \max\{\mathrm{LT}(r_0\partial^{m_0} \cdot f_0\partial^{n_0}e_0)\} \cup \{\mathrm{LT}(r_0\partial^{m_0} \cdot f_{n,e}\partial^n e) \mid \partial^n e < \partial^{n_0}e_0\} \cup \{\mathrm{LT}(r_m\partial^m \cdot f_0\partial^{n_0}e_0) \mid \partial^m < \partial^{m_0}\} \cup \{\mathrm{LT}(r_m\partial^m \cdot f_{n,e}\partial^n e) \mid \partial^m < \partial^{m_0} \wedge \partial^n e < \partial^{n_0}e_0\} = \max\{\partial^{m_0+n_0}e_0\} \cup \{\partial^{m_0+n}e \mid \partial^n e < \partial^{n_0}e_0\} \cup \{\partial^{m+n_0}e_0 \mid \partial^m < \partial^{m_0}\} \cup \{\partial^{m+n}e \mid \partial^m < \partial^{m_0} \wedge \partial^n e < \partial^{n_0}e_0\} = \partial^{m_0+n_0}e_0$
   Since all emerging elements different from $\partial^{m_0+n_0}e_0$ are strictly smaller than $\partial^{m_0+n_0}e_0$, the assertion follows.
3. This is a specialization of the previous item.
4. If $\lambda < \mu$ then $k < l$ and so $k + u < l + u$ i.e., $\partial^{k+u} < \partial^{l+u}$. Therefore $\lambda s = \partial^k\partial^u e = \partial^{k+u}e < \partial^{l+u}e = \partial^l\partial^u e = \mu s$.
5. Let $s < t$. If $u < v$ then $k + u < k + v$, $\partial^{k+u} < \partial^{k+v}$. Therefore $\lambda s = \partial^k\partial^u e = \partial^{k+u}e < \partial^{k+v}e' = \partial^k\partial^v e' = \lambda t$. If $u = v$ then $e < e'$ and again $\lambda s < \lambda t$.
6. Let $\lambda < \mu$. Points 3. and 4. gives $\mathrm{LT}(\lambda f) = \lambda\,\mathrm{LT}(f) < \mu\,\mathrm{LT}(f) = \mathrm{LT}(\mu f)$.
7. Using point 2. twice provides $\mathrm{LT}(\mathrm{LT}(r)f) = \mathrm{LT}(r)\mathrm{LT}(f) = \mathrm{LT}(rf)$. This yield the statement.
8. $f \preceq g$ implies $\mathrm{LT}(f) \leq \mathrm{LT}(g)$, $\lambda\,\mathrm{LT}(f) \leq \lambda\,\mathrm{LT}(g)$ (by 5.), $\mathrm{LT}(\lambda f) \leq \mathrm{LT}(\lambda g)$ (by 3.), $\lambda f \preceq \lambda g$ (definition of $\preceq$).
9. This is the conjunction of points 6. 7. and 8.

Since $\Lambda \cong \mathbb{N}^n$ the ring $\mathbb{D}$ admits a quotient $q\colon \Lambda E \times \Lambda E \longrightarrow \mathbb{D} \times \mathbb{D}$. From this, together with Proposition 7.1 we derive the existence of an S-polynomial $S\colon F \times F \longrightarrow F$. Therefore, the parameters as required in Theorem 6.1, this theorem provides the existence of Gröbner bases in F. We will now demonstrate that they can be computed.

Consider a ring A, $\sigma_1, \sigma_2 \in \mathrm{Aut}(A)$ and let δ_1, δ_2 be σ_1, σ_2-skew derivations respectively. Suppose that all these maps commute with each another and set $\partial_1 = (\sigma_1, \delta_1)$. Then we can build the Ore-algebra $A_1 := A\{\partial_1\}$ as discussed at the beginning of the section (the difference being that A need not be a field). The ring A_1 being an extension of A allows to componentwise extend the maps σ_2, δ_2 to A_1

$$\widetilde{\sigma_2}\Big(\sum_k a_k\partial_1^k\Big) = \sum_k \sigma_2(a_k)\partial_1^k$$
$$\widetilde{\delta_2}\Big(\sum_k a_k\partial_1^k\Big) = \sum_k \delta_2(a_k)\partial_1^k.$$

We will omit the tilde, writing these maps σ_2, δ_2 again. With this notation we obtain

Proposition 7.2. $\partial_2 := (\sigma_2, \delta_2)$ is an Ore-variable over A_1.

Proof. It is clear that the maps $A_1 \underset{\delta_2}{\overset{\sigma_2}{\rightrightarrows}} A_1$ are additive. We have to show that $\sigma_2 \in \mathrm{Aut}(A_1)$ and that δ_2 is a σ_2-skew derivation. These results in tedious but easy calculations.

Given Ore-variables $\partial_1, \dots, \partial_n$ over the ring A (all maps pairwise commuting), we may iterate the adjunction described above arriving at the ring $A\{\partial_1\}\{\partial_2\}\cdots\{\partial_n\}$.

Proposition 7.3. Let $\partial_1, \dots, \partial_n$ be Ore-variables over K, where $\partial_i = (\sigma_i, \delta_i)$ with $\sigma_i \in \mathrm{Aut}(K)$ $(1 \leq i \leq n)$, all maps pairwise commuting. Then the Ore algebra $\mathbb{D}$ defined by $\partial_1, \dots, \partial_n$ is isomorphic as a ring to $K\{\partial_1\}\cdots\{\partial_n\}$.

So, under the above hypotheses, the two rings $K\{\partial_1, \cdots, \partial_n\}$ and $K\{\partial_1\}\cdots\{\partial_n\}$ coincide.

Corollary 7.1. Let the Ore-ring $\mathbb{D}$ be defined by the Ore-variables $\partial_i = (\sigma_i, \delta_i)$ $(1 \leq i \leq n)$ where all σ_i are automorphisms. Then $\mathbb{D}$ is Noetherian. Consequently each finitely generated module over $\mathbb{D}$ is Noetherian. In particular, if E is a finite set and $F = \mathbb{D}^{(E)}$, then, starting from an arbitrary set $X \subseteq F$, the Buchberger algorithm terminates.

Proof. Because all σ_i are automorphisms and K is Noetherian, so is $\mathbb{D} = K\{\partial_1\}\cdots\{\partial_n\}$ (cf. [29] page 17). Theorem 6.2 yields the result.

7.5. The Ring of Difference-Differential Operators

Let $\delta = (\delta_1, \dots, \delta_m)$ be a tuple of ordinary derivations and $\sigma = (\sigma_1, \dots, \sigma_n)$ a tuple of automorphisms of K. All these maps are assumed to commute with each other. The ring D is then constructed as the free K-module on the set of formal expressions

$$\delta^k\sigma^l = \delta_1^{k_1}\cdots\delta_m^{k_m}\sigma_1^{l_1}\cdots\sigma_n^{l_n}, \quad (k_i \in \mathbb{N}, l_j \in \mathbb{Z})$$

and a product that reflects the properties of derivations and automorphisms. We consider the elements of the set $\Lambda = \{\delta^k\sigma^l \mid (k,l) \in \mathbb{N}^m \times \mathbb{Z}^n\}$ as the distinguished monomials. Consequently elements of D are finite K-linear combinations

$$\sum_{(k,l)\in\mathbb{N}^m\times\mathbb{Z}^n} a_{k,l}\delta^k\sigma^l, \quad (a_{k,l} \in K)$$

and the product is driven by the rules

$$\delta_i \cdot c = c\,\delta_i + \delta_i(c) \quad \sigma_j \cdot c = \sigma_j(c)\sigma_j, \quad (c \in K).$$

We call D a $\Delta\Sigma$-ring over K.

A left module over D is also called a *difference-differential module*, or $\Delta\Sigma$-module over K. In the literature the tuples δ and σ are denoted informally as the sets Δ and Σ, whence the name. Note though, that the mappings δ_i need not be distinct. The same is the case with the σ_j.

The concept covers difference modules ($\Delta = \emptyset$) as well as differential modules ($\Sigma = \emptyset$) as special instances.

Proposition 7.4. Consider a field $\mathbf{k}$ with $\mathrm{char}(\mathbf{k}) = 0$. Let $K = \mathbf{k}[x_1,\ldots,x_m]$, $\Delta = \{\frac{d}{dx_1},\ldots,\frac{d}{dx_m}\}$ and $\Sigma = \emptyset$. Then the resulting $\Delta\Sigma$-ring is the Weyl-algebra $A_m(\mathbf{k})$ (cf. [6]).

Proof. This is due to the fact that partial derivatives have no relations among each other. Precisely: Let $\Delta^\star$ be the monoid generated (in $\mathrm{End}_{\mathbf{k}}(K)$) by Δ. Then $\Delta^\star \cong \mathbb{N}^m$ and $A_m(\mathbf{k})$ is a free K-module with basis $\Delta^\star$.

For computing the Hilbert function of a finitely gnerated difference-differential module, Winkler and Zhou introduced the concept of *relative Gröbner bases* (w.r.t. generalized term orders on $\mathbb{N}^m \times \mathbb{Z}^n$) [37]. Our approach is to present a difference-differential ring as a quotient of another ring that allows computing a Gröbner basis.

We use the notation

$$y_s^k = (\delta^k \circ \sigma^s)(y) \quad (k \in \mathbb{N}^m,\ s \in \mathbb{Z}^n).$$

For the free D-module $F = D^{(E)}$, the product $D \times F \longrightarrow F$ can then be written explicitly

$$\delta^k\sigma^l \cdot y\delta^r\sigma^s e = \sum_{u \le_\pi k} \binom{k}{u} y_l^{k-u}\delta^{u+r}\sigma^{l+s}e \qquad (20)$$
$$(k, r \in \mathbb{N}^m;\ l, s \in \mathbb{Z}^n;\ y \in K;\ e \in E).$$

This formula specializes to the basic structure formulae

$$\delta^k\sigma^l \cdot y = \sum_{u \le_\pi k} \binom{k}{u} y_l^{k-u}\delta^u\sigma^l$$

and

$$\delta^k\sigma^l \cdot \delta^r\sigma^s = \delta^{k+r}\sigma^{l+s}.$$

For $\lambda = \delta^k\sigma^l \in \Lambda$ we set

$$\nu_1(\lambda) = |k|, \quad \nu_2(\lambda) = |l|, \quad \nu_0 = \nu_1 + \nu_2. \qquad (21)$$

We may realize $\Delta\Sigma$-rings as quotients of Ore-algebras. Starting from $\Delta = \{\delta_1,\ldots,\delta_m\}$ and $\Sigma = \{\sigma_1,\ldots,\sigma_n\}$ we define Ore-variables

$$\begin{array}{rcll} \partial_i &=& (\delta_i, \mathrm{id}) & (1 \le i \le m) \\ \eta_j &=& (0, \sigma_j) & (1 \le j \le n) \\ \phi_j &=& (0, \sigma_j^{-1}) & (1 \le i \le n) \end{array}$$

and let $\mathbb{O}$ be the Ore-algebra defined by them. Let I be the 2-sided ideal generated by the set $\{\eta_j \cdot \phi_j - 1 \mid 1 \le j \le n\}$. Then $\mathbb{O}/I \cong D$.

This representaion allows the construction of Gröbner bases for submodules of finitely generated free modules over D out of Gröbner bases for the corresponding modules over $\mathbb{O}$. Cf. also Lemma 3.1 and [15].

Consider the epimorphism $\pi\colon \mathbb{O} \longrightarrow D$. We can write down generically an inverse image $u \in \mathbb{O}$ for arbitrary $a \in D$: If $a = \sum_{(k,l)\in\mathbb{N}^m\times\mathbb{Z}^n} a_{k,l}\delta^k\sigma^l$ then set

$$u = a = \sum_{(k,l)\in\mathbb{N}^m\times\mathbb{Z}^n} a_{k,l}\partial_1^{k_1}\cdots\partial_m^{k_m}\zeta_1^{|l_1|}\cdots\zeta_n^{|l_n|}$$

where $\zeta_j = \eta_j$ if $l_j \ge 0$, and $\zeta_j = \phi_j$ for $l < 0$.

Let be given a left ideal $N = D \cdot \{g_1,\ldots,g_q\} \subseteq D$. Chosen inverse images $h_1,\ldots,h_q$ for $g_1,\ldots,g_q$, the left ideal $\pi^{-1}(N) \subseteq \mathbb{O}$ is generated by the set

$$H = \{h_1,\ldots,h_q\} \cup \{\eta_j \cdot \phi_j - 1 \mid 1 \le j \le n\}.$$

Let ρ be a Gröbner reduction for $\pi^{-1}(N)$, computed by stepwise extending H, and $a \in D$. Choose an inverse image u of a. Then $a \in N$ iff $u \xrightarrow[\rho]{\star} 0$.

8. Conclusion

Given a module M and a submodule $N \subset M$, the goal of reduction is to compute a set of normal forms that allow to decide the membership problem for N. This is what the classical Gröbner basis computation provides for ideals in a polynomial ring over a field, and what similar adapted concepts yield for certain submodules over particular rings. Usually the process of computing such a basis is by iteration of a reduction step that produces a new element g out of an element f given as an input. In order to make sense, such a reduction has to obey certain properties. Clearly its iteration has to stop after finitely many steps and it should output a unique normal form as its result.

We have formulated these requirements in a list of four axioms that are appropriate for describing reduction relations for modules over a ring with basis.

The axioms are carefully dicussed and examples are provided for illustration. Depending on the ring there are several concepts that can be used to define a reduction. Among them we discuss possible term orders, filtrations and rank functions.

In the presence of a term order we consider three types of reductions: leading term reduction, T-reduction and classical reduction. Each of them is dicussed in detail and their interrelations are discribed. Then we discuss the case when the submodule N is finitely generated, describe the appropriate concept of an S-polynomial and demonstrate the equivalence of the full reduction concept with Gröbner bases.

The last part of the paper is devoted to examples that examine the introduced concepts.

Acknowledgements

This work has been partially supported by the Austrian Science Fund (FWF): W1214-N15, project DK11.

References

[1] Adams, W. and Loustaunau, P (1994). An Introduction to Gröbner Bases. Graduate Series in Mathematics, 3. American Mathematical Society.

[2] Becker, T., Weispfenning, V. and Kredel, H. (1993). Gröbner bases: a computational approach to commutative algebra. Graduate texts in mathematics, Springer-Verlag.

[3] Bergman, G., M. (1978). The diamond lemma for ring theory. Advances in Mathematics, 29: 178–218.

[4] Bossaller, D. P. and Lopez-Permouth, S. R. (2019). Algebras having bases that consist solely of strongly regular elements. Journal of Pure and Applied Algebra 223: 3485–3498.

[5] Buchberger, B. (2006). An algorithm for finding the basis blements in the residue class ring modulo a zero dimensional polynomial ideal. English translation in Jornal of Symbolic Computation, Special Issue on Logic, Mathematics and Computer Science: Interactions, 41, (3–4): 475–511. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965.

[6] Coutinho, S.C. (1995). A primer of algebraic D-modules. London Mathematical Society Student Texts. Cambridge University Press.

[7] Cox, D., Little, J. and O'Shea, D. (1997). Ideals, varieties and algorithms - an introduction to computational algebraic geometry and commutative algebra. (2. ed.), Undergraduate texts in mathematics. Springer.

[8] Cox, D., Little, J. and O'Shea, D. (1998). Using algebraic geometry. Graduate Texts in Mathematics. Springer.

[9] Donga, R. and Dongming Wang (2021). Computing strong regular characteristic pairs with Gröbner bases. Journal of Symbolic Computation, 104: 312–327.

[10] Dotsenko, V. and Khoroshkin, A. (2010). Gröbner bases for operads. Duke Mathematical Journal 153 (2): 363–396. https://doi.org/10.1215/00127094-2010-026

[11] Dönch, C. and Levin, A. (2012). Computation of bivariate characteristic polynomials of finitely generated modules over Weyl algebras. ArXiv e-prints:1212.1833.

[12] Dönch, D. (2013). Characterization of relative Gröbner bases. Journal of Symbolic Computation, 55: 19–29.

[13] Dotsenko, V. and Khoroshkin, A. (2010). Gröbner bases for operads. Duke Mathematical Journal, 153 (2): 363–396. https://doi.org/10.1215/00127094-2010-026

[14] Eisenbud, D. (1995). Commutative algebra with a view toward algebraic geometry. Graduate Texts in Mathematics. Springer.

[15] Fürst, C. and Landsmann, G. (2015). Computation of dimension in filtered free modules by Gröbner reduction. In Proceedings of the International Symposium for Symbolic and Algebraic Computation, ISSAC '15. ACM.

[16] Fürst, C. and Landsmann, G. (2015). Three examples of Gröbner reduction over noncommutative rings. RISC Report Series 15–16, Research Institute for Symbolic Computation (RISC), Johannes Kepler University Linz, Schloss Hagenberg, 4232 Hagenberg, Austria.

[17] Gao, X., Guo, L. and Rosenkranz, M. (2015). Free integro-differential algebras and Gröbner-Shrishov bases. Journal Algebra, 442: 354–396.

[18] Huang, G. and Zhou, M. (2015). Termination of algorithm for computing relative Gröbner bases and difference differential dimension polynomials. Frontiers of Mathematics in China, 10 (3).

[19] Sungsoon Kim and Dong-il Lee (2018). Gröbner-Shirshov bases for Temperley-Lieb algebras. Palestine Journal of Mathematics, 7 (Special Issue I): 11–17.

[20] Kolchin, E. R. (1964). The notion of dimension in the theory of algebraic differential equationes. Bull. Amer. Math. Soc. 70: 570–573.

[21] Kolchin, E. R. (1973). Differential algebra and algebraic groups. Academic Press Inc.

[22] Kreuzer, M. and Kriegl, M. (2014). Gröbner bases for syzygy modules of border bases. Journal of Algebra and Its Applications, 13 (6).

[23] Maletzky, A. (2021). A generic and executable formalization of signature-based Gröbner basis algorithms. Journal of Symbolic Computation 106: 23–47.

[24] Mikhalev, A. V., Levin, A., Pankratiev, E. V. and Kondratieva, M. V. (1998). Differential and difference dimension polynomials. Mathematics and its applications. Springer.

[25] Levin, A. (2007). Gröbner bases with respect to several term orderings and multivariate dimension polynomials. In Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ISSAC '07, New York: 251–260.

[26] Levin, A. (2007). Gröbner bases with respect to several orderings and multivariable dimension polynomials. Journal of Symbolic Computation, 42 (5): 561–578.

[27] Levin, A. (2012). Multivariate difference-differential dimension polynomials. ArXiv e-prints:1207.4757.

[28] Levin, A. (2013). Multivariate difference-differential dimension polynomials and new invariants of difference-differential field extensions. ArXiv e-prints, Feb. 2013.

[29] McConnell, J. C. and Robson, J. C. (1987). Noncommutative Noetherian rings. Wiley series in pure and applied mathematics. Wiley.

[30] Pauer, F. (2007). Gröbner bases with coefficients in rings. Journal of symbolic computation, 42: 1003–1011.

[31] Donga, R. and Wang, D. (2021). Computing strong regular characteristic pairs with Gröbner bases. Journal of Symbolic Computation, 104: 312–327.

[32] Rolnicka, D. and Spencer, G. (2019). On the robust hardness of Gröbner basis computation. Journal of Pure and Applied Algebra, 223: 2080–2100.

[33] Shibuta, T. (2011). Gröbner bases of contraction ideals. Journal of Algebraic Combinatorics, 36 (1).

[34] Winkler, F. (1996). Polynomial Algorithms in Computer Algebra. Texts and Monographs in Symbolic Computation Springer.

[35] Zhou, M. and Winkler, F. (2006). Gröbner bases in difference-differential modules. In Proceedings of the 2006 international symposium on Symbolic and algebraic computation, ISSAC '06: 353–360, New York, ACM.

[36] Zhou, M. and Winkler, F. (2007). Computing difference-differential Groebner Bases and difference-differential dimension polynomials. RISC Report Series 07–01, Research Institute for Symbolic Computation (RISC), Johannes Kepler University Linz, Schloss Hagenberg, 4232 Hagenberg, Austria.

[37] Zhou, M. and Winkler, F. (2008). Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules. Journal of Symbolic Computation, 43 (10): 726–745.

[38] Yunnan Li and Li Guo (2021). Construction of free differential algebras by extending Gröbner-Shirshov bases. Journal of Symbolic Computation, 107: 167–189.

[39] Zihao Qi, Yufei Qin, Kai Wang and Guodong Zhou (2021). Free objects and Gröbner-Shirshov bases in operated contexts. Journal of Algebra, 584: 89–124.