On an Algorithm for Enumerating Generating Sets of Modules over Euclidean Domains

Maja Wanda Maria Waldhausen

Ph. D. Thesis
University of St Andrews
June 2005

I, Maia Watkins, hereby certify that this thesis, which is approximately 36,500 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

date 21/06/05 signature of candidate

I was admitted as a research student in November 2001 and as a candidate for the degree of PhD in November 2001; the higher study for which this is a record was carried out in the University of St Andrews between 2001 and 2005.

date 21/06/05 signature of candidate

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application of that degree.

date 21.6.05 signature of supervisor

In submitting this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker.

date 21/06/05 signature of candidate

To Iain and my parents

Acknowledgements

Firstly I would like to express my gratitude to my first supervisor Professor S. A. Linton for all his guidance, assistance and encouragement; and I would also like to thank my second supervisor Professor E. F. Robertson. Secondly I would like to thank all the people from CIRCA, in particular my office neighbour D. Sutherland, without whom lunch-breaks and also the rest of the time would not have been nearly so interesting.

Furthermore I would like to thank Professor Dr. G. Hiß and the people from Lehrstuhl D of the Department of Mathematics at the University of Aachen for their hospitality in summer 2003. In particular I am grateful to Dr. J. Müller, Dr. M. Neunhöffer and Professor em. Dr. J. Neubüser for many interesting and instructive discussions.

My final and special thanks goes to my parents and to I. Gordon for all their love, support and patience.

This thesis has been typed using the P. Taylor diagrams package for LaTeX.

Abstract

In this thesis a method for the enumeration of generators of modules over ordered Euclidean domains is presented. This method is based on the ideas of the coset enumeration algorithm for subgroups of finitely presented groups. The coset enumeration algorithm has first been described by J. Todd and H. Coxeter in [43] as a method for hand calculation.

G. Labonté [18] and S. Linton [25] independently developed a linear version of the coset enumeration algorithm, the so-called *vector enumeration* algorithm. There a finitely presented module $\mathcal{M}$ over a finitely presented k-algebra is required, where k denotes a field. The vector enumeration procedure computes a basis B of $\mathcal{M}$ considered as module over k, together with a matrix representation that describes the action of the algebra generators on the elements of the basis B.

We shall present a generalisation of the vector enumeration procedure. This procedure is called the *module generator enumeration* procedure or, abbreviated, the *MGE-procedure.* We extend here to the case where we are not given a field k but a Euclidean domain instead. This case is more complicated since the elements of a domain that is not a field do not necessarily have inverses. Moreover, a module over a domain does not generally have a basis: such a module can have torsion. As a consequence of this, the MGE-procedure must possibly handle exceedingly large numbers, but also vectors of large size.

In this thesis we present a result for certain submodules of modules which are part of the input of the MGE-procedure. This result corresponds to a theorem by O. Schreier [40] on presentations of subgroups of finite index of finitely presented groups. We shall prove that for a submodule $\mathcal{N}$ of a finitely generated and free module in a certain situation a finite generating set exists. This result will be applied to modules that are connected to the input of the MGE-procedure in order to prove termination of the MGE-procedure.

Moreover, we link subroutines of the MGE-procedure to concepts of Gröbner bases and prefix Gröbner bases of modules over Euclidean domains.

These connections shall be used in order to show correctness and termination of the procedure.

We also demonstrate how a finite set of generators for a submodule $\mathcal{N}$, that satisfies the preconditions of the equivalent of the Schreier-Theorem, can be extracted from the output when the MGE-procedure has terminated. We construct relations on these generators which yields a presentation of $\mathcal{N}$ in terms of the generators given. This construction forms a linear analogue of the modified Todd-Coxeter procedure as it has been described in [2] or [41].

The MGE-procedure as well as the extended version for the construction of a submodule presentation have been implemented in GAP [15] as part of this thesis. We will give an outline of the strategy of the MGE-procedure as it has been implemented and we give a description of the main subroutines in pseudo-code. We discuss results and runtimes of some examples of the MGE-procedure and we give a conclusion and an outlook of the MGE-procedure as it has been implemented in GAP.

Contents

Chapter 0

Introduction

In this thesis we shall describe a method for enumerating the generators of modules over ordered Euclidean domains. It is based on the ideas of the coset enumeration algorithm for subgroups of finitely presented groups. The coset enumeration algorithm was first described by J. Todd and H. Coxeter in [43] as a method for hand calculation; it is also known as the Todd-Coxeter Algorithm. Since it was first introduced, different approaches and methods of complete automation of the Todd-Coxeter algorithm have been developed; further descriptions, amongst many other places, can be found in [16, 32, 41].

G. Labonté [18] and S. Linton [25] independently developed a linear version of the coset enumeration algorithm, the so-called *vector enumeration* algorithm; here we suppose that we are given a finitely presented module $\mathcal{M}$ over a finitely presented k-algebra where k denotes a field. The vector enumeration procedure computes a basis of $\mathcal{M}$ considered as module over k, together with a matrix representation describing the action of the algebra generators on the basis of $\mathcal{M}$. Another approach working with left Kan extensions in category theory has been developed by S. Carmody et. al. in [10].

We shall present a generalisation of the vector enumeration procedure on the basis of the vector enumeration algorithm as it was developed by S. Linton. We extend to the case where we are not given a field k but instead a Euclidean domain that allows a total ordering of its elements.

We call this procedure the *module generator enumeration* procedure which is abbreviated by "MGE-procedure". Such an algorithm is applicable in the setting of representation theory (compare for instance J. Müller, [31]); another application is also the computation of polycyclic quotients of finitely presented groups as has been pointed out by C. Leedham-Green in [21]. Recent work by B. Eick, A. Niemeyer and O. Panaia on the computation of polycyclic presentations using vector enumeration methods can be found in [13].

Additional Conventions

In the following we will generally denote the Euclidean domain by S, the finitely presented algebra by P. We assume that P is the quotient algebra of a free and finitely generated algebra A by a two-sided ideal generated by a finite set of relations $R \subset A$. In the course of the MGE-procedure we aim to construct, for a given finitely presented P-module $\mathcal{M}$, a finitely generated S-module Θ that is P-module isomorphic to $\mathcal{M}$. The elements of the domain S are not necessarily invertible, so it is possible that Θ contains torsion-elements; these are elements $v \in \Theta, v \neq 0$, such that there exists $\lambda \in S$, where $\lambda \neq 0_S$, with $\lambda \cdot v = 0$. An index of notation can be found on p. 179.

0.1 Overview

Chapter 1

In the course of the procedure we consider $\mathcal{M}$ mainly as A-module (we show in Lemma 1.1.5 that a P-module is an A-module as well). If we suppose that $\mathcal{M}$ is generated by n elements then there exists a free, n-generated A-module $\mathcal{F}$ of which $\mathcal{M}$ is a quotient-module. However, the finite number of algebra-relations R of the algebra P gives rise to an infinite number of module-relations for $\mathcal{M}$ as an A-module. We call this infinite set $Rels$, and $\mathcal{M}$ can be written as the quotient-module

$$\mathcal{M} = \mathcal{F}/\mathcal{N}$$

where $\mathcal{N}$ is the A-submodule of $\mathcal{F}$ generated by the set $Rels \subset \mathcal{F}$.

As in the Todd-Coxeter procedure we aim to obtain information about the S-module we wish to construct by investigating the relations of $\mathcal{M}$. This can also be interpreted as a step-by-step construction of a generating set of the module $\mathcal{N}$. In order for this to terminate it is however necessary that $\mathcal{N}$ is finitely generated.

In the case of groups, O. Schreier [40] showed that subgroups of finite index of finitely generated groups must be finitely generated themselves. For a detailed discussion of this see for instance [40, 41]. We translate this result into the setting of modules over a principal ideal domain S and a finitely generated S-algebra, respectively, which leads to the following theorem:

Theorem 1.2.1 *Let $A = \langle X \rangle$ be a free algebra over a principal ideal domain S. We assume that A is generated by the finitely generated free monoid X^* and we let P be a finitely presented quotient-algebra of A. Moreover, let $\mathcal{F}$ be a free module over A, generated by a finite set Y with a submodule $\mathcal{N}$ and let $\mathcal{M}$ be a P-module such that $\mathcal{M} = \mathcal{F}/\mathcal{N}$. If $\mathcal{M}$ is P-module isomorphic to a finitely generated S-module, then $\mathcal{N}$ has a finite set of generators as an A-module.*

In the proof of the theorem we describe a finite generating set of $\mathcal{N}$. These generators correspond to the Schreier-generators of subgroups of finite index of finitely presented groups but here the situation is more complex. We distinguish between three different types of generators: those caused by the action of the algebra generators $x \in X$; those caused by torsion in the finitely generated S-module and those which are caused by S-linear dependencies among the A-module generators $y \in Y$ of $\mathcal{M}$.

Chapter 2

In this chapter we shall give an outline of the motivation for the MGE-procedure. Since we aim to extract information about an S-module generating set of $\mathcal{M}$ from a finite subset of the set of relations $Rels$, the existence of a finite generating set for $\mathcal{N} = \langle Rels \rangle_A$ is a prerequisite for the termination of the MGE-procedure. When we investigate $r \in Rels$ then we know that r naturally lies in $\mathcal{N}$; every proper prefix of r, an element of the form

$y.w \in \mathcal{F}$, is however possibly contained in a congruence class of $\mathcal{F}$ modulo $\mathcal{N}$ different from the class of elements of $\mathcal{N}$. Such congruence classes are of special interest to us as they possibly correspond to elements contained in the S-module generating set of Θ.

Whenever a relation $r_{(\iota)} \in Rels\backslash\{r_{(1)}, \ldots, r_{(\iota-1)}\}$ has been investigated and the information we gained from $r_{(\iota)}$ has been processed we can interpret this as forming an A-module $\mathcal{N}_{(\iota)}$,

$$\mathcal{N}_{(\iota)} = \mathcal{N}_{(\iota-1)} + \langle r_{(\iota)} \rangle_A,$$

to gradually approximate the A-module $\mathcal{N}$ and therefore a set of S-module generators for $\mathcal{M} = \mathcal{F}/\mathcal{N}$ as well.

The result of Theorem 1.2.1 gives the justification for the MGE-procedure as it ensures, in the case that $\mathcal{M}$ is P-module isomorphic to a P-module Θ that has a finite generating set as S-module, that any ascending sequence of A-modules

$$\mathcal{N}_{(0)} \subset \mathcal{N}_{(1)} \subset \cdots \mathcal{N}_{(\iota)} \cdots \subset \mathcal{N}_{(\nu)} = \mathcal{N},$$

where $\mathcal{N}_{(\iota)} = \mathcal{N}_{(\iota-1)} + \langle r_{(\iota)} \rangle_A$ for a relation $r_{(\iota)} \in Rels\backslash\{r_{(1)}, \ldots, r_{(\iota-1)}\}$, terminates.

We aim to formalise the process of enumerating the S-module generating set of $\mathcal{M}$. For bookkeeping reasons we first define a set of alphabets $B_{(0)}, \ldots, B_{(\iota)}, \ldots, B_{(\nu)}$ where a set $B_{(\iota)} = \{b_1, \ldots, b_{m(\iota)}\}$ denotes an S-module generating set for a certain S-module. For all $0 \leq \iota \leq \nu$ the set $B_{(\iota)}$ is a finite ordered set with elements that are taken from an infinite pool of elements $\mathcal{B}$ in bijection to $\mathbb{N}$.

The set $B_{(0)}$ can be understood as a first approximation of the generating set for the S-module $\Theta \cong \mathcal{M}$, but normally many further adjustments must take place. The examination of a relation $r_{(\iota)} \in Rels$ might make it necessary to add further elements to the set of S-module generators, namely whenever a prefix of $r_{(\iota)}$ has been found which is not contained in the S-linear span of any previously investigated prefixes. We will assign $b' \in \mathcal{B}\backslash B_{(\iota)-1}$ to this prefix. Moreover we might discover that an element $b \in B_{(\iota)}$ is contained in the S-linear span of other $b_{i_1}, \ldots b_{i_t} \in B_{(\iota)}$ which would imply that b is redundant as a further S-module generator. In this case we shall remove b

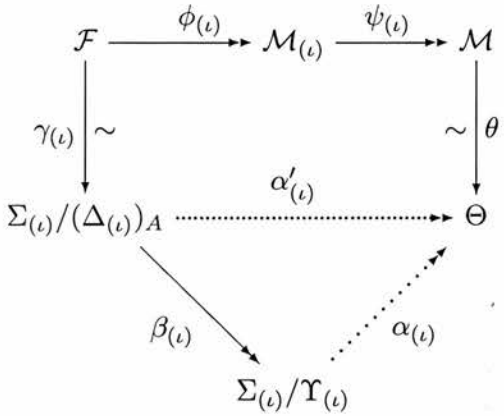
from the set of possible S-module generators and we also say that b has been *deleted*. We distinguish between the subset $B^d_{(\iota)} \subset B_{(\iota)}$ of deleted S-module generators and the subset of undeleted S-module generators $B^u_{(\iota)}$.

Extending the S-module generating set $B_{(\iota)}$ by a further element $b' \in \mathcal{B}\backslash B_{(\iota)}$ is called a *definition step*. As different generating sets $B_{(\iota)}$ can accompany a relation $r_{(\iota+1)}$ we distinguish between these which gives sets $B_{(\iota)_0}, B_{(\iota)_1}, \ldots, B_{(\iota)_{t(\iota)}}$. If we are given an S-module generating set $B_{(\iota)_j}$ we then set

$$B_{(\iota)_{j+1}} := B_{(\iota)_j} \cup \{b_m\}$$

where b_m corresponds to the prefix which has been found last and where we ensure that $b_m > max\{b \in B_{(\iota)_j}\}$.

We form the free S-module $\Sigma_{(\iota)} := \langle B_{(\iota)} X^* \rangle_S$ and an S-submodule $\Delta_{(\iota)_j}$ which is generated by elements $b.x - b'$ induced by definition steps in the following way. Suppose that $b = \rho(y.w)$ but $\rho(y.wx) \notin \langle B \rangle$. We make the definition $b' := \rho(y.wx)$. Then b' and $b.x$ both correspond to the element $y.wx$, although in different stages, such a stage is specified by the index "$(\iota)_j$", of the computation. Then we define $\Delta_{(\iota)_j}$ as that S-module which is generated by the elements of the form $b.x - b'$. It follows from the construction of $\Delta_{(\iota)_j}$ that $\mathcal{F} \cong \Sigma/(\Delta)_A$ for all $(\iota)_j$, where $(\Delta)_A$ denotes the A-closure of Δ. We aim to construct S-modules $\Sigma_{(\iota)}, \Delta_{(\iota)}$ and $\Upsilon_{(\iota)}$ such that the following diagram commutes:



and eventually we wish to obtain modules $\Sigma_{(\nu)}$ and $\Upsilon_{(\nu)}$ accompanying the A-module $\mathcal{N}_{(\nu)} = \mathcal{N}$ such that $\Theta_{(\nu)} := \Sigma_{(\nu)}/\Upsilon_{(\nu)}$ is isomorphic to $\Theta = \mathcal{M}_S$

by a P-module isomorphism $\alpha_{(\nu)}$.

Since we aim to keep the number of S-module generators for $\Theta_{(\nu)}$ as small as possible, an important part of the procedure is the active search for those generators which are redundant as they are contained in the S-linear span of generators with smaller indices. We aim to obtain such linear dependencies by mapping $r \longmapsto v_r \in \langle B \rangle$ for $r \in Rels$. As $r \in \mathcal{N}$ it follows that $\alpha'(v_r)$ must be zero in Θ, so we can deduce that $\alpha'(HT(v_r)) = \alpha'(RED(v_r))$ must hold for the head term $HT(v_r)$ and the reduct of v_r which is defined as $RED(v_r) := HT(v_r) - v_r$. We will call such an element v_r a *coincidence.*

Let $v_r = \sum_{i=1}^{m} \lambda_i \cdot b_i$. If the head coefficient λ_m is a unit of S we say that v_r is an *applicable coincidence.* We can deduce that $b_m \sim \lambda_m^{-1} \cdot RED(v_r)$ and it follows that b_m is redundant as S-module generator for Θ and can be deleted. In order to conclude that a generator b_m is S-linear dependent to other generators it is however essential that the head coefficient λ_m is a unit of S which is not necessarily the case if S is not a field. It follows that we might encounter coincidences which we cannot process in the described way. In this case we say that such a coincidence is an *inapplicable coincidence* and it is stored in a separate list with elements which are ordered by their head monomials. This list is called the *torsion sequence* and denoted by L.

The S-modules $\Upsilon_{(\iota)}$, which we introduced above satisfying $\Sigma_{(\nu)}/\Upsilon_{(\nu)} \cong \mathcal{M}$, are defined as the A-module closure of that S-module that is generated by the elements induced by the definition steps together with elements in Σ induced by coincidences. To be precise, let $\pi : \Sigma \longrightarrow\!\!\!\!\!\rightarrow \Sigma/(\Delta_{(\iota)})_A$; we set $K \subset \Sigma$ to be the set such that for all $k \in K$ we have $\pi(k) = c$ where c is a coincidence which has been found up to that stage of the MGE-procedure. Moreover we denote by H the generating set of Δ. We then define $\Upsilon = \langle H, K \rangle_A$, and we denote the product on Σ/Υ by the generators $x \in X$ by $(b + \Upsilon) \star x$.

In Chapter 2 we also give a description of the tools which are used to formalise the process of processing the relations and thus enumerating the S-module generators. The action of the generators $x \in X$ of the algebra A on the S-module generators $b \in B^u$ is presented by the entries of a multiplication table $T_{(\iota)}$: this table corresponds to the table used in the Todd-Coxeter

Enumeration. The table $T_{(\iota)}$ takes into account possibly found coincidences up to the stage (ι) and the rows of $T_{(\iota)}$ are in a one-one relation to the elements of $B_{(\iota)}$. Furthermore, coincidences that have been detected but which could not be processed immediately are stored in the *coincidence stack* Cp; coincidences that have already been processed but which have been found to be inapplicable are stored in the torsion sequence $L_{(\iota)}$. We define $\Lambda_{(\iota)}$ as the free S-module that is generated by $l \in L_{(\iota)}$. We will show in Chapter 5 that

$$\Theta_{(\nu)} \cong_P \langle B^u_{(\nu)} \rangle_S / (\Lambda_{(\nu)})_A.$$

when the MGE-procedure terminates.

Chapter 3

We introduce Gröbner bases for free S-modules and the respective A-module closures. B. Reinert et. al. [36, 37] have studied interpretations of the Todd-Coxeter procedure in terms of *prefix Gröbner bases*. We will use the terminology of Gröbner basis theory such as ordering and reduction in order to describe and interpret certain processes of the MGE-procedure. Moreover, in subsequent chapters properties of certain kinds of Gröbner bases will be used to prove correctness and termination of the MGE-procedure.

We assume that S is an ordered Euclidean domain. We describe the concept of ordering and reduction for the elements of finitely generated and free S-modules Ξ and the respective A-module closures Υ. In the latter case we will order elements $v \in \Upsilon$ by the maximal length of words $w \in X^*$ of summands $y.w$ of v; we call this *ordering by weight* and we denote that v_1 is greater than v_2 by

$$v_1 \succ_{wei} v_2 \qquad \text{for } v_1, v_2 \in \Sigma.$$

We describe *critical pairs*. These are a phenomenon caused if the reduction by a set of elements does not lead to a canonical irreducible (or *minimal*) element. B. Buchberger described in [6, 7] the effect of critical pairs on reduction and the close connection to Gröbner bases. His computational approach includes the so-called $\mathfrak{s}$*-polynomial* which is defined in order to

detect critical pairs. We shall apply terms such as the $\mathfrak{s}$-polynomial or a Gröbner basis to the setting of free S-modules and we shall describe certain properties of such S-module Gröbner bases. In particular if we are given a submodule Ξ of the free S-module Σ such that Ξ is generated by a finite S-module Gröbner basis then we can show that reduction of an element $v \in \Xi$ by H leads to the minimal element $\overline{v} = 0$ (Corollary 3.1.14, p. 59).

We then present in Theorem 3.1.17 Buchberger's Theorem in the case of finitely generated submodules of free S-modules. In Theorem 3.1.21 (p. 65) we show that there exists a finite S-module Gröbner basis for a given finitely generated S-module from which we can moreover construct an S-module Gröbner basis containing elements that are in minimal form with respect to each other.

In Section 3.2 we introduce prefix-reduction on free A-modules and prefix Gröbner bases. Detailed descriptions of prefix Gröbner bases for ideals of monoid and group rings can be found for instance in [35]. We shall discuss connections between prefix-reduction and prefix Gröbner-bases which provide similar results to the case of S-modules. Next we introduce the concept of *prefix-closure* (Definition 3.2.16, p. 77): if we are given elements $v_1, v_2 \in \Sigma$ and $w \in X^*$ such that $HM(v_1).w = HM(v_2)$ we then denote the element $v_1.w$ as the prefix-closure of v_1 and v_2 and we say that a set H is *prefix-closed* if the prefix-closure for every such pair is already contained in H.

We show in Lemma 3.2.17 that the process of prefix-closing a finite set $H \subset \Sigma$ is finite, leading to a finite prefix-closed set $\widetilde{H}$. When $\widetilde{H}$ has been formed as the prefix-closure of a set H then we show in Lemma 3.2.18 that the respective A-modules generated by those sets are equal,

$$\langle H \rangle_A = \langle \widetilde{H} \rangle_A.$$

As the process of constructing a prefix-closed S-module Gröbner basis for a finitely generated A-module is finite (Proposition 3.2.19) we can show in Theorem 3.2.20 that, given a finitely generated S-module Ξ, a prefix-closed S-module Gröbner basis for Ξ also is a prefix Gröbner basis for the A-module closure $(\Xi)_A$. From this theorem we can deduce in particular that

there exists a finite prefix Gröbner basis for the A-module closure Υ of a finitely generated S-module Ξ.

Chapter 4

We present the main routines of the MGE-procedure in pseudo-code and we prove correctness of the respective procedures. We aim to apply the Gröbner basis methods which have been developed in the previous chapter to the setting of the MGE-procedure. Let H denote the generating set of Δ, the S-module which is induced by the definition steps of the MGE-procedure. We show in Lemma 4.2.1 (p. 94) that H is a prefix Gröbner basis for $(\Delta)_A$. It follows that a representative $\overline{v}$ of a class $(v+(\Delta)_A) \in \Sigma/(\Delta)_A$ can be chosen in a canonical way and therefore we can define a map $\zeta : \Sigma/(\Delta)_A \longrightarrow \Sigma$, mapping a class $(v + (\Delta)_A)$ to its canonical representative $\overline{v}$. We show that ζ indeed forms an S-module homomorphism.

From now onwards we distinguish between applicable coincidences which have already been processed, the set of these is denoted Ca, and the set of pending coincidences Cp. We form an S-module Π which is generated by the set $H \cup Ca \cup Cp \cup L$ and the respective A-module closure Ψ. We demonstrate how this module represents the information stored in the tools of the MGE-procedure (Lemma 4.2.5, p. 96), so for instance the set $H \cup Ca$ corresponds to the information contained in the multiplication table. Accordingly we abbreviate $\widetilde{T} := H \cup Ca$.

We then show the correctness of the procedure HANDLING INAPPLICABLE COINCIDENCES. We prove that applicable coincidences cannot be contained in the S-linear span of elements of L in the case that two prerequisites are satisfied: firstly we demand that $HM(l_i) > HM(l_j)$ whenever $j > i$ for all $l \in L$ (we call this *pivot-form*), moreover we demand that only inapplicable coincidences are contained in L. In this case we say that L is *reduced*. We can relate the procedure PROCESSING A COINCIDENCE to prefix-reduction and prefix-closure (Proposition 4.2.11) which proves that this procedure is finite.

Next we introduce the notion of an *MGE-basis*. This is a certain type of prefix Gröbner basis (Definition 4.2.14) and we can show that the module Ψ,

as defined above, is generated by an MGE-basis in the case that $Cp = \emptyset$ and where it is also verified that L is reduced and in pivot-form (Lemma 4.2.15). For the partial converse of this statement we need a constraint on the multiplication table. We demand that T is *connected* (Definition 4.2.17, p. 104): this constraint essentially implies that every $b \in B^u$ is contained as a sum or a prefix of at least one element of the set $\widetilde{T}$.

So if T is connected and the generating set of Ψ is an MGE-basis then we show in Lemma 4.2.19 that $\langle Cp \rangle_A \subset \langle \widetilde{T} \cup L \rangle_A$. It follows that in this case the coincidences stored in Cp do not lead to any further reductions of elements of the table and the torsion sequence. Thereafter we prove termination and correctness of the procedure CLEARING COINCIDENCES where we show that CLEARING COINCIDENCES constructs from a given generating set $\widetilde{T} \cup L \cup Cp$ for $\Psi \subset \Sigma$ an MGE-basis G which is a finite set of elements of Σ' such that $\Psi \subset \langle G \rangle$ but where it is ensured that $\Sigma/\Psi \cong_A \Sigma'/\langle G \rangle_A$.

We define Φ as the A-module closure of the free S-module which is generated by that subset of $\widetilde{T}$ which corresponds to the undeleted rows of T, together with the elements of L. We show in Proposition 4.2.22 that $\Sigma/\Psi \cong_A \Sigma^u/\Phi$ if the generating set of Ψ is an MGE-basis. We complete this chapter with Theorem 4.2.23. Suppose we are given at stage (ι) of the computation a connected multiplication table T and a coincidence stack $Cp = \emptyset$. The theorem states that then those rows of T which correspond to the undeleted S-module generators $b \in B^u$ together with the elements of the torsion sequence L encode a set of generators for the submodule $\Phi_{(\iota)}$ such that

$$\mathcal{F}/\mathcal{N}_{(\iota)} \cong \Sigma^u_{(\iota)}/\Phi_{(\iota)}.$$

This theorem in particular verifies that the main procedure, in the case it terminates, returns the correct result.

Chapter 5

We introduce the *image-induced ordering* " $\succ_{ii}$ " on the elements of $\mathcal{F}$ which is an ordering determined by the MGE-procedure. More accurately, this ordering is fixed by the image of the homomorphism $\chi : \mathcal{F} \longrightarrow \Sigma$ which is defined as the composition of $\gamma : \mathcal{F} \longrightarrow \Sigma/(\Delta)_A$ with $\zeta : \Sigma/(\Delta)_A \longrightarrow \Sigma$.

So if $f_1, f_2 \in \mathcal{F}$, then

$$f_1 \succ_{ii} f_2 \text{ if and only if } \chi(f_1) \succ_{wei} \chi(f_2).$$

Furthermore we define prefix-reduction rules on the elements of $\mathcal{F}$, using the ordering $\succ_{ii}$. These reduction-rules resemble the computing of the undeleted image $u(v)$ of an element $v \in \Sigma$. Thus we reduce $f \in \mathcal{F}$ with $\chi(f) = v$ by certain elements $q \in \mathcal{F}$ with $\chi(q) \in \langle B \rangle$ where moreover $HM(\chi(q))$ is a prefix of a summand of v and where we have that $\lambda \geq HC(q)$ for the coefficient λ at this summand of v. The ordering "$\succ_{ii}$" provides a well-founded ordering for the elements of $\mathcal{F}$ in the sense that the prefix-reduction as described above does not lead to any cycles or infinite reduction-sequences (Lemma 5.1.8, p. 117).

Connections between the generating sets of the S-modules Σ, Υ and certain sets of congruence classes of $\mathcal{F}$ modulo a submodule $\mathcal{N}$ are investigated. If we can choose a representative $\overline{f} \in |f|_{\mathcal{N}}$ of a congruence classes $|f|_{\mathcal{N}}$ such that $\overline{f}$ is prefix-minimal with respect to the generating set of $\mathcal{N}$ by " $\succ_{ii}$ " then we call $|f|_{\mathcal{N}}$ an *important class* (Definition 5.2.1, p. 119). In the course of an MGE-procedure we construct a generating set for $\mathcal{N}$ as the preimage of those elements which are contained in the generating set of Υ. We show in Lemma 5.2.3 that a congruence class $|f|_{\mathcal{N}}$ is important if and only if a representative $\overline{f} \in |f|_{\mathcal{N}}$ can be chosen such that $\chi(\overline{f}) = b \in B^u$. Moreover, if both $\mathcal{F}$ as well as the submodule $\mathcal{N}$ are finitely generated then we can show in Lemma 5.2.6 that the number of important classes is finite. Let $\mathcal{M} = \mathcal{F}/\mathcal{N}$. If $\mathcal{M}$ is isomorphic to a finitely generated S-module then a congruence class of $\mathcal{F}$ modulo $\mathcal{N}$ is either important or it has a representative which is contained in the S-linear span of the representatives of a finite set of important classes (Lemma 5.2.7). We can conclude that in this case there must exist a representative $\overline{f}$ such that $\chi(\overline{f}) \in \langle B^u \rangle_S$ for every congruence class $|f|_{\mathcal{N}}$.

In Section 5.3 we describe the properties that must be satisfied by the multiplication table, the coincidence stack and the torsion sequence accompanying an A-module $\mathcal{N}_{(\nu)}$ in order for the MGE-procedure to terminate. We demand five properties, firstly that we have $b \star x \in \langle B^u_{(\nu)} \rangle_S$ for every

pair $b \in B^u$ and $x \in X$. This property applies to the entries of the multiplication table and if this condition is satisfied by the entries of a table T we say that T is *closed*. Secondly we demand that $Cp = \emptyset$, and moreover we demand that for every $l \in L$ the A-module closure is contained in L as well. From this it follows in particular that $(\Lambda)_A = \Lambda$ for the S-linear span Λ of L. The last two of these five conditions apply to the relations of $\mathcal{M}$. Here we demand that for all algebra-relations $r \in R$ and $b \in B^u$ we have that $b.r \in \Sigma_{(\nu)}$ can be prefix-reduced by generators of $\Upsilon_{(\nu)}$ to 0. Similarly we require that for every module relation $\omega \in U \subset \mathcal{F}$ the element $\chi(\omega) \in \Sigma_{(\nu)}$ can be prefix-reduced by generators of $\Upsilon_{(\nu)}$ to 0.

If these conditions are satisfied we can show that $\mathcal{M}$ is P-module isomorphic to the quotient-module of a free S-module with finite generating set B^u by the S-module Λ (Proposition 5.3.5, p. 126). In the course of the MGE-procedure we have constructed an infinitely generated S-module $\Sigma = \langle BX^* \rangle$ such that $\mathcal{M}$ is A-module isomorphic to the quotient-module of Σ by the A-module closure Υ of a finitely generated S-module. As the table T is closed, the conditions of Proposition 4.2.22 are satisfied and we can deduce that $\mathcal{M}$ is A-module isomorphic to the S-module Σ^u/Φ. Moreover we can even conclude, again since T is closed, that $v \sim_{\Upsilon_{(\nu)}} \overline{v} \in \langle B^u \rangle_S$ for every $v \in \Sigma$. Therefore

$$\mathcal{M} \cong \Sigma^u/\Phi \cong \langle B^u \rangle_S/(\Lambda)_A = \langle B^u \rangle_S/\Lambda,$$

and since all algebra-relations $r \in R$ hold, these isomorphisms must even be P-module isomorphisms. From this proposition it follows that every congruence class of $\mathcal{F}$ modulo $\mathcal{N}_{(\nu)} = \mathcal{N}$ is important or has a representative which lies in the S-linear span of representatives of important classes (Corollary 5.3.6). We complete Chapter 5 with the main theorem.

Theorem 5.3.8 *Let $\mathcal{F}$ be a finitely generated and free A-module. If $\mathcal{M}_P$ is isomorphic to a finitely generated S-module $\Theta_{(\nu)}$ then the computation of the MGE-procedure reaches a final state where the given torsion sequence is reduced and in pivot-form, provided that we are following a fair strategy.*

Chapter 6

We describe how a finite presentation for a certain A-module can be constructed. The presented algorithm follows closely the idea of extended coset enumeration which is also known as the modified Todd-Coxeter algorithm (see for instance [2, 41]). We shall translate this into the following. Let $\mathcal{D}$ denote the free P-module that is generated by a set Y' in bijection to the generating set of $\mathcal{F}$ and let $\widehat{\mathcal{N}}$ denote the submodule of $\mathcal{D}$ such that $\mathcal{M}_P = \mathcal{D}/\widehat{\mathcal{N}}$. We shall show how an A-module presentation for $\widehat{\mathcal{N}}$ can be constructed in the case that $\mathcal{M}$ is P-module isomorphic to a finitely generated S-module. Since there exists a canonical A-module epimorphism $\phi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}$ we can consider $\mathcal{D}$ as an A-module where every $d \in \mathcal{D}$ is of the form $d = f + \langle YX^*R \rangle_A$.

We have proved in Theorem 1.2.1 that $\mathcal{N}$ is a finitely generated A-module if $\mathcal{M} = \mathcal{F}/\mathcal{N}$ is isomorphic to a finitely generated S-module. We show in Lemma 6.1.1 that then $\widehat{\mathcal{N}}$ has a finite generating set as A-module as well. We follow the ideas of C. Sims in the description of the construction of this presentation as presented in [41].

As has been discussed in Chapter 4, the multiplication table together with the torsion sequence gives rise to a set of elements of Σ. If there are no coincidences pending in Cp, this set forms a generating set for the module Υ from which, after termination of the MGE-procedure, we obtain a finite generating set for $\mathcal{N}_A$.

By assumption the MGE-procedure has already terminated, and so the multiplication table must be closed and it follows that every $v \in \Sigma$ is congruent modulo Υ to an element $\overline{v} \in \langle B^u \rangle_S$. An element of $\mathcal{M}$ corresponds to a congruence class of $\mathcal{F}$ modulo $\mathcal{N}$, and as $\mathcal{M} \cong \Sigma/\Upsilon$ we can assign to every $v \in \Sigma$ a representative $f_v \in \mathcal{F}$ of a class $|f|_{\mathcal{N}}$, and correspondingly we can assign a representative $\widehat{f}_v := \phi(f_v)$. We choose f_v as the preimage $\gamma^{-1}(\pi(\overline{v}))$ of the unique minimal element $\overline{v} \in \langle B^u \rangle_S$ where $\pi : \Sigma \longrightarrow\!\!\!\!\!\rightarrow \Sigma/(\Delta)_A$ denotes the canonical quotient-map. We choose $f_0 = 0$ as the representative of $\mathcal{N}$.

Since the table is closed this implies in particular that there exists $\overline{v} \in \langle B^u \rangle_S$ such that $b.x \sim_\Upsilon \overline{v}$ for every pair $b \in B^u, x \in X$. It follows that

$\gamma^{-1}(\pi(b)).x \sim_{\mathcal{N}} \gamma^{-1}(\pi(\overline{v}))$ and therefore in particular

$$\gamma^{-1}(\pi(b)).x - \gamma^{-1}(\pi(\overline{v})) \in \mathcal{N}.$$

Moreover in the case that $b.x \not\sim_{(\Delta)_A} \overline{v}$ then $f_b.x \sim_{\mathcal{N}} f_{\overline{v}}$ but $f_b.x \neq f_{\overline{v}}$ and we obtain a nonzero element $f_b.x - f_{\overline{v}} \in \mathcal{N}$. In a similar way we can construct elements which are induced by the torsion-elements of Θ. If $b \in B^u$ but $\lambda \cdot b \in \Upsilon$ then it follows that

$$\lambda \cdot f_b \neq f_{\lambda \cdot b} = f_0.$$

If $\mathcal{M}$ is not cyclic a third type of generator is possible. In the case that an A-module generator $y_k \in Y$ is congruent modulo $\mathcal{N}$ to an S-linear combination $\sum_{i=1}^{k_j} \lambda \cdot y_i$ then it follows that

$$f_{b_k} \sim_{\mathcal{N}} f_{\sum_{i=1}^{k-j} \lambda_i \cdot b_i}$$

where we have set $b_i := \gamma(y_i)$ in the course of the MGE-procedure. We denote by E the generating set of $\mathcal{N}$ induced by the MGE-basis G of Υ such that $E = \{\gamma^{-1}(\pi(G))\}$. We show in Lemma 6.1.2 that then each $e \in E$ is of the form either $e = f_b.x - f_v, e = \lambda \cdot f_b$, or $e = y_k - f_{b_k} = y_k - \sum_{i=1}^{k_j} \lambda \cdot y_i$.

If we set $\mathcal{K} := \langle E \rangle_A$ we can define a homomorphism $\alpha : \mathcal{K} \longrightarrow \mathcal{N}$ and since E generates $\mathcal{N}$ this morphism α must be surjective. Furthermore we define $\beta : \mathcal{K} \longrightarrow \widehat{\mathcal{N}}$ as the composition of α and ϕ which implies that β must be surjective as well. We however cannot assume that β is injective. In particular if the algebra P is not free then $\widehat{\mathcal{N}}$ cannot be a free A-module and accordingly β cannot be injective. We introduce a congruence relation " $\approx$ " on the elements of $\mathcal{K}$ such that

$$k_1 \approx k_2 \quad \text{if} \quad \beta(k_1) = \beta(k_2);$$

similarly we define a congruence relation " $\equiv$ " on the elements of $\mathcal{F}$, namely

$$f_1 \equiv f_2 \quad \text{if} \quad \phi(f_1) = \phi(f_2).$$

In order to specify notation we introduce certain elements $\Omega(v, a) \in \mathcal{K}$. We set $\Omega(v, a)$ such that

$$\alpha\big(\Omega(v, a)\big) \equiv f_v.a - f_{v.a},$$

furthermore we set $\Omega(y_i)$ such that

$$\alpha\big(\Omega(y_i)\big) \equiv y_i - f_{b_i}.$$

Here we suppose that we have set $b_i := \gamma(y_i)$ in the MGE-procedure. In Lemma 6.1.7 up to Corollary 6.1.15 we shall develop a constructive way of expressing elements $\Omega(v, a)$ modulo " $\approx$ " as A-linear combination of elements $\Omega(b, x)$ together with elements of the form $\Omega(b, \lambda)$.

Thereafter we have the means to describe relations on the elements of $\mathcal{K}$ in order to construct an A-module presentation for $\widehat{\mathcal{N}}$ in terms of the generating set E. We describe two sets of relations which must be satisfied for the elements of $\mathcal{K}$. The first set is induced by the set of algebra relations R of the algebra P : we define $Z_1 \subset \mathcal{K}$ as the following set

$$Z_1 = \{\Omega(b, a_1) - \Omega(b, a_2) \mid b \in B^u, a_2 = a_1 + r \text{ for } r \in R\}.$$

The second set of relations is induced by the choice of the representatives f_b. We set $f_b := \gamma^{-1}(\pi(v))$ where $\overline{v}$ is minimal with respect to the MGE-basis of $\Upsilon \subset \Sigma$. Since an image $b \in B$ under γ is assigned whenever it becomes necessary to trace a relation, we might encounter elements of $\mathcal{F}$ such that $y_{i_1}.w_{j_1} \succ_{ii} y_{i_2}.w_{j_2}$ but where $y_{i_1}.w_{i_1}x \prec_{ii} y_{i_2}.w_{i_2}x$. In particular it is possible that an element $f_v = y.wx \in \mathcal{F}$ is minimal whereas it has a non-minimal prefix $y.w$. However, if $y.w$ is non-minimal then this implies that $y.w = \alpha(HM(e))$. In this case the tracing of f_v might lead to linear combinations of $e \in E$ with respect to the image under α. We set $\Omega(f) \in \mathcal{K}$ such that $\alpha(\Omega(f)) \equiv \sum_{i=1}^{n} \alpha(\Omega(y_i)).a_i + \sum_{i=1}^{n} \alpha(\Omega(b_i, a_i))$ for $f = \sum_{i=1}^{n} y_i.a_i$. In particular for $e \in E$ we have that $\alpha(e) \in \mathcal{N}$ and we can show that $\alpha(e) \equiv \alpha\big(\Omega(\alpha(e))\big)$ must hold. Accordingly we define $Z_2 \subset \mathcal{K}$ as

$$Z_2 = \{e - \Omega(\alpha(e)) \mid e \in E\}.$$

We show in Lemma 6.2.3 that $\Omega(v, a_1) \sim_{Z_1} \Omega(v, a_2)$ holds for all $v \in \Sigma$ and all a_1, a_2 with $a_2 = a_1 + q$ where q is contained in the ideal generated by the algebra relations R. We show in Lemma 6.2.4 that $k \sim_{Z_2} \Omega(\alpha(k))$ for all $k \in \mathcal{K}$. From this we can deduce in Corollary 6.2.5 that we obtain a presentation

$$\widehat{\mathcal{N}} = \langle E \mid Z_1 \cup Z_2 \rangle_A.$$

We conclude Chapter 6 with Theorem 6.2.6 which gives upper bounds on the numbers of generators and relations which are needed for the presentation for $\widehat{\mathcal{N}}_A$ that is constructed from a given MGE-procedure.

Chapter 7

In Section 7.1 we describe those parts of the implementation of the MGE-procedure where routines might slightly differ from the general description of the routines presented in Chapter 4 or where a description of closer detail is indicated. For instnace we describe here how elements are stored in the course of the procedure and we specify the lookahead method which is used by the MGE-procedure. In Section 7.2 we give a set of examples together with the respective runtimes. Here we state how many definition steps have been necessary, the length of the output and also how many S-module generators have been deleted in the normal mode compared to the lookahead mode.

Chapter 1

Preliminaries

In this chapter we shall introduce terminology used for the module generator procedure. We describe the setting in a wider sense as well as showing some of the results which will be needed for the procedure.

Section 1.1: We introduce algebraic systems such as rings, principal ideal domains, algebras, modules and describe ideas used for the module generator procedure such as presentations of algebras and modules or the greatest common divisor of elements of a principal ideal domain.

Section 1.2: O. Schreier [40] has shown that for a finitely generated group G with subgroup H and index $[G : H] < \infty$ a finite set of generators for H can be constructed. These generators are known as Schreier-generators. We shall translate the Schreier-generator Theorem into the setting of modules over principal ideal domains and the corresponding result shall be shown.

1.1 Basic Definitions and Notation

We shall describe a linear version of the algorithm for coset enumeration. For a detailed description of this algorithm, which is also known as the Todd-Coxeter algorithm see, for instance, [43, 32, 41]. We call this algorithm the **module generator enumeration procedure** and we shall normally use "MGE-procedure" as an abbreviation for this. The input of the MGE-procedure includes a certain ring S. We demand that S is a *Euclidean domain.* Given a ring S we write the multiplication of elements $s_1, s_2 \in S$

by $s_1 \cdot s_2$. Moreover given maps $f : \mathcal{M} \longrightarrow \mathcal{N}$ and $g : \mathcal{N} \longrightarrow \mathcal{P}$, we write the composition of the maps f and g by

$$g \circ f : \mathcal{M} \longrightarrow \mathcal{P}.$$

Definition 1.1.1 *We call a ring a* **domain** *if it has the following properties: S is a commutative ring with $1_S \neq 0_S$, so the ring S itself is non-trivial. A domain S does not have any zero-divisors, so that if $s_1 \cdot s_2 = 0_S$ for $s_1, s_2 \in S$ it then follows that $s_1 = 0_S$ or $s_2 = 0_S$ or that $s_1 = s_2 = 0_S$.*

Definition 1.1.2 *Let $E = \{e_0, e_1, e_2, \dots\}$ be a set. Let " $\succeq$ " denote a binary relation on E that satisfies the following two properties:*

1. *If $e \succeq e'$ and $e' \succeq e$ for $e, e' \in E$ then $e = e'$;*
2. *If $e \succeq e'$ and $e' \succeq e''$ for $e, e', e'' \in X$ then $e \succeq e''$.*

Then we call $\succeq$ an **ordering** *on E. We say that a given ordering $\succeq$ is a* **total ordering** *if we have either $e \succeq e'$ or $e' \succeq e$ for every pair of elements $(e, e') \in E$.*

Definition 1.1.3 *We call a ring S an* **ordered ring** *if S has a total ordering $\geq$ such that for $s_1, s_2, s_3 \in S$ the following holds:*

1. *if $s_1 \geq s_2$ then $s_1 + s_3 \geq s_2 + s_3$;*
2. *if $s_1 \geq 0$ and $s_2 \geq 0$ then $s_1 \cdot s_2 \geq 0$.*

Example 1.1.4 *Examples of ordered Euclidean domains are $\mathbb{Z}$ and also $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{7}]$. An example of a Euclidean domain that is not ordered is the ring of Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ as it is a subring of the complex numbers.*

Let I be the ideal of S generated by a set of elements $\{s_1, s_2, \dots, s_m\} \in S$. We shall write

$$I = \langle s_1, s_2, \dots, s_m \rangle.$$

If S is a **principal ideal domain**, or PID, then for each ideal I in S there exists a single element $\widetilde{s} \in S$ such that $I = \langle \widetilde{s} \rangle$. A domain S is called a

Euclidean domain if there exists a norm on the elements of S which is a function $\nu : S \setminus \{0_S\} \longrightarrow \mathbb{Z}^+ \cup \{0\}$. Additionally, the **Eulidean algorithm** can be applied to every pair of elements of a Euclidean domain S. This means that for a given pair s_1, s_2 there exist elements $\lambda, \kappa \in S$ with $s_2 = \lambda \cdot s_1 + \kappa$ where moreover $\nu(\kappa) < \nu(s_1)$ or $\kappa = 0_S$ holds.

The Euclidean algorithm can be used to compute the **greatest common divisor**, which we call μ, of elements $\kappa_1, \kappa_2 \in S$. The extended Euclidean algorithm moreover provides elements $s_1, s_2 \in S$ such that

$$\mu = s_1 \cdot \kappa_1 + s_2 \cdot \kappa_2.$$

We usually denote the greatest common divisor of κ_1 and κ_2 by $GCD(\kappa_1, \kappa_2)$ and similarly we denote the least common multiple by $LCM(\kappa_1, \kappa_2)$. As can be found in the literature, see for instance M. Artin, [3] Section 11.2, every Eulidean domain is a PID; the converse, however, is not true.

As the next piece of input we introduce a free monoid-algebra over S which we call A. For this, let X denote a finite set and X^* the free monoid generated by X. We define the binary operation on elements $w, w' \in X^*$ as multiplication which we shall write as concatenation ww'. We call an element $w \in X^*$,

$$w = x_1 x_2 \dots x_m,$$

a **word** of X^*. We denote by ε the empty word in the monoid X^*.

Such an algebra over a ring S can be considered as an S-module which has a compatible ring-structure. We shall work with algebras over commutative rings. We choose to describe the scalar-multiplication as an action on the module from the left which gives a function $S \times A \longmapsto A$ such that

$$(s, a) \longmapsto s \cdot a.$$

An element $a \in A$ has the form

$$a = \sum_{w \in X^*} s_w \cdot w$$

where we have $s_w \neq 0$ only for finitely many coefficients. The elements of X^* act on the right on elements of A, which we write as:

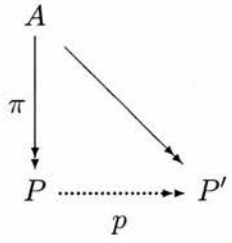
$$(a, w) \longmapsto a.w \in A.$$

Since the algebra A is free, we can consider it as the free S-module with basis X^* and we denote this by $A = \langle X \rangle_S$. Since the set X is finite, we say that A is **finitely generated as an algebra**.

Now let R denote a finite set of elements of A and let $I = \langle R \rangle$ denote the two-sided ideal in A generated by the set R. We define an S-algebra, which we call P, together with a canonical quotient homomorphism

$$\pi : A \longrightarrow\!\!\!\!\!\rightarrow P$$

as the universal quotient algebra of A for which $\pi(I) = 0$. Hence for every S-algebra P' which is a quotient of A such that the elements of R get mapped to 0, there exists a surjective S-algebra homomorphism $p : P \longrightarrow\!\!\!\!\!\rightarrow P'$ making the following diagram commutative:



Such a universal quotient algebra P is called the **finitely presented algebra** which is generated by a set X and which has **relations** R. We present such an algebra P in terms of its generators and relations as follows:

$$P = \langle X \mid R \rangle_S.$$

The next part of input for the MGE-procedure consists of the description of a certain module over the algebra P which we call $\mathcal{M}$. We suppose here that $\mathcal{M}$ is a right P-module. Then multiplication of elements $m \in \mathcal{M}$ by elements $p \in P$ shall be denoted by $m.p$. It forms a mapping $\mathcal{M} \times P \longrightarrow \mathcal{M}$ with $(m, p) \longmapsto m.p$.

We suppose that $\mathcal{M}$ has a finite set of n generators as a right P-module. Generally, every module generated by a set of certain cardinality, say t, is the quotient-module of a free module (over the same ring) generated by a set also of cardinality t. Therefore there exists an n-generated, free module

$$\mathcal{D} := P^n$$

with generating set $Y' = \{y'_1, \ldots, y'_n\}$ (we might also write $\mathcal{D} = \langle Y' \rangle_P$) together with a P-module epimorphism $\widetilde{\psi} : \mathcal{D} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{M}$. The kernel of the map $\widetilde{\psi}$ is a P-submodule of $\mathcal{D}$ which we call $\widehat{\mathcal{N}}$. We suppose that $\widehat{\mathcal{N}}$ is generated by a finite set of elements $\widetilde{U} \in \mathcal{D}$ (as a P-module). Then $\mathcal{M}$ is the universal P-module for which the **module-relations** $\widetilde{U}$ hold and $\mathcal{M}$ is the finitely presented P-module which can be written as

$$\mathcal{M} = \langle Y' \mid \widetilde{U} \rangle_P.$$

Moreover we introduce the free module over the free algebra A for the further description of the procedure. This free module is generated by the finite set Y with $Y \cong Y'$, and we will denote it by

$$\mathcal{F} := \langle Y \rangle_A.$$

Since the algebra P is a quotient-ring of A, every P-module "inherits" the A-module structure and hence can be considered as an A-module itself:

Lemma 1.1.5 *Let R be a ring and P an R-algebra that is quotient of the free R-algebra A by an ideal $I \subset A$. Let $\mathcal{M}$ denote a (right) P-module. Then $\mathcal{M}$ is a (right) A-module as well.*

Proof. Let $\pi : A \longrightarrow\!\!\!\!\!\rightarrow P$ denote again the canonical quotient-homomorphism which maps an element $a \in A$ to $a + I \in P$. We can define the action of $a \in A$ on elements of $m \in \mathcal{M}$ by

$$m.a := m.\pi(a).$$

Let $p_1, p_2 \in P$ be such that $p_i = \pi(a_i)$ for $i \in \{1, 2\}$. Then $m.(a_1 + a_2) = m.(\pi(a_1 + a_2)) = m.(\pi(a_1) + \pi(a_2)) = m.(p_1 + p_2)$, since $\mathcal{M}$ is a P-module this must be equal to $m.p_1 + m.p_2 = m.\pi(a_1) + m.\pi(a_2)$ which again is the definition of the multiplication of elements of A, namely $m.a_1 + m.a_2$.

Similarly we obtain that $(m_1 + m_2).a = m_1.a + m_2.a$ for $m_1, m_2 \in \mathcal{M}$ and $a \in A$. Moreover $m.(a_1 a_2) := m.(\pi(a_1 a_2)) = m.(\pi(a_1)\pi(a_2)) = (m.\pi(a_1))\pi(a_2)$ which is the definition of $(m.a_1)a_2$, also $m.1_A = m.\pi(1_A) = m.1_P = m$ and it follows that $\mathcal{M}$ is an A-module. □

Therefore, the P-module $\mathcal{D}$ is an A-module also and there is a canonical A-module homomorphism

$$\phi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}$$

which maps the generators $y_i \in Y$ to $\phi(y_i) = y_i'$, the set of generators $y_i' \in Y'$ of $\mathcal{D}$. Considered as A-module, the module $\mathcal{D}$ is not free and in fact the finite set of algebra-relations now gives rise to an infinite set of module-relations: each of the relations $r \in R$ has to be applied to every (one-term) element of the form $y.w \in \mathcal{F}$ for $y \in Y, w \in X^*$. Hence the finite set R gives rise to an infinite set of elements of $\mathcal{F}$,

$$YX^*R := \{y.wr \mid y \in Y, w \in X^*, r \in R\};$$

and therefore, as an A-module, $\mathcal{D}$ satisfies the presentation

$$\mathcal{D}_A = \langle Y \mid YX^*R \rangle.$$

Remark 1.1.6 *In the following we shall use curly letters such as $\mathcal{F}, \mathcal{D}, \mathcal{M} \ldots$ in order to denote modules over an algebra. In general, when we use modules over the domain S we want to use Greek letters such as $\Sigma, \Upsilon, \Xi \ldots$. However, in times of heavy usage of S-modules we may use curly letters as well. Whenever ambiguities might appear we shall use an index as in $\mathcal{N}_S$ or $\mathcal{N}_A$ in order to emphasize that we refer to the module $\mathcal{N}$ as module over the rings S or A, respectively.*

The technique of the MGE-procedure is based on the vector enumeration procedure [25] which computes a matrix representation for a finite dimensional and finitely generated module over a k-algebra where k is a field. For the MGE-procedure we shall generalise this to the case of modules over a Euclidean domain.

This makes the situation more complicated since, when working with modules over a Euclidean domain, **torsion elements** might occur. If we denote by Γ a module over a Euclidean domain S, then a torsion element of Γ is a non-zero element $v \in \Gamma$ for which there exists $s \in S, s \neq 0$, such that $s \cdot v = 0$. In this case s is called an **exponent** of v. It follows that, unlike a

vector-space which is a module over a field, a module over a ring does not generally have a basis. If Γ however is a finitely generated module over a PID (so in particular this holds for a Euclidean domain as well) Γ can be written as the direct sum

$$\Gamma = \Phi_1 \oplus \Phi_2$$

of a free submodule Φ_1 and a submodule Φ_2 which is generated by the torsion generators of Γ; the dimension of Φ_1 is uniquely determined. See for instance S. Lang, in [19] Theorem 7.1 of Chapter 3, for this result. We call Φ_2 the **torsion-submodule** of Γ and the **rank** of Γ is defined as the dimension of the free submodule Φ_1.

The input of the MGE-procedure consists of the finite description of the algebra P by its set of generators X and its finite set of relations R, and moreover of a finite presentation of the module $\mathcal{M}$. However, in the whole course of the procedure we want to consider $\mathcal{M}$ as A-module and in that sense, $\mathcal{M}$ is generated by the set Y. Furthermore, instead of the set of P-module relations $\widetilde{U}$ we choose a set of elements $U \in \mathcal{F}$ for which $\phi(U) = \widetilde{U}$. The elements of $\mathcal{M}_A$ are expressed in terms of the module-generators Y, words made up from elements of the monoid X^* and coefficients which are elements of S. There is again a canonical epimorphism of $\mathcal{D}_A \longrightarrow\!\!\!\!\!\rightarrow \mathcal{M}_A$; we denote by $\mathcal{N}$ the submodule which is generated by the (possibly infinite) set $U \cup YX^*R \subset \mathcal{F}$ and accordingly $\mathcal{M}_A = \mathcal{F}/\mathcal{N}$. It follows that $\mathcal{M}$ satisfies the presentation

$$\mathcal{M}_A = \langle Y \mid U \cup YX^*R \rangle.$$

Example 1.1.7 *Let $A = \langle X \rangle$ be the free $\mathbb{Z}$-algebra generated by $X = \{x_1, x_2\}$ and let $\mathcal{F}_A = \langle y \rangle$ denote the free A-module which is generated by the single element y. We set P to be the finitely presented algebra which is quotient of A by the ideal generated by the element $r = x_2^3 - 1_A \in A$ and we choose elements $u_1, u_2 \in \mathcal{F}$ such that $u_1 = y.x_1^2$ and $u_2 = y.x_1x_2 - y.x_2x_1$ as module-relations of a P-module $\mathcal{M}$. Then, considered as P-module, $\mathcal{M}$ satisfies the finite presentation*

$$\mathcal{M}_P = \langle y' \mid y'.x_1^2, y'.x_1x_2 - y.x_2x_1 \rangle_P.$$

However, as module over the algebra A, we obtain the corresponding presentation

$$\mathcal{M}_A = \langle y \mid y.x_1^2, y.x_1x_2 - y.x_2x_1, y.(x_2^3 - 1), y.x_1(x_2^3 - 1), y.x_1^2(x_2^3 - 1), \ldots \rangle_A$$

and this presentation clearly is not finite at all.

In the case where we apply the MGE-procedure to a P-module $\mathcal{M}$ the input consists of a finite description of the algebra A, the set of algebra-relations R, the set of module-generators Y' and of the set of module-relations U, these considered as elements of the free A-module $\mathcal{F}$. The procedure then works with the elements of $\mathcal{F}$. It aims to obtain information of a module $\Theta_S \cong \mathcal{M}$ by applying the relations of $\mathcal{M}$ to the elements of $\mathcal{F}$ considered as a free module over S.

We shall show that the MGE-procedure terminates if the input of the MGE-procedure specifies a P-module $\mathcal{M}$ which is P-module isomorphic to a P-module Θ. In the given situation a P-module certainly is an S-module as well. We demand the additional condition on the module Θ which we construct, that Θ is generated by a finite set of elements as module over the ring S. In the construction we will consider Θ mainly as module over S. We will however ensure at every point of the construction that Θ is a P-module as well.

To process torsion-elements which occur in the MGE-procedure, we will use the Euclidean algorithm in order to obtain the greatest common divisor $\widetilde{s}$ of a pair s_1, s_2 of elements of S. The extended version of the Euclidean algorithm provides elements $\lambda_1, \lambda_2, t_1, t_2 \in S$, such that λ_1 and λ_2 are relatively prime with respect to each other and $\lambda_1 \cdot s_1 + \lambda_2 \cdot s_2 = \widetilde{s}$, and $t_i \cdot \widetilde{s} = s_i$ for $i \in \{1, 2\}$, so that $\lambda_1 \cdot t_1 + \lambda_2 \cdot t_2 = 1_S$.

The procedure aims to construct from the given input the action of the generators $x \in X$ of the algebra P on the generators of Θ. If the procedure terminates it will have constructed the generating set of a finitely generated and free S-module Γ. Possibly occurring torsion-elements are stored in an ordered list which we shall call the **torsion sequence** and which is contained in the output. We will obtain Θ as the quotient-module of Γ by a submodule

that is generated by those elements contained in the torsion sequence. The action of the algebra generators $x \in X$ on the elements of Θ will be described by a set of S-module endomorphisms. Each algebra-generator x is mapped to a matrix m_x, the entries of which are elements of the ring S. Every such matrix m_x then describes an S-module endomorphism on the set of generators of the S-module Θ which fixes the submodule generators by the torsion sequence.

Lemma 1.1.8 *Let S be a principal ideal domain, P a finitely presented S-algebra and let $\mathcal{M}_P$ be a P-module which is P-module isomorphic to a P-module Θ which is finitely generated as S-module. We can construct a set of matrices m_x, presenting S-module endomorphisms, that describe the action of each of the generators $x \in X$ of P on the generators of Θ. In the case where Θ is not torsion-free, a torsion sequence can be constructed containing a finite set of elements describing the torsion in Θ.*

Proof. Let $\varphi : \mathcal{M} \longrightarrow \Theta$ denote a P-module isomorphism of $\mathcal{M}$ to Θ. As Θ is finitely generated as module over S there must exist a free P-module Γ with finite S-module generating set such that Θ is a quotient-module of Γ. Then there exists a canonical S-module projection $\pi : \Gamma \longrightarrow\!\!\!\!\!\rightarrow \Theta$.

Moreover, since Θ is a finitely generated module over a PID, Θ can be decomposed into a free submodule Ξ, suppose of rank m, and a torsion-submodule Υ :

$$\Theta = \Xi \oplus \Upsilon.$$

Then Υ is finitely generated as well, say by $v_1, \ldots, v_t$. Hence there are non-zero elements $q_1, \ldots, q_t \in S$ such that $q_1 \cdot v_1 = \cdots = q_t \cdot v_t = 0$. We choose the q_i in such a way that there do not exist $\lambda, \widetilde{q}_i \in S$, where λ is not a unit, with $q_i = \lambda \cdot \widetilde{q}_i$.

We can choose the free module Γ such that it is a module of minimal rank, accordingly we choose Γ with rank $m + t$. We order the generators of Γ in such a way that, with respect to the projection π, we have that $b_{m+i} \overset{\pi}{\longmapsto} v_i$ for $1 \leq i \leq t$. We define $\Phi = \langle q_1 \cdot b_{m+1}, \ldots, q_t \cdot b_{m+t} \rangle$ and thus $ker(\pi) = \Phi$. The torsion sequence which we will construct then is just such a list of generators of Φ.

Let $\omega \in \mathcal{M}$. We set $\varphi(\omega) = \sum_{i=1}^{m+t} \lambda_i \cdot b_i + \Phi$ and $\varphi(\omega.x) = \sum_{i=1}^{m+t} \lambda_i' \cdot b_i + \Phi$. We do not demand here that $\lambda_i, \lambda_i' \in S$ are necessarily non-zero. As φ is a P-module isomorphism we certainly have that $\varphi(\omega).x = \varphi(\omega.x)$ for $x \in X$. Thence

$$(\sum_{i=1}^{m+t} \lambda_i \cdot b_i + \Phi).x = \sum_{i=1}^{m+t} \lambda_i' \cdot b_i + \Phi$$

and this can be expressed as a square matrix m_x with $m + t$ rows that has as entries elements $\kappa_i \in S$. □

If the MGE-procedure terminates then the output will consist of a finite set of generators $\{b_1, \ldots, b_{m+t}\}$ of the free S-module Γ together with the respective pre-image of $b_i + \Phi$ in $\mathcal{M}$. Moreover a set of matrices m_x in one-one correspondence to the set of algebra generators $x \in X$ is given and an ordered list L, the torsion sequence, describes the torsion in Θ : the list L contains elements $\sum_{j=1}^{m} \lambda_j \cdot b_j \in \Phi$. Depending on the generating set B which will be constructed by the procedure, the elements of L are not necessarily in the form $\lambda \cdot b$ where λ is the exponent (thence $\lambda \cdot b = 0$ in Θ). By application of a Smith Normal Form computation on the generating set B this could be achieved. Then however information about which elements of $\mathcal{F}$ gave rise to which of the respective S-module generators of Θ might get lost.

1.2 Schreier Generators for Submodules

Let $\mathcal{M} = \mathcal{F}/\mathcal{N}$, where $\mathcal{F}$ is a finitely generated A-module and we suppose that $\mathcal{M}$ is P-module isomorphic to a P-module that is finitely generated as S-module. We shall prove that then a finite generating set for $\mathcal{N}$ exists. O. Schreier introduced in [40] a method for constructing a finite generating set for a subgroup of finite index in a finitely generated group; we translate this method to the setting of modules as above. The result of this theorem will be an important part of the proof of termination of the MGE-procedure.

Theorem 1.2.1 *Let $A = \langle X \rangle$ be a free algebra over a principal ideal domain S. We assume that A is generated by the finitely generated free monoid X^* and we let P be a finitely presented quotient-algebra of A. Moreover, let*

$\mathcal{F}$ be a free module over A, generated by a finite set Y with a submodule $\mathcal{N}$ and let $\mathcal{M}$ be a P-module such that $\mathcal{M} = \mathcal{F}/\mathcal{N}$. If $\mathcal{M}$ is P-module isomorphic to a P-module that is finitely generated as S-module, then $\mathcal{N}$ considered as A-module has a finite set of generators.

Proof. Let r be an arbitrary element in $\mathcal{N}$. When considered as element of $\mathcal{F}$, r is of the following form:

$$r = \sum_{i=1}^{n} y_i.a_i = \sum_{i=1}^{n} y_i.(\sum_{w \in X^*} \lambda_w \cdot w)$$

where $a_i \in A$, $\lambda_w \in S$. Since for an element $a \in A$, $a = \sum_{w \in X^*} \lambda_w \cdot w$, we have that $\lambda_w \neq 0$ only for a finite number of the coefficients λ_w, the element r can be written as:

$$r = \sum_{i=1}^{n} y_i.(\sum_{j=1}^{m} \lambda_{i,j} \cdot w_{i,j}) = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{i,j} \cdot y_i.w_{i,j}.$$

Let π denote the canonical A-module epimorphism $\pi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{M}_A$ which maps an element $f \in \mathcal{F}$ to the class $(f + \mathcal{N})$. So an element $v \in \mathcal{M}$ corresponds to a congruence class $f + \mathcal{N}$ for $f \in \mathcal{F}$. By assumption, the module $\mathcal{M}$ is P-module isomorphic to a P-module Θ which is finitely generated as S-module. We denote the isomorphism by $\varphi : \mathcal{M} \longrightarrow \Theta$. Since the ring S is a PID, Θ can be decomposed as

$$\Theta = \Psi_1 \oplus \Psi_2,$$

where Ψ_1 denotes the free submodule of Θ, and Ψ_2 the torsion-submodule of Θ. Both these modules are again finitely generated as S-modules, and we denote by $\{\beta_1, \ldots, \beta_\mu\}$ and by $\{\beta_{\mu+1}, \ldots, \beta_t\}$ the generating sets of Ψ_1 and Ψ_2 respectively. This yields a set of generators $\{\beta_1, \ldots, \beta_t\}$ of Θ. If we set $b_k := \varphi^{-1}(\beta_k)$ for $1 \leq k \leq t$, we then obtain a finite set of elements $B = \{b_1, \ldots, b_t\}$ which generates $\mathcal{M}$. Again we can decompose the module $\mathcal{M}$ into a free submodule Φ_1 and a torsion-submodule Φ_2, $\mathcal{M} = \Phi_1 \oplus \Phi_2$. Since φ is an P-module isomorphism we must have in particular that $\Phi_i = \varphi^{-1}(\Psi_i)$ for $i \in \{1, 2\}$. It follows that each of the generators $b_k \in B$ must

either be a generator of Φ_1 or of Φ_2. Every b_k corresponds to a coset $f_k + \mathcal{N}$ for $1 \leq k \leq t$ and for each such coset we choose a representative in $\mathcal{F}$ which we denote by $\overline{f}_k$.

Next, consider the free S-module of rank t. We define a morphism $\psi : S^t \longrightarrow \mathcal{M}$ which maps

$$(\lambda_1, \ldots, \lambda_t) \overset{\psi}{\longmapsto} \lambda_1 \cdot b_1 + \cdots + \lambda_t \cdot b_t$$

for an element $(\lambda_1, \ldots, \lambda_t) \in S^t$. The map ψ then is surjective and it generates an equivalence relation " $\sim$ " on the elements of S^t : we say that tuples are equivalent, denoted by

$$(\lambda_1, \ldots, \lambda_t) \sim (\lambda'_1, \ldots, \lambda'_t),$$

if $\psi(\lambda_1, \ldots, \lambda_t) = \psi(\lambda'_1, \ldots, \lambda'_t)$, i.e. if for the corresponding classes of $\mathcal{F}$ we have that $\sum_{i=1}^{t} \lambda_i \cdot (f_i + \mathcal{N}) = \sum_{i=1}^{t} \lambda'_i \cdot (f_i + \mathcal{N})$. From these equivalence classes in S^t generated by " $\sim$ " we choose representatives, and we will call the set of all those representatives Z. Given $(\lambda_1, \ldots, \lambda_t) \sim (\lambda'_1, \ldots, \lambda'_t)$, if we have chosen the element $(\lambda_1, \ldots, \lambda_t)$ as the representative lying in the set Z, then $\sum_{i=1}^{t} \lambda_i \cdot \overline{f_i}$ is the representative of the cosets $\sum_{i=1}^{t} \lambda_i \cdot (f_i + \mathcal{N})$ and $\sum_{i=1}^{t} \lambda'_i \cdot (f_i + \mathcal{N})$. We choose the t-tuple $(0, \ldots, 0)$ as the representative of the coset of $\mathcal{N}$. The set Z then is a subset of S^t and, by construction, it is in a one-one bijection to the elements of $\mathcal{M}$.

Now, every element $f \in \mathcal{F}$ can be decomposed as $f = \overline{f} + r$, where $\overline{f}$ is a representative of a coset implied by the map π, and an element $r \in \mathcal{N}$. Since for all $f \in \mathcal{F}$ we have that $\pi(f) = \pi(\overline{f})$, therefore

$$\overline{f.x} + \mathcal{N} = \pi(\overline{f.x}) = \pi(f.x) = \pi(f).x = \pi(\overline{f}).x = (\overline{f} + \mathcal{N}).x = \overline{f}.x + \mathcal{N}$$

for $f \in \mathcal{F}$ and $x \in X$ and it follows that $\overline{f}.x - \overline{f.x} \in \mathcal{N}$. We set $\Omega(f, x) \in \mathcal{N}$ such that

$$\Omega(f, x) := \overline{f}.x - \overline{f.x}.$$

More generally we can define for $f \in \mathcal{F}$ and $a \in A$ an element $\Omega(f, a)$ with

$$\Omega(f, a) := \overline{f}.a - \overline{f.a},$$

which then also must be an element of $\mathcal{N}$. Additionally we define elements $\Omega(y_i) := y_i - \overline{y_i}$ for module generators $y_i \in Y$ of $\mathcal{F}$ in the case that $y_i \neq \overline{y}_i$. Moreover, in the case that $\mathcal{M}$ has a non-trivial torsion-submodule, there are generators $b \in B$ of $\mathcal{M}$ and $\lambda \in S$ such that $b \neq 0$ but where $\lambda \cdot b = 0$ in $\mathcal{M}$. Accordingly there exist $f \in \mathcal{F}$ such that $\lambda \cdot \overline{f} \neq \overline{\lambda \cdot f}$ and we define

$$\Omega(f, \lambda) := \lambda \cdot \overline{f} - \overline{\lambda \cdot f}.$$

As a coefficient, $\lambda \in S$ can be considered as an element $\lambda \cdot \varepsilon \in A$, an element $\Omega(f, \lambda)$ is a special case of $\Omega(f, a)$ for $a \in A$. However, in order to be able to distinguish between elements Ω which are caused specifically by torsion and those which are not, we will use the terminology of $\Omega(f, \lambda)$ as well. We will show now that every element $r \in \mathcal{N}$ is in fact contained in the A-linear span of such elements Ω :

Proposition 1.2.2 *If $r \in \mathcal{N}$ then r is contained in the A-linear span of elements $\Omega(f, x), \Omega(f, \lambda)$ and $\Omega(y_i)$.*

Proof. Let $r \in \mathcal{N}$. Then $r = \sum_{i=1}^{n} y_i.a_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{i,j} \cdot y_i.w_{i,j}$. Suppose that $w_{i,j} = x_{1_{i,j}} \dots x_{l_{i,j}} \in X^*$ is a word of length l. We will write for abbreviation $w_{i,j}^{(k)} = x_{1_{i,j}} \dots x_{k_{i,j}}$ and also ${}^{[k]}w_{i,j} = x_{k_{i,j}} \dots x_{l_{i,j}}$ for $1 \leq k \leq l$. Accordingly $w = w^{(k-1)}{}^{[k]}w$ for all $w \in X^*$. Furthermore we set $w^{(n)} = {}^{[m]}w = \varepsilon$ for all $n < 1$ and all $m > l$. Then each of the summands $\lambda \cdot y.w := \lambda_{i,j} \cdot y_i.w_{i,j}$, for $1 \leq i \leq n$ and $1 \leq j \leq m$, is equal to

$$\lambda \cdot y.w - \lambda \cdot y.\overline{w^{(1)}}{}^{[2]}w + \lambda \cdot y.\overline{w^{(1)}}{}^{[2]}w + \dots + \lambda \cdot y.\overline{w^{(l-1)}}{}^{[l]}w - \lambda \cdot y.\overline{w} + \lambda \cdot y.\overline{w}.$$

We denote again by l the length of $w_{i,j}$ and we also set $f_{i,j}^{(k-1)} := y_i.w_{i,j}^{(k-1)}$. Therefore a summand $\lambda_{i,j} \cdot y.w_{i,j}$ of r can be expressed as

$$\lambda_{i,j} \cdot \Omega\big(y_i\big).w_{i,j} + \sum_{k=1}^{l} \lambda_{i,j} \cdot \Omega\big(f_{i,j}^{(k-1)}, x_{k_{i,j}}\big).{}^{[k+1]}w_{i,j} + \lambda_{i,j} \cdot \overline{y_i.w_{i,j}}.$$

We denote by $\langle \Omega(\mathcal{F}, X) \rangle_A$ the A-submodule of $\mathcal{F}$ which is generated by the infinite set of elements $\Omega(f, x)$ for $f \in \mathcal{F}$ and $x \in X$. Moreover, we abbreviate $q := \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{i,j} \cdot \overline{y_i.w_{i,j}}$ for an element $r \in \mathcal{N}$. Then

$$(r - q) \in \langle \Omega(y_1), \dots, \Omega(y_n) \rangle_A + \langle \Omega(\mathcal{F}, X) \rangle_A.$$

In order to proceed with the proof of this proposition we now need the following lemma:

Lemma 1.2.3 *The elements q can be expressed using a finite number of elements $\Omega(f, \lambda)$ where $f \in \mathcal{F}$ and $\lambda \in S$.*

Proof. We have that $q = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{i,j} \cdot \overline{y_i w_{i,j}}$, and a summand $\overline{y_i . w_{i,j}}$ of q is a representative of a coset $f + \mathcal{N}$ and for every such representative there then exists a tuple in Z corresponding to it, suppose the corresponding tuple if of the form $(\lambda_1, \ldots, \lambda_t)$. Hence, every $\lambda_{i,j} \cdot \overline{y_i . w_{i,j}}$ can be written in terms of representatives of the generators $b_\mu \in B$ of the module $\mathcal{M}$ with coefficients from the corresponding tuple in Z. We obtain

$$\lambda_{i,j} \cdot \overline{y_i . w_{i,j}} = \lambda_{i,j} \cdot \sum_{\mu=1}^{t} \lambda'_\mu \cdot \overline{f_\mu}.$$

As q is an element of $\mathcal{N}$, we abbreviate by $\widetilde{\lambda}_{i,j,\mu} := \lambda_{i,j} \cdot \lambda'_\mu$, so that

$$q = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{\mu=1}^{t} \widetilde{\lambda}_{i,j,\mu} \cdot \overline{f_\mu} \sim_{\mathcal{N}} 0.$$

Let, as before, Φ_1 denote the free submodule of $\mathcal{M}_S$ and Φ_2 the torsion-submodule of $\mathcal{M}_S$. We distinguish between the following two cases:

In the first case the torsion submodule Φ_2 is trivial, so $\mathcal{M}$ is a free S-module and the generators $b_\mu \in B$ form a basis for $\mathcal{M}$. We can conclude that each of the coefficients $\widetilde{\lambda}_{i,j,\mu}$ must be zero. It follows that $\lambda \cdot \overline{f} = \overline{\lambda \cdot f}$ for all $\lambda \in S$ and $f \in \mathcal{F}$ and accordingly $\Omega(f, \lambda) = 0$.

In the second case the torsion-submodule Φ_2 is not trivial. By assumption, $\mathcal{M}$ is finitely generated as module over the PID S. It follows that Φ_2 must be finitely generated itself. Therefore we can choose a finite number of elements $\kappa \in S$ such that for a subset $\{\nu_1, \ldots \nu_s\}$ of the set of indices $\{1, \ldots, t\}$ we have that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \widetilde{\lambda}_{i,j,\nu_\iota} = \kappa_\iota \neq 0$$

and $\kappa_\iota \cdot b_{\nu_\iota} = 0$ in $\mathcal{M}$ and where moreover all exponents of elements of the torsion-submodule can be obtained as multiples of those elements. These κ_ι are elements of the form

$$\Omega(f_{\nu_\iota}, \kappa_\iota) = \kappa_\iota \cdot \overline{f}_{\nu_\iota} - \overline{\kappa_\iota \cdot f_{\nu_\iota}}.$$

Since the torsion-submodule is finitely generated we can choose a finite number of non-zero elements of this form as generators. So we add all such elements $\Omega(f_{\nu_1}, \kappa_1), \ldots, \Omega(f_{\nu_s}, \kappa_s)$ to the generating set for $\mathcal{N}$. □

This completes the proof of Proposition 1.2.2 as it now follows that $r \in \langle \Omega(y_1), \ldots, \Omega(y_n), \Omega(f_{\nu_1}, \kappa_1), \ldots, \Omega(f_{\nu_s}, \kappa_s) \rangle_A + \langle \Omega(\mathcal{F}, X) \rangle_A$. □

For the proof of Theorem 1.2.1 it remains to show that the A-module $\langle \Omega(\mathcal{F}, X) \rangle_A$ has a finite generating set:

Lemma 1.2.4 *There exists a finite set which generates* $\langle \Omega(\mathcal{F}, X) \rangle_A$.

Proof. As above, we again decompose an element $f \in \mathcal{F}$ as

$$f = \overline{f} + r,$$

where $\overline{f}$ has been chosen as a representative of a congruence class $f + \mathcal{N}$. Accordingly we can insert this into $\Omega(f, x)$ which yields

$$\Omega(f, x) = \Omega(\overline{f} + r, x) = \overline{(\overline{f} + r).x} - \overline{(\overline{f} + r).x}.$$

Let $v \in \mathcal{M}$ such that $v = \pi(f)$. Then $v = \sum_{\mu=1}^{t} \lambda_\mu \cdot b_\mu$ and for every $b_\mu \in B$ there exists a representative $\overline{f}_\mu \in \mathcal{F}$ with $\overline{f}_\mu \in f_\mu + \mathcal{N}$ such that $b_\mu = \pi(\overline{f}_\mu)$. Moreover, we can choose a tuple $(\kappa_1, \ldots, \kappa_t) \in Z$ which corresponds to $v = \sum_{\mu=1}^{t} \lambda_\mu \cdot b_\mu$.

Hence, modulo $\mathcal{N}$, we can write $\overline{f}$ as

$$\overline{f} = \sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu.$$

The elements r and $r.x$ respectively are contained in $\mathcal{N}$: on the one hand we can write $\overline{f} = \overline{\overline{f} + r} = \overline{\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu}$ but we also have that $\overline{f}.x + r.x + \mathcal{N} = \overline{f}.x + \mathcal{N}$, so $\overline{\overline{f}.x + r.x} = \overline{\overline{f}.x}$. It follows that

$$\Omega(f,x) = \overline{f}.x - \overline{f.x} = \overline{\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu.x} - \overline{(\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu).x}.$$

As before we must have that

$$\overline{\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu.x} + \mathcal{N} = \overline{(\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu).x} + \mathcal{N},$$

so there must be a tuple $(\lambda'_1, \ldots, \lambda'_t) \in Z$ which corresponds to the image of $\overline{\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu.x}$ under π, such that $\pi(\overline{\sum_{\mu=1}^{t} \kappa_\mu \cdot \overline{f}_\mu.x}) = \sum_{\mu=1}^{t} \lambda'_\mu \cdot b_\mu$. It follows that

$$\Omega(f,x) = \sum_{\mu=1}^{t} \lambda'_\mu \cdot \overline{f}_\mu.x - \sum_{\mu=1}^{t} \lambda'_\mu \cdot \overline{f_\mu.x} = \sum_{\mu=1}^{t} \lambda'_\mu \cdot (\overline{f}_\mu.x - \overline{f_\mu.x}).$$

Since $\sum_{\mu=1}^{t} \lambda'_\mu \cdot (\overline{f}_\mu.x - \overline{f_\mu.x}) = \sum_{\mu=1}^{t} \lambda'_\mu \cdot \Omega(f_\mu, x)$ we can conclude that an element $\Omega(f,x)$, for arbitrary $f \in \mathcal{F}$ and algebra generators $x \in X$, lies in the A-linear span of the set elements of the form $\Omega(f_\mu, x)$. This set is finite and it follows that the module $\langle \Omega(\mathcal{F}, X) \rangle_A$ then is finitely generated. □

We can conclude that every $r \in \mathcal{N}$ lies in the A-linear span of the finite set

$$\{\Omega(y_i) \mid y_i \in Y\} \cup \{\Omega(f_{\nu_1}, \kappa_1), \ldots, \Omega(f_{\nu_s}, \kappa_s)\} \cup \{\Omega(f_\mu, x) | 1 \leq \mu \leq t, x \in X\}.$$

Thus we have found a finite generating set for the A-module $\mathcal{N}$. □

Chapter 2

The MGE-Procedure

This chapter will deal with the mathematical interpretation of and the motivation for different sub-procedures of the MGE-procedure. The data contained at each stage in the MGE-procedure formalises certain modules over the ring S. We will highlight the connections between the different steps the procedure takes and those S-modules.

Section 2.1: We will give an outline of the input of the MGE-procedure and explain the motivation for the procedure. Similarly to the Todd-Coxeter procedure, we aim to draw conclusions about the S-module, that we want to construct, from the given set of relations of the module $\mathcal{M}$.

Section 2.2: We will introduce a new alphabet which will be used as a generating set for certain S-modules. We will introduce free S-modules Σ and give an outline how Σ and certain submodules of Σ will accompany the procedure.

Section 2.3: We will describe the definition step which is needed in order to bring relations of $\mathcal{M}$ into computable form. Moreover, we will explain the effects of such definition steps on the S-modules which are formalised at each stage by the procedure.

Section 2.4: Similarly to the Todd-Coxeter procedure, relations of the module $\mathcal{M}$ will lead to elements which must be zero in $\Theta_S \cong \mathcal{M}$, the so-called coincidences. We will introduce certain S-modules which are induced by the coincidences of the procedure. Moreover, we will describe the effect of possible torsion elements on the method of processing the coincidences in

the MGE-procedure in the case where the ring S is not a field.
Section 2.5 : We give a brief overview of the data which is stored in the MGE-procedure and which holds a description of the S-modules accompanying the procedure.

2.1 Mathematical Outline of the procedure

We again denote by $\mathcal{F} = \langle Y \rangle_A$ the free module over the free algebra $A = \langle X \rangle_S$ generated by a finite set of symbols $Y = \{y_1, \ldots, y_n\}$, and by $\mathcal{D} = \langle Y' \rangle_P$ the free n-generated module over the finitely presented S-algebra $P = \langle\, X \mid R \,\rangle$. We assume that the Euclidean domain S is an ordered ring.

From this point onwards, the input of the MGE procedure consists of a fixed P-module $\mathcal{M}$, given by the finite presentation $\mathcal{M} = \langle Y' \mid \widetilde{U} \rangle_P$. A further part of the input consists of the finite description of the algebra P by its set of generators X and its finite set of relators R.

We denote by U the set of pre-images in $\mathcal{F}$ of the set of module-relations $\widetilde{U} \in \mathcal{D}$ under the epimorphism $\phi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}$. The set of algebra-relations R are elements of the algebra A and they act on the free module $\mathcal{F}_A$. Instead of treating the relations $r \in R$ as algebra-relations we will consider them as elements of the module $\mathcal{F}$. Then the finite set R gives rise to a set of elements

$$YX^*R = \{y.wr \mid y \in Y, w \in X^*, r \in R\},$$

and as there are infinitely many words $w \in X^*$ the set YX^*R must be infinite if $R \neq \emptyset$.

As we have seen in Lemma 1.1.5, the finitely presented P-module $\mathcal{M}$ can be considered as module over the free algebra A where it has a presentation

$$\mathcal{M}_A = \langle Y \mid U \cup YX^*R \,\rangle.$$

The set $\{U \cup YX^*R\}$ generates an A-submodule of $\mathcal{F}$: we set $\mathcal{N} = \langle U \cup YX^*R \rangle$ and therefore

$$\mathcal{M}_A = \mathcal{F}/\mathcal{N}.$$

In the description of the MGE-procedure we will consider $\mathcal{M}$ mainly as module over A. Since the set of all of the relations of $\mathcal{M}_A$ will be used

often, we will abbreviate it by

$$Rels := \{U \cup YX^*R\}.$$

The module $\mathcal{N}$ is a submodule of the finitely generated A-module $\mathcal{F}$. Using an argument similar to the Schreier-Generator Theorem for groups, we showed in Section 1.2 that there must exist a finite generating set for the module $\mathcal{N}$ in the case that the quotient-module $\mathcal{M}$ is P-module isomorphic to a P-module which is finitely generated as S-module. We will show now that in this case there exists a finite subset $\widetilde{R}$ of $Rels$ such that $\mathcal{N} = \langle \widetilde{R} \rangle_A$.

Lemma 2.1.1 *Let $\mathcal{N} = \langle Rels \rangle$ be a free A-module generated by the infinite set $Rels$ and suppose that $\mathcal{N}$ is finitely generated. Then there exists a finite subset $\widetilde{R}$ of $Rels$ that generates $\mathcal{N}$.*

Proof. Let $G = \{g_1, \ldots, g_t\}$ denote the finite generating set of $\mathcal{N}$. Since G generates $\mathcal{N}$ we have that $g_j \in \mathcal{N}$ and therefore $g_j = \sum_{i \in I} r_i a_{ij}$, where $r_i \in Rels$ and $a_{ij} \in A$, for all $g_j \in G$. We define a set $I_j \subset I$ by the rule

$$I_j = \{i \in I \mid a_{ij} \neq 0\}.$$

The set I_j must be a finite set and g_j is obtained as sum over this set. Now let

$$K = \cup_{1 \leq j \leq t} I_j,$$

this is a finite union of finite sets, so K is a finite subset of I. Then the set $\widetilde{R}' := \{r_k \mid k \in K\}$ generates $\mathcal{N}$. Let $\mathcal{N}' = \langle \widetilde{R}' \rangle_S$ denote the submodule of $\mathcal{N}$ generated by $\widetilde{R}'$. Then $\mathcal{N}'$ contains g_j for each $g_j \in G$. It follows that $\mathcal{N}'$ must contain the submodule which is generated by G which by assumption is the module $\mathcal{N}$. We can conclude that $\mathcal{N}' = \mathcal{N}$. □

Therefore, if a module $\Theta \cong \mathcal{M}$ exists as described above then we will be able to find a finite set of elements $\{r_{(1)}, \ldots, r_{(\nu)}\} \subset \mathcal{F}$ such that $\mathcal{N} = \langle r_{(1)}, \ldots r_{(\nu)} \rangle_A$. This will lead to a finite ascending sequence of A-submodules

$$\mathcal{N}_{(0)} \subset \mathcal{N}_{(1)} \subset \cdots \subset \mathcal{N}_{(\nu)} = \mathcal{N}$$

where $\mathcal{N}_{(0)}$ is the zero A-module and $\mathcal{N}_{(\nu)} = \mathcal{N}$ and where we obtain the module with index (ι) from the one with index $(\iota - 1)$ by

$$\mathcal{N}_{(\iota)} = \mathcal{N}_{(\iota-1)} + \langle r_{(\iota)} \rangle_A.$$

We can form the quotient A-module $\mathcal{M}_{(\iota)} := \mathcal{F}/\mathcal{N}_{(\iota)}$, and if $\mathcal{N}_{(\nu)} = \mathcal{N}$ then certainly $\mathcal{M}_{(\nu)} = \mathcal{M}$.

We intend to find a finitely presented S-module Θ with the MGE-procedure and we demand that, after termination, all the relations of $\mathcal{M}_A$ hold when they are applied to elements of Θ. So if a finite generating set for $\mathcal{N} = \langle Rels \rangle$ exists we can actually find a finite subset of the originally infinite generating set $Rels$ such that this finite subset has the same A-linear span as the infinite set of all those relations of $\mathcal{M}$.

Since the algebra A itself is a module over S – although one with infinite generating set X^* – the A-module $\mathcal{F}$ is an S-module as well. As an A-module, $\mathcal{F}$ is generated by the set $Y = \{y_1, \ldots, y_n\}$, so an element $f \in \mathcal{F}$ is of the following form:

$$f = \sum_{i=1}^{n} \sum_{j}^{m_i} \lambda_{i,j} \cdot y_i.w_{i,j}$$

with $\lambda_{i,j} \in S$ and $w_{i,j} \in X^*$. A summand of f is a term $\lambda_{i,j} \cdot y_i.w_{i,j}$ which lies in the A-linear span of the generator y_i. However, when considered as elements of an S-module, elements such as y_i and $y_i.w_{i,j}$ are linearly independent. In a free module there cannot exist an S-linear combination such that an element $y_i.w_{i,j}$ can be expressed in terms of elements $y_l.\widetilde{w}_l \in \mathcal{F}$ if either $y_l \neq y_i$, or $\widetilde{w}_l \neq w_{i,j}$ or both are different.

Therefore, $\mathcal{F}$ considered as S-module is generated by the infinite set $\{y_i.w \mid y_i \in Y, w \in X^*\}$ and so is $\mathcal{M}$ when considered as quotient-module of $\mathcal{F}_S$ by $\mathcal{N}_S$. We however aim to construct a finitely generated S-module Θ :

$$\Theta = \Gamma/\Phi,$$

where Γ denotes a free S-module, finitely generated by a set $b_1, \ldots, b_t$, and where we factor out a submodule $\Phi \subset \Gamma$ which is generated by the finite set of elements $\lambda_i \cdot b_i$ for torsion-elements $b_{i_1}, \ldots, b_{i_m}$ of Θ with the respective exponents $\lambda_{i_1}, \ldots, \lambda_{i_m}$.

Remark 2.1.2 *In the MGE-computation as it has been implemented in GAP we do not necessarily obtain elements of the form $\lambda_i \cdot b_i$ but instead we might obtain elements such as $v = \sum_{j=1}^{k} \lambda_j \cdot b_j$ where the coefficients are not units of S and where b_j for $1 \leq j \leq k$ are torsion-elements of Θ. By applying a Smith normal form computation a generating set could be obtained such that all generators of Φ are of the form $\lambda_i \cdot b_i$. Then however we would lose information about which elements of $\mathcal{F}$ gave rise to generators $b \in \mathcal{B}$ of Θ.*

Since the MGE-procedure follows the idea of the Todd-Coxeter procedure we intend to derive information about the S-module Θ by examining a finite subset of the relations $r \in Rels$. We construct the basis of the free module Γ progressively as we consider the relations and we also want to deduce information about torsion possibly arising from these relations. To see when a new basis element is needed we need some terminology and introduce the following:

Definition 2.1.3 *Let $w = x_1 \dots x_l$ denote a word in the free and finitely generated monoid X^*. We call a word $w' = x_1 \dots x_{l-j} \in X^*$ a* **prefix** *of w if there exists $w'' \in X^*$ such that $w'w'' = w$. The word w'' is called a* **suffix** *of w if w has a prefix w' and $w'w'' = w$.*

In a similar way we define a prefix of an element g of a module $\mathcal{G}$. Let an element g be of the form:

$$g = \sum_{i=1}^{n} \sum_{k=1}^{m} \lambda_{ik} \cdot y_i.w_{ik} \qquad \text{with } \lambda_{ik} \in S, y_i \in Y \text{ and } w_{ik} \in X^*.$$

Then for every summand $\lambda_{ik} \cdot y_i.w_{ik}$ of g we call an element $y_i.w'$ **a prefix of** *g* **at** *$\lambda_{ik} \cdot y_i.w_{ik}$ if there exists a word $w'' \in X^*$ such that $w'w'' = w_{ik}$ from which*

$$y_i.w'w'' = y_i.w_{ik}$$

follows. When we want to emphasize that a prefix p is a prefix of an element $g \in \mathcal{G}$ we will denote this by $p]g$. We define the **suffix** *of $g \in \mathcal{G}$ similarly. A prefix will be called a* **proper prefix** *if $w'' \neq \varepsilon$ both in the case of elements of a monoid as well as for the elements of a module.*

The relations in *Rels* give rise to congruence classes of elements of $\mathcal{F}_S$ and there may (or may not) be a finite subset in the set *Rels* which will give rise to a finite set of S-module generators for a module Γ. Such a finitely generated module Γ does not necessarily exist as can be seen for instance in the following example:

Example 2.1.4 *Let* $P = \langle x_1, x_2 \mid x_1x_2x_1 + x_1 \rangle_S$ *and let* $\mathcal{M} = \langle y \mid y.x_1^2 - y \rangle_P$. *Since there are no relations involving the algebra-generator* x_2 *acting on* y *there is an infinite set* $y.x_2, y.x_2^2, y.x_2x_1x_2, y.x_2^3 \ldots$ *of elements of* $\mathcal{M}$ *which are* S*-linear independent with respect to each other. It follows that there cannot exist a finitely generated* S*-module* Γ *of which an* S*-module* Θ_S *isomorphic to* $\mathcal{M}$ *could be a quotient-module.*

If a nonzero finite subset of the set of relations however exists which S-linearly spans all relations we can conclude that $\mathcal{M}$ is P-module isomorphic to a finitely presented S-module Θ as for instance in the next example:

Example 2.1.5 *Let* $P = \langle x_1, x_2 \mid x_1x_2x_1 + x_1, x_2^2 - 1 \rangle_S$ *and let* $\mathcal{M} = \langle y \mid y.x_1^2 - y \rangle_P$. *Then the relations give rise to the infinite set of congruence classes* $\lambda \cdot y + \mathcal{N}$, $\lambda \cdot y.x_1 + \mathcal{N}$, $\lambda \cdot y.x_1x_2 + \mathcal{N}$, $\lambda \cdot y.x_2 + \mathcal{N}$ *and* $\lambda \cdot y.x_2.x_1 + \mathcal{N}$, *where* $\lambda \in S$. *Only these five different types of infinite sets of congruence classes are necessary.*

From these five infinite sets of classes it suffices to choose the set of classes $\{1 \cdot y + \mathcal{N}, 1 \cdot y.x_1 + \mathcal{N}, 1 \cdot y.x_1x_2 + \mathcal{N}, 1 \cdot y.x_2 + \mathcal{N}, 1 \cdot y.x_2x_1 + \mathcal{N}\}$ *since the elements of classes with coefficients* $\lambda \neq 1$ *lie in the* S*-linear span of this set.*

The motivation for the MGE-procedure comes from the following: Let y_i and $y_i.w, w \neq \varepsilon$, denote elements of $\mathcal{F}$. Then $y_i.w$ does not lie in the S-linear span of y_i. For elements $r \in Rels \subset \mathcal{F}$, such an element r naturally lies in $\mathcal{N} = \langle Rels \rangle_A$, but its proper prefixes may lie in congruence classes outside $\mathcal{N}$. These classes will be of special interest to us. In order to deal with them we introduce a series of alphabets $B_{(\iota)}$, with $0 \leq \iota \leq \nu$, and also a set of S-modules, denoted $\Sigma_{(\iota)_j}$, which we will describe now.

2.2 S-modules $\Sigma_{(\iota)_j}$

Following the idea of Todd and Coxeter we want to draw conclusions about the set of generators of the S-module Θ from the set of relations $Rels$ of $\mathcal{M}$. As module over the free algebra A we have that $\mathcal{M}_A = \mathcal{F}/\mathcal{N}$, where $\mathcal{N} = \langle Rels \rangle_A$, and we have seen that there exists a finite generating set for $\mathcal{N}_A$ if $\mathcal{M}$ is isomorphic to a finitely generated S-module. In this case there exists a finite subset $\{r_{(1)}, \ldots, r_{(\nu)}\} \subset Rels$ generating $\mathcal{N}$ which gives rise to an ascending, finite chain of A-modules

$$\mathcal{N}_{(1)} \subset \cdots \subset \mathcal{N}_{(\nu)} = \mathcal{N}$$

such that $\mathcal{N}_{(\iota)} := \langle r_{(1)}, \ldots, r_{(\iota)} \rangle$ for $1 \leq \iota \leq \nu$. To each such module $\mathcal{N}_{(\iota)}$ we will assign a sequence of free S-modules $\Sigma_{(\iota)_0} \subset \cdots \Sigma_{(\iota)_j} \subset \cdots \Sigma_{(\iota)_{t(\iota)}}$. The generating set of a module $\Sigma_{(\iota)_j}$, for $0 \leq j \leq t(\iota)$, depends in particular on the set of generators of the module $\mathcal{N}_{(\iota)}$ and also on the prefixes of these generators. Moreover we will construct certain submodules $\Xi_{(\iota)_j}$ and $\Upsilon_{(\iota)_j}$ of $\Sigma_{(\iota)_j}$ which are induced by the generators $r_{(1)}, \ldots, r_{(\iota)}$ of $\mathcal{N}_{(\iota)}$. We will also explain the technique with which we bring relations $r_{(1)}, \ldots, r_{(\iota)}$ into a computable form. We will now explain in detail how the S-modules $\Sigma_{(\iota)_j}$ are found and how they are connected to a module $\mathcal{N}_{(\iota)}$.

We will start by introducing a new alphabet which will be used for bookkeeping reasons: Let $\mathcal{B} = \{b_1, b_2, \ldots\}$ denote an infinite, countable set in bijection to the set of natural numbers $\mathbb{N}$. We can consider $\mathcal{B}$ as the pool from which we draw possible S-module generators for the construction of Θ. The elements of $\mathcal{B}$ are ordered by their indices. In the first step, we assign to every module generator $y_i \in Y$ of $\mathcal{F}$ an element $b_i \in \mathcal{B}$. Compared to the Todd-Coxeter procedure this corresponds to allocating the coset with the number 1 to the coset of the subgroup whose index we will want to compute. However, since $\mathcal{M}$ is not necessarily a quotient-module of a cyclic module we might have to allocate more than one S-module generator from the set $\mathcal{B}$, namely n, the number of generators of $\mathcal{M}$.

We shall describe this process of allocating an element from $\mathcal{B}$ to certain elements of $\mathcal{F}$ of the form $y_i.w$ by defining a set of maps $\rho_{(\iota)_k}$ for

$0 \leq \iota \leq \nu$ and $k \in \{0, \ldots, t_\iota\}$. These maps have as domain a certain (finite) subset of elements of $\mathcal{F}$ and as codomain a (finite) subset of $\mathcal{B}$. The first step in which we allocate a subset of $\{b_1, \ldots, b_n\} \subset \mathcal{B}$ to each of the generators $y_i \in Y$ leads to the set $B_{(0)} := \{b_i \in \mathcal{B} \mid b_i := \rho_{(0)_0}(y_i)\}$. Hence $\rho_{(0)_0} : \{y_1, \ldots, y_n\} \longrightarrow B_{(0)}$ provides a bijection between the set of module generators of $\mathcal{M}_A$ and the set $B_{(0)}$.

Notation 2.2.1 *We will use indices enclosed in brackets in order to describe to which submodule $\mathcal{N}_{(\iota)}$ a "tool" (such as for instance a mapping such as $\rho_{(0)_0}$) belongs to. Moreover, to each $\mathcal{N}_{(\iota)}$ there will be a set of tools such as modules $\Sigma_{(\iota)_j}, \Sigma_{(\iota)_{j+1}}, \ldots$ and mappings $\rho_{(\iota)_j}, \rho_{(\iota)_{j+1}}, \ldots$ belonging to it which will be denoted by an additional index for the index (ι). Since the tools with index $(\iota)_0$, for all $1 \leq \iota \leq \nu$ have a distinguished role in the procedure, we will omit this index 0. Whereas a module $\Sigma_{(\iota)_0}$ corresponds directly to $\mathcal{N}_{(\iota)}$, modules $\Sigma_{(\iota)_j}$ with $j \neq 0$ which are also associated to $\mathcal{N}_{(\iota)}$ can be understood as "stepping stones" towards obtaining a module $\Sigma_{(\iota+1)_0}$ which then will be a tool corresponding to $\mathcal{N}_{(\iota+1)}$.*

We will use the set $B_{(0)}$ as generating set for the free S-module $\langle B_{(0)} \rangle_S$ and we moreover define

$$\Sigma_{(0)} := \langle B_{(0)} X^* \rangle_S,$$

as the free and infinitely generated S-module with generating set $B_{(0)}X^* = \{b.w \mid b \in B_{(0)}, w \in X^*\}$. It follows from the construction of $\Sigma_{(0)}$ that it can be provided with an A-module structure: the multiplication of generators of A on elements of $\Sigma_{(0)}$ is given by the free concatenation $(v, x) \longmapsto v.x$ of $v \in \Sigma_{(0)}$ and $x \in X$. We extend $\rho_{(0)}$ to all generators of $\mathcal{F}_S$ where we set

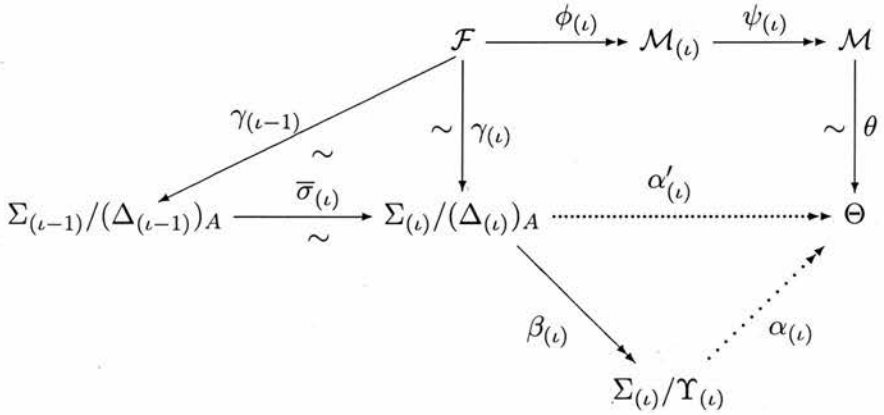
$$\rho_{(0)}(y_i.w) := \rho_{(0)}(y_i).w.$$

Moreover we define $\gamma_{(0)} : \mathcal{F} \longrightarrow \Sigma_{(0)}$ as the S-linear extension of $\rho_{(0)}$ which indeed yields an A-module isomorphism of $\mathcal{F}$ and $\Sigma_{(0)}$.

Remark 2.2.2 *The S-modules we are working with are induced by A-modules, therefore situations occur where we have to consider the A-module*

closure instead of the S-module itself. We will not provide every such module with a new name although we will make an exception with the module $\Upsilon_{(\iota)}$ which will be introduced in the next section. Instead, we will generally denote the A-module closure of for instance a module Ω_S by $(\Omega)_A$.

So far we have described in detail only the module $\Sigma_{(0)}$ but generally for all $0 \leq \iota \leq \nu$ we aim to construct S-modules $\Sigma_{(\iota)}, \Delta_{(\iota)}$ and $\Upsilon_{(\iota)}$ such that they give rise to a commutative diagram:



where $\mathcal{M}_{(\iota)} = \mathcal{F}/\mathcal{N}_{(\iota)}$ and where accordingly $\phi_{(\iota)} : \mathcal{F} \twoheadrightarrow \mathcal{M}_{(\iota)}$ and $\psi_{(\iota)} : \mathcal{M}_{(\iota)} \twoheadrightarrow \mathcal{M}$ are the canonical quotient maps with kernels $\mathcal{N}_{(\iota)}$ and $\mathcal{N}/\mathcal{N}_{(\iota)}$ respectively. We will show that, in the case when $\mathcal{M}$ is P-module isomorphic to a finitely generated S-module Θ, there exists (ν) such that $\Theta_{(\nu)} := \Sigma_{(\nu)}/\Upsilon_{(\nu)}$ is isomorphic as P-module to $\mathcal{M}$ and the MGE-procedure will reach termination.

With this in mind we aim to progressively build up certain submodules $\Upsilon_{(\iota)}$ such that $\Upsilon_{(\iota)} \subset \Upsilon_{(\iota+1)}$. We want to ensure, at all stages of the MGE-procedure, that there exist A-module-homomorphisms $\alpha_{(\iota)} : \Sigma_{(\iota)}/\Upsilon_{(\iota)} \longrightarrow \Theta$ and $\alpha'_{(\iota)} : \Sigma_{(\iota)}/\Delta_{(\iota)} \longrightarrow \Theta$ such that the diagram above commutes. Then if $\mathcal{M}$ is P-module-isomorphic to a finitely generated S-module $\Theta_{(\nu)}$ we will show that $\alpha_{(\nu)}$ gives a P-module isomorphism between $\Theta_{(\nu)} = \Sigma_{(\nu)}/\Upsilon_{(\nu)}$ and $\mathcal{M}$. If $(\iota) = 0$ then the modules $\mathcal{N}_{(0)}$ and $\Upsilon_{(0)_0}$ are trivial, and we define

$$\alpha'_{(0)} = \alpha_{(0)} := \theta \circ \psi_{(0)} \circ \phi_{(0)} \circ \gamma_{(0)}^{-1}.$$

Remark 2.2.3 *From now on we will say that* $(\iota)_j < (\iota')_{j'}$ *if either*

1. $(\iota) < (\iota')$, *or*
2. $(\iota) = (\iota')$ *and* $j < j'$

holds.

In the following section we will explain how to obtain maps and S-modules for $(\iota)_j \neq (0)_0$ and we will introduce the required terminology.

2.3 Definition Step and S-modules $\Delta_{(\iota)_j} \subset \Sigma_{(\iota)_j}$

Let $\mathcal{N}_{(\iota)} = \langle r_{(1)}, \ldots, r_{(\iota)} \rangle_S$ and suppose that we are investigating a relation $r \in Rels \backslash \{r_{(1)}, \ldots, r_{(\iota)}\}$ at the current stage of the MGE-procedure. In order to be able to draw conclusions about the S-module Θ we want to form a map $\rho_{(\iota)_t}$ which maps all the prefixes of r to elements of a module $\langle B_{(\iota)_t} \rangle_S, t \geq 0$. Note that here the second index t depends on the relation r, its set of prefixes, and also on the prefixes of the previously investigated relations $r_{(1)}, \ldots, r_{(\iota)}$. Suppose we are given at this stage the set $B_{(\iota)_j}, 0 \leq j \leq t-1$, as a set of generators such that there is at least one prefix p of r that is not mapped to $\langle B_{(\iota)_j} \rangle_S$ by the mapping $\rho_{(\iota)_j}$. Then when we detect $p]r$ we will extend the given generating set and we obtain a set $B_{(\iota)_{j+1}} \supset B_{(\iota)_j}$. Accordingly, we define a mapping $\rho_{(\iota)_{j+1}}$ extending the range of those elements $y.w \in \mathcal{F}$ which get mapped to the (new) set $B_{(\iota)_{j+1}}$ of possible S-module generators.

Definition 2.3.1 *Let* $f_1 \in \mathcal{F}$ *and suppose that there exists* $f_2 \in \mathcal{F}$ *such that* f_1 *is congruent modulo* $\mathcal{N}_{(\iota)}$ *to* f_2 *and that* f_2 *gets mapped by* $\rho_{(\iota)_j}$ *to an element* $v := \rho_{(\iota)_j}(f_2)$ *such that* $v \in \langle B_{(\iota)_j} \rangle$. *We then say that* f_1 *is* **reachable modulo** $\mathcal{N}_{(\iota)}$ **with** $\rho_{(\iota)_j}$.

Example 2.3.2 *Let* $(\iota)_j = (0)_0$. *Each of the* A*-module generators in* $Y = \{y_1, \ldots, y_n\}$ *of* $\mathcal{F}$ *is reachable by* $\rho_{(0)_0}$. *Every element of* $\mathcal{F}$ *of the form* $y_i.w$, *where* $w \neq \varepsilon$, *however gets mapped to* $\rho_{(0)_0}(y_i.w) = b_i.w \in \Sigma_{(0)_0} \backslash \langle B_{(0)} \rangle$ *and, since* $\mathcal{N}_{(0)}$ *is zero, cannot be reachable with* $\rho_{(0)_0}$.

We assume now that each of the prefixes of the relation r is reachable modulo $\mathcal{N}_{(\iota)}$ with $\rho_{(\iota)_{j+1}}$, so that $j+1=t$ for t as above. We also assume that we have stored all possibly occurring congruences of prefixes of r to S-linear combinations of prefixes of relations which have been examined at an earlier point. If these conditions are satisfied we will use the relation $r \in Rels$ as an additional generator and we form

$$\mathcal{N}_{(\iota+1)} := \mathcal{N}_{(\iota)} \cup \langle r \rangle_A.$$

Let $r \in Rels \backslash \{r_{(1)}, \ldots, r_{(\iota)}\}$. Whenever we find that a prefix $p]r$ is not known to be reachable with $\rho_{(\iota)_k}$ modulo $\mathcal{N}_{(\iota)}$ we conclude, from the knowledge we have at that point of the computation, that $p]r$ may give rise to a new S-module generator for Θ. If, in the process of examining the relation r, we have encountered prefixes $p_{i_1}, \ldots, p_{i_t}$ such that $p_{i_j}]r, 1 \leq j \leq t$, had not been reachable with the given maps $\rho_{(\iota)_{j-1}}$ we have to add t elements to the set $B_{(\iota)_0}$ in order to make each of the prefixes reachable: every time an element $b' \in \mathcal{B} \backslash B_{(\iota)_{j-1}}$ is assigned to an element $p_{i_j}]r \in \mathcal{F}$ we set $B_{(\iota)_j} := B_{(\iota)_{j-1}} \cup \{b'\}$ and accordingly

$$\Sigma_{(\iota)_j} := \langle B_{(\iota)_j} X^* \rangle_S.$$

This process of allocating an S-module generator from the set $\mathcal{B} \backslash B_{(\iota)_j}$ is called a **Definition Step**. We can embed $\Sigma_{(\iota)_j}$ into $\Sigma_{(\iota)_{j+1}}$ and, more generally, we can define an embedding

$$emb_{(\iota)_j}^{(\kappa)_l} : \Sigma_{(\iota)_j} \hookrightarrow \Sigma_{(\kappa)_l}$$

for $(\iota)_j \leq (\kappa)_l$. Whenever we pursue a definition step for a prefix $p]r$, we define a mapping $\rho_{(\iota)_{j+1}}$ by $\rho_{(\iota)_{j+1}}(p) := b'$. We set $\rho_{(\iota)_{j+1}}(y.w) = \rho_{(\iota)_j}(y.w)$ for all $y.w \in \mathcal{F}$ which were reachable already by $\rho_{(\iota)_j}$. We again A-linearly extend the domain whenever it is necessary: this again yields a mapping which has as domain the module $\mathcal{F}$. Therefore every $f \in \mathcal{F}$ which is congruent modulo $\mathcal{N}_{(\iota)}$ to the prefix $p]r$ now becomes reachable by the new mapping $\rho_{(\iota)_{j+1}}$.

Now suppose that, for elements of $\mathcal{F}$, $p_k.x = p$ and moreover that $\rho_{(\iota)_j}(p_k) = b''$. Then

$$emb_{(\iota)_j}^{(\iota)_{j+1}}\left(\rho_{(\iota)_j}(p_k.x)\right) = emb_{(\iota)_j}^{(\iota)_{j+1}}\left(\rho_{(\iota)_j}(p_k)\right).x = b''.x$$

but on the other hand $\rho_{(\iota)_{j+1}}(p_k.x) = \rho_{(\iota)_j}(p) = b'$. We obtain a congruence relation of elements of $v', v'' \in \Sigma_{(\iota)_{j+1}}$, namely that $v' \sim v''$, if the following two conditions are satisfied:

1. there exist elements $b', b'' \in \langle B_{(\iota)_{j+1}} \rangle$ and a word $w \in X^*$ such that $v' = b'.w$ and $v'' = b''.w$;

2. There exists an index "$(\iota)_j$" such that $emb_{(\iota)_j}^{(\iota)_{j+1}}(\rho_{(\iota)_j}(p_k.x)) = b''.x$ but where also $\rho_{(\iota)_{j+1}}(p_k.x) = b'$ for $p_k \in \mathcal{F}$ and $x \in X$.

This leads to the definition of a submodule of $\Sigma_{(\iota)_j}$: We denote by

$$\Delta_{(\iota)_j} := \langle b_1.x - b'_1, \ldots, b_j.x - b'_j \rangle_S$$

that S-submodule of $\Sigma_{(\iota)_j}$ that is generated by the set of all the elements $(b.x - b') \in \Sigma_{(\iota)_j}$ where a Definition Step became necessary in order to make an element $y.wx \in \mathcal{F}$ reachable by some map ρ. Note that the generating set of $\Delta_{(\iota)_j}$ also includes all those elements $(b.x - b')$ which are induced by definition steps for prefixes of $r_{(\kappa)}$ with $\kappa < \iota$. Then whenever $\rho_{(\kappa)_i}(y.w) = b$ and $\rho_{(\kappa)_i}(y.wx) = b.x$ and where a definition step then leads to the $\rho_{(\kappa)_{i+1}} = b'$ for $(\kappa)_i < (\iota)_k$ an element $b.x - b'$ had been added to the generating set of $\Delta_{(\iota)_j}$.

Example 2.3.3 *Let* $P = \langle x_1, x_2 \mid x_1x_2x_1 + x_1, x_2^2 - 1 \rangle_{\mathbb{Z}}$ *and let* $\mathcal{M} = \langle y_1, y_2 \mid y_2.x_1^2 - y_2 \rangle_P$. *Then* $B_{(0)} = \{b_1, b_2\}$. *If we choose* $y_2.x_1^2 - y_2$ *as the first relation to investigate then this leads to* $b_3 = \rho_{(0)_1}(y_2.x_1)$ *and* $b_4 = \rho_{(0)_2}(y_2.x_1^2)$ *and accordingly* $B_{(1)} = \{b_1, b_2, b_3, b_4\}$. *By* $\rho_{(0)_0}$ *we have* $\rho_{(0)_0}(y_2.x_1) = b_2.x_1$, *by* $\rho_{(0)_1}$ *we however have* $\rho_{(0)_1}(y_2.x_1) = b_3$. *Similarly we have* $\rho_{(0)_1}(y_2.x_1^2) = b_3.x_1$ *and* $\rho_{(0)_2}(y_2.x_1^2) = b_4$. *Accordingly we define* $\Delta_{(0)_1} = \langle b_2.x_1 - b_3 \rangle_{\mathbb{Z}}$ *and* $\Delta_{(0)_2} = \langle b_2.x_1 - b_3, b_3.x_1 - b_4 \rangle_{\mathbb{Z}}$.

Since we always consider the effect of such a definition step for an A-module we are mainly interested in this case in the congruence of elements generated by the A-closure of $\Delta_{(\iota)_j}$. Accordingly, we will define by $\pi : \Sigma_{(\iota)_j} \twoheadrightarrow \Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A$ the canonical quotient-map mapping to the quotient-module by the A-module closure of $\Delta_{(\iota)_j}$.

It follows that a definition step for a pair $b \in B_{(\iota)_j}, x \in X$ corresponds to an A-module isomorphism

$$\sigma_{(\iota)_{j+1}} : \Sigma_{(\iota)_j} \longrightarrow \Sigma_{(\iota)_{j+1}}/\langle b.x - b' \rangle_A$$

where $b.x \overset{\sigma_{(\iota)_{j+1}}}{\longmapsto} b'$ and where all those elements $v \in \Sigma_{(\iota)_j}$ of which $b.x$ is not a prefix get mapped to $emb_{(\iota)_j}^{(\iota)_{j+1}}(v)$ and accordingly concatenation of maps yields an isomorphism

$$\Sigma_{(0)_0} \underset{\cong}{\overset{\overline{\sigma}_{(\iota)_{j-1}} \circ \cdots \circ \sigma_{(0)_1}}{\longrightarrow}} \Sigma_{(\iota)_{j-1}}/(\Delta_{(\iota)_{j-1}})_A \underset{\cong}{\overset{\overline{\sigma}_{(\iota)_j}}{\longrightarrow}} \Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A,$$

where $\overline{\sigma}_{(\iota)_{j+1}} : \Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A \longrightarrow \Sigma_{(\iota)_{j+1}}/(\Delta_{(\iota)_{j+1}})_A$ is induced by $\sigma_{(\iota)_{j+1}}$.

Again we denote by $\gamma_{(\iota)_j}$ the S-linear extension of $\rho_{(\iota)_j}$; the homomorphism $\gamma_{(\iota)_j} : \mathcal{F} \longrightarrow \Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A$ is equal to the composition $\gamma_{(\iota)_j} = \sigma_{(\iota)_j} \circ \cdots \circ \sigma_{(0)_1} \circ \gamma_{(0)_0}$ and it follows that $\gamma_{(\iota)_j}$ provides an A-module isomorphism of $\mathcal{F}$ and $\Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A$ for all $(0)_0 \leq (\iota)_j \leq (\nu)_0$.

Remark 2.3.4 *In order to ensure termination of the MGE-procedure we will follow the following rule: we want to make sure that whenever we make a new assignment at a stage $(\iota)_j$ with an element $b' \in \mathcal{B} \backslash B_{(\iota)_j}$ that then*

$$b' > max\{b \in B_{(\iota)_j}\}.$$

Hence we demand that the index of b' is greater than the index of each of the earlier defined S-generators. In particular if we are given prefixes p_k and p_{k+1} such that $p_k.x = p_{k+1}$ and where $\rho_{(\iota)_j}(p_k]r) = b'$ and $\rho_{(\iota)_j}(p_{k+1}]r) = b''$ it then follows that $b' < b''$.

Definition 2.3.5 *Let $v \in \Sigma_{(\iota)_j}$ and suppose there is at least one prefix $p]v$ such that $p \notin \langle B_{(\iota)_j} \rangle_S$. We will call the gradual procedure of assigning an element $b' = \overline{\sigma}_{(\iota)_{j+1}}(p)$ to every prefix of v the* **tracing** *of the element v.*

Remark 2.3.6 *By abuse of notation we will speak of the tracing of elements of $\Sigma/(\Delta)_A$ as well as of elements of $v \in \Sigma$.*

The S-module $\langle B_{(\iota)_j}\rangle_S$ denotes a finitely generated submodule of $\Sigma_{(\iota)_j}$ for all $0 \leq \iota \leq \nu$ and $0 \leq j \leq t(\iota)$. When we assign S-module generators from the infinite set $\mathcal{B}$ to the prefixes of a relation r, we aim for all prefixes, and in particular for the element r itself, to become reachable with a map $\rho_{(\iota)_j}$ for some $j \leq t(\iota)$. After enough definition steps have taken place we will eventually obtain an image under $\gamma_{(\iota)_{t(\iota)}}$ for r which is contained in $\langle B_{(\iota)_{t(\iota)}}\rangle_S$. Since $r \in \mathcal{F}$ is a relation for $\mathcal{M}$ we can deduce that $\gamma_{(\iota)_{t(\iota)}}(r)$ must be contained in the kernel of a mapping of $\Sigma_{(\iota)}/(\Delta_{(\iota)})_A$ mapping to an S-module Θ isomorphic to $\mathcal{M}$. We aim to form an S-module $\Upsilon_{(\iota)}$ which has a generating set containing elements which are induced by elements such as $\gamma_{(\iota)_{t(\iota)}}(r)$. We aim to construct Θ as the quotient-module of some $\Sigma_{(\nu)}$ by some $\Upsilon_{(\nu)}$. We will introduce the terminology needed in the following section.

2.4 Coincidences

2.4.1 Coincidences as Generators of S-modules

Let $r \in Rels$ denote the relation that gets examined at the current stage of the procedure and suppose that we have examined relations $r_{(1)}, \ldots, r_{(\iota)}$ beforehand which gave rise to the module $\mathcal{N}_{(\iota)} \subset \mathcal{F}$. We aim to set $\mathcal{N}_{(\iota+1)} := \mathcal{N}_{(\iota)} \cup \langle r\rangle_A$ and in order to do so we have to ensure that all prefixes of r have been made reachable. We can achieve this by the definition procedure of the previous section which yields a generating set $B_{(\iota)_{t(\iota)}}$.

In order to extend the submodule by adding r to the set of generators for constructing a module $\mathcal{N}_{(\iota+1)}$, certain conditions are needed. Firstly we demand that enough definition steps have been made such that all prefixes of r, including r itself, are reachable with $\rho_{(\iota)_{t(\iota)}}$ so that the image of r under $\gamma_{(\iota)_{t(\iota)}}$ is contained in $\langle B_{(\iota)_{t(\iota)}}\rangle_S$.

Now let $v_r := \gamma_{(\iota)_{t(\iota)}}(r)$. Then $v_r = \sum_{i=1}^{m} \lambda_i \cdot b_i$, for $\lambda_i \in S$ and $b_i \in B_{(\iota)_{t(\iota)}}$. Supposing that the map $\alpha'_{(\iota)_{t(\iota)}} : \Sigma_{(\iota)_{t(\iota)}}/(\Delta_{(\iota)_{t(\iota)}})_A \longrightarrow\!\!\!\!\!\rightarrow \Theta$ exists as described in the commutative diagram on page 25, then as the element r acts trivially on $\mathcal{M}$, we can conclude that v_r must lie in the kernel of the map $\alpha'_{(\iota)_{t(\iota)}}$. We will call an element such as v_r a **coincidence**. Additionally to

$\gamma_{(\iota)_{t(\iota)}}(r) \in \langle B_{(\iota)_{t(\iota)}} \rangle_S$ we demand that the knowledge about every coincidence gets stored in order for it to get applied to other reachable elements. When these two conditions are met then we may add the relation r to the set of generators and we define $\mathcal{N}_{(\iota+1)} = \mathcal{N}_{(\iota)} + \langle r \rangle_A$. Furthermore we set $\Sigma_{(\iota+1)_0} := \Sigma_{(\iota)_{t(\iota)}}$ and, if r is not contained in the S-linear span of the previous relations $r_{(1)}, \ldots, r_{(\iota)}$, then the coincidence will lead to a non-trivial additional generator of a certain submodule of $\Sigma_{(\iota+1)_0}$, extending the submodule that we will need to factor out in order to obtain an S-module isomorphic to $\mathcal{M}$.

In the following, we will distinguish between two kinds of coincidences. Depending on the type, the MGE-procedure will handle them in different ways. In order to describe the way we distinguish between these we need the following definition:

Definition 2.4.1 *Let B be a finite ordered set with elements $b_1, \ldots b_m$ ordered by their index and let $\langle B \rangle_S$ denote the free S-module generated by the set B. An element $v \in \langle B \rangle$ then is of the form $v = \sum_{i=1}^{k} \lambda_i \cdot b_i$ where $k \leq m$ where we suppose that $\lambda_i \neq 0$ for all $1 \leq i \leq k$.*

- *We define the* **head monomial** *of v as the generator $b_k \in B$ and we will denote the head monomial by $HM(v)$.*
- *We define the term $\lambda_k \cdot b_k$ as the* **head term** *of v which we will denote by $HT(v)$.*
- *We will call the coefficient λ_k of b_k in v the* **head coefficient** *of v and we will denote this by $HC(v)$.*

Correspondingly, we want to denote by $RED(v)$ the **reduct** *of v where*

$$RED(v) := HT(v) - v.$$

Remark 2.4.2 *Since the head monomial of an element $v \in \langle B_{(\iota)_k} \rangle$ only consists of a single generator $b \in B_{(\iota)_k}$ it actually would be more appropriate to call this specific element a "head generator". However, since we will extend the ordering on elements of $\langle B_{(\iota)_k} \rangle$ to an ordering of the elements*

$v \in \Sigma_{(\iota)_k}$ we will then also have to deal with elements of the form $b.w$, where $w \in X^*\backslash\varepsilon$, as possible head monomials of an element v. In order to remain consistent with the used terminology we will therefore call an element $b \in B_{(\iota)_k}$ with $b = HM(v)$ of $v \in \langle B_{(\iota)_k}\rangle$ a "head monomial" as well.

Mathematically, coincidences can be seen as generating a submodule of $\Sigma_{(\iota)}/(\Delta_{(\iota)})_A$. We will denote this module by $\Omega_{(\iota)}$, and since $\gamma_{(\iota)}$ provides an A-module isomorphism of $\mathcal{F}$ and $\Sigma_{(\iota)}/(\Delta_{(\iota)})_A$ it follows that

$$(\Omega_{(\iota)})_A = \langle \gamma_{(\iota)}(r_{(1)})), \gamma_{(\iota)}(r_{(2)})), \ldots, \gamma_{(\iota)}(r_{(\iota)}))\rangle_A$$

is isomorphic to $\mathcal{N}_{(\iota)} = \langle r_{(1)} \ldots, r_{(\iota)}\rangle_A$. Note that, as $\gamma_{(\kappa)}(r_{(\kappa)}) \in \langle B\rangle_S$ for all $1 \leq \kappa \leq \iota$, it follows that $\gamma_{(\kappa)}(r_{(\kappa)}) = \gamma_{(\iota)}(r_{(\kappa)})$.

In order to obtain a P-module that is finitely generated as S-module and that is P-module isomorphic to $\mathcal{M}$ we would have to factor out the A-closure of $\Omega_{(\iota)}$ from $\Sigma_{(\iota)}/(\Delta_{(\iota)})_A$. Taking the A-closure of Ω is necessary as the coincidences are induced by the relations of an A-module. We will show now that instead of factoring out the submodule $(\Omega)_A$ from $\Sigma/(\Delta)_A$, we can form a quotient-module of Σ by a certain submodule Υ instead:

Lemma 2.4.3 *There is an S-module $\Upsilon \subset \Sigma$ such that*

$$\Sigma/\Upsilon \cong (\Sigma/(\Delta)_A)/(\Omega)_A.$$

Proof. By the Correspondence Theorem there is a bijection between the submodules of $\Sigma/(\Delta)_A$ and those submodules of Σ which contain $(\Delta)_A$. Thus there exists

$$\Upsilon := \{v \in \Sigma \mid v + (\Delta)_A \in (\Omega)_A\},$$

and therefore $\Upsilon/(\Delta)_A = (\Omega)_A$. It follows then from the Isomorphism Theorem that $(\Sigma/(\Delta)_A)/(\Omega)_A = (\Sigma/(\Delta)_A)/(\Upsilon/(\Delta)_A) \cong \Sigma/\Upsilon$.

Now let $\{c_1, \ldots, c_m\}$ denote the generating set of $(\Omega)_A$. Then for every c_i there is $k_i \in \Sigma$ such that $c_i = k_i + (\Delta)_A$; we furthermore denote by $\{h_1, \ldots, h_t\}$ the generating set of $(\Delta)_A$. Then the set $\{k_1, \ldots, k_m, h_1, \ldots, h_t\}$ generates Υ : as $k_i + (\Delta)_A = c_i \in (\Omega)_A$ and also $h_i + (\Delta)_A = 0 + (\Delta)_A \in (\Omega)_A$ it follows that $\langle k_1, \ldots, k_m, h_1, \ldots, h_t\rangle \subset \Upsilon$.

On the other hand let $v \in \Upsilon$, then $v + (\Delta)_A \in (\Omega)_A$ and accordingly $v + (\Delta)_A = \sum_{i=1}^{m} c_i.a_i = \sum_{i=1}^{m} \big(k_i + (\Delta)_A\big).a_i = \sum_{i=1}^{m} k_i.a_i + (\Delta)_A$ where $a_i \in A$. It follows that $v - \sum_{i=1}^{m} k_i.a_i \in (\Delta)_A$ and $v - \sum_{i=1}^{m} k_i.a_i = \sum_{j=1}^{t} h_j.a'_j$. Therefore, $v = \sum_{i=1}^{m} k_i.a_i + \sum_{j=1}^{t} h_j.a'_j$ and we can conclude that $v \in \langle k_1, \ldots, k_m, h_1, \ldots, h_t \rangle_A$ which shows the demanded equality of modules. □

Therefore, instead of working with a coincidence $c \in \Sigma/(\Delta)_A$, we can choose an element $k \in \Sigma$ such that $k + (\Delta)_A = c$. Such a choice is not unique, but we will see later that there are certain conditions which will enable us to make a choice in a unique way.

If we denote by K the set of elements of Σ induced by the set of coincidences in $\Sigma/(\Delta)_A$ then the elements of K, together with the elements $b.x - b'$ which are induced by the definition steps, give rise to a submodule Υ. We will form the quotient-module $\Theta_{(\iota)} := \Sigma_{(\iota)}/\Upsilon_{(\iota)}$ in order to eventually obtain some stage (ν) such that $\Theta_{(\nu)} \cong \mathcal{M}$.

By assumption, a finitely generated S-module Θ, which is isomorphic to $\mathcal{M}$, exists, so there must exist an index (ν) such that $\mathcal{N} = \mathcal{N}_{(\nu)}$. We will show that $\Theta_{(\nu)}$ is isomorphic to Θ.

Proposition 2.4.4 *Let ν such that $\mathcal{N}_{(\nu)} = \mathcal{N}$. Then the module $\mathcal{N}_{(\nu)}$ gives rise to A-modules $\Sigma_{(\nu)}, \Delta_{(\nu)}, \Omega(\nu)$ and $\Upsilon_{(\nu)}$ such that*

$$\Sigma_{(\nu)}/\Upsilon_{(\nu)} \cong \Theta.$$

Proof. By construction, $\Sigma_{(0)} \cong \mathcal{F}$. Each further definition step gives rise to an isomorphism $\overline{\sigma}_{(\iota)_{j+1}} : \Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A \longrightarrow \Sigma_{(\iota)_{j+1}}/(\Delta_{(\iota)_{j+1}})_A$. The morphism $\gamma_{(\iota)_j}$ forms an A-module isomorphism for all $(0)_0 \leq (\iota)_j \leq (\nu)_0$, thus we obtain $(\Omega_{(\nu)})_A = \gamma_{(\nu)}(\mathcal{N}_{(\nu)}) \cong \mathcal{N}_{(\nu)}$ and it follows from Lemma 2.4.3 that $\big(\Sigma/(\Delta)_A\big)/(\Omega)_A \cong \Sigma/\Upsilon$ for all indices $(\iota)_j$. Since $\mathcal{N}_{(\nu)} = \mathcal{N}$ we can deduce that

$$\Theta \cong \mathcal{M} \cong \mathcal{F}/\mathcal{N}_{(\nu)} \cong \Sigma_{(\nu)}/\Upsilon_{(\nu)}.$$

□

2.4.2 Coincidences in the Procedure

Let $v \in \langle B_{(\iota)} \rangle$ denote a coincidence and suppose that $v = \sum_{i=1}^{m} \lambda_i \cdot b_i$ so that $HT(v) = \lambda_m \cdot b_m$. Since $v = \gamma(r)$ where $r = 0 \in \mathcal{M}$ it follows that the head term $HT(v)$ and the reduct $RED(v)$ must have the same image in an S-module Θ which is isomorphic to $\mathcal{M}$ under a map $\alpha'_{(\iota)} : \Sigma/(\Delta)_A \longrightarrow \Theta$. We can conclude that the elements $HT(v)$ and $RED(v)$ must be congruent as elements of $\Theta_{(\nu)}$.

Practically, in terms of the procedure, we aim to replace, whenever that is possible, the S-module generator $HM(v) = b_m$ by the linear combination $HC(v)^{-1} \cdot RED(v)$. However, in order to ensure termination of the procedure, we always define the head term as that non-trivial summand b_m of an element v, such that

$$m = \mathbf{max}\{i \mid b_i \text{ summand of } v \text{ with } \lambda_i \neq 0\}$$

and as the coefficients λ_i in our case come from a ring they are not necessarily units. So the inverse $HC(v)^{-1}$ does not need to exist. Because of this we will distinguish between the following two cases:

1. *the applicable coincidences,*
2. *the inapplicable coincidences.*

Applicable Coincidences and Consequences

We will begin with the case where $HC(v)$ is a unit of S for a given coincidence v. Let $b_m = HM(v)$. Since $HM(v)$ and $(\lambda_m^{-1} \cdot \sum_{i=1}^{m-1} \lambda_i \cdot b_i)$ must have the same image when mapped to Θ we can conclude that b_m becomes redundant as an S-module generator for $\Theta_{(\nu)}$ as it is contained in the S-linear span of those generators which have a non-zero coefficient as summands of $RED(v)$. In this case we will call v an **applicable coincidence**. We aim to keep the list of S-module generators as small as possible, so we will remove the element b_m from the generating set for $\Theta_{(\nu)}$ and we then say that we **replace** $b_m = HM(v)$ by the **replacement** $HC(v)^{-1} \cdot RED(v) = (\lambda_m^{-1} \cdot \sum_{i=1}^{m-1} \lambda_i \cdot b_i)$. In order to emphasize that we replace an element b_m we will denote its replacement by r_{b_m}.

Example 2.4.5 *Let* $\mathcal{M}_A = \langle y_1, y_2 \mid y_1.x^2 - y_2, 2 \cdot y_2, y_2.x + y_2 \rangle$ *the module over the free* $\mathbb{Z}$*-algebra* A *generated by one element* x*. We begin by setting* $b_1 := \rho_{(0)}(y_1)$ *and* $b_2 := \rho_{(0)}(y_2)$*. One possible way of assigning* S*-module generators (in the way of choosing which element* $y.w$ *gets assigned to which* S*-module generator) leads to the following:*

- *Induced by the relation* $y_1.x^2 - y_2$ *we pursue definition steps resulting in* $b_3 := \rho_{(0)_1}(y_1.x)$ *and* $b_4 := \rho_{(0)_2}(y.x^2)$*. Therefore we obtain the coincidence* $c = \gamma_{(0)_{t(\iota)}}(y_1.x^2 - y_2) = \gamma_{(0)_2}(y_1.x^2 - y_2) = b_4 - b_2$*. Since* $HC(c) = 1$ *the coincidence is applicable and we can replace* $HM(c) = b_4$ *by the reduct* $RED(c) = b_2$*.*

- *The next relation we will examine is* $2 \cdot y_2$ *from which we can deduce that* $\gamma_{(1)_{t(1)}}(2 \cdot y_2) = \gamma_{(1)_0}(2 \cdot y_2) = 2 \cdot b_2$ *lies in the kernel of a surjective map* $\beta_{(\nu)}$ *to some* $\Theta_{(\nu)} \cong \Theta$*. In this case the head coefficient* 2 *is not a unit in* $\mathbb{Z}$ *and therefore we cannot conclude that the element* b_2 *itself is redundant as generator for the* S*-module we want to construct.*

The second case stated in the example above shows a coincidence c which has a head coefficient which is not invertible; we will call such coincidences **inapplicable coincidences**. For reasons of termination, inapplicable coincidences will be dealt with in a different way from the applicable coincidences. This will be explained in greater detail in the following section.

Remark 2.4.6 *Note that, to ensure termination of the MGE-procedure, we have to make sure that the head generator of the replacement* $r_b = RED(c)$ *of an element* $b = HM(c)$ *has smaller index than the element* b *itself. This is necessary since the set* $\mathcal{B}$*, from which we draw the* S*-module generators, is bounded below but not above. We achieve this by our choice of the head monomials above. Moreover, the choice of head monomials will also prevent an inapplicable coincidence, such as "*$2 \cdot b_2 - b_1$*," being treated as an applicable coincidence by deleting* b_1 *and replacing it by* $2 \cdot b_2$*.*

From now onwards we want to be able to distinguish between elements $b \in B$ that have been found to be redundant as S-module generators for $\Theta_{(\nu)}$

and which we have replaced by an S-linear combination of other elements of B, and those elements which are still found to be necessary as generators for $\Theta_{(\nu)}$. This leads to the following definition:

Definition 2.4.7 *Let $B_{(\iota)_j}$ denote the set of possible S-module generators of $\Theta_{(\nu)}$ found at a certain stage of the MGE-procedure. We will call those elements of $B_{(\iota)_j}$ which were found to be redundant as generators of $\Theta_{(\nu)}$ the* **deleted generators** *and we will denote the subset of these by $B^d_{(\iota)_j}$. We will call the set $B_{(\iota)_j} \backslash B^d_{(\iota)_j}$ the set of* **undeleted generators** *and we will denote it by $B^u_{(\iota)_j}$.*

Let $v = \sum_{i=1}^{m} \lambda_i \cdot b_i \in \langle B_{(\iota)_j} \rangle_S$. We define the **undeleted image** *$u_{(\iota)}(v)$ of v, after having obtained the information of the set of relations $\{r_{(1)}, \ldots, r_{(\iota)}\}$, as follows:*

$$u_{(\iota)}(v) := \sum_{i=1}^{m} \lambda_i \cdot \begin{cases} b_i \text{ if } b_i \in B^u_{(\iota)_j} \\ u_{(\iota)}(r_{b_i}), \text{ otherwise.} \end{cases}$$

Remark 2.4.8 *Since the undeleted image $u_{(\iota)_j}(v)$ of an element $v \in \langle B_{(\iota)_j} \rangle$ depends on the relations $\{r_{(1)}, \ldots, r_{(\iota)}\}$ it follows that*

$$u_{(\iota)_{j_1}}(v) = u_{(\iota)_{j_2}}(v)$$

for all $(1) \leq (\iota) \leq (\nu)$ and all $j_1, j_2 \in \{0, \ldots, t(\iota)\}$.

Notation 2.4.9 *We will use an exponent "u" as for instance in $\Sigma^u_{(\iota)}$ for the S-modules of the MGE-procedure in order to indicate that instead of a generating set $B_{(\iota)}$ the respective S-module is generated by a set $B^u_{(\iota)}$.*

Lemma 2.4.10 *The S-module $\Sigma_{(\iota)_j}/\Upsilon_{(\iota)_j}$ can be provided with the structure of an A-module where we define the product by the A-module generators $x \in X$ as follows: Let $b \in B_{(\iota)_j}$, then*

$$(b + \Upsilon) \star x := \begin{cases} u_{(\iota)_j}(b') \text{ if } (b.x) \sim_{\Delta_{(\iota)_j}} b' \in \langle B_{(\iota)_j} \rangle_S \subset \Sigma_{(\iota)_j} \\ b.x, \text{ the free product in } \Sigma_{(\iota)_j}, \text{ otherwise.} \end{cases}$$

Proof. If the product "$\star$" corresponds to the free concatenation then it is clear that it admits the A-module structure. In the other case the claim

follows as the undeleted image $u_{(\iota)}(v)$ is additive. The undeleted image only depends on the generators $b \in B_{(\iota)}$ that have been deleted and that are contained as summands in an element $v \in \langle B_{(\iota)} \rangle_S$, but not on the coefficients $\lambda \neq 1_S$. □

We suppose again that $c \in \langle B_{(\iota)_{t(\iota)}} \rangle_S$ is an applicable coincidence which implies that $HM(c) \sim HC(c)^{-1} \cdot RED(c)$. Since coincidences are caused by A-module relations coincidences imply the following congruences

$$HM(c) \star w \sim HC(c)^{-1} \cdot RED(c) \star w$$

in $\Sigma_{(\iota)}/\Upsilon_{(\iota)}$ for all $w \in X^*$. In particular when we aim to replace $HM(c) = b_m$ but where $b_m \star x \in \langle B_{(\iota)} \rangle_S$ for any $x \in X$, say $b_m \star x = v \in \langle B_{(\iota)} \rangle_S$, we will consider the congruence

$$v \sim HC(c)^{-1} \cdot RED(c) \star x.$$

as possibly leading to a new coincidence in order to capture possible congruences of S-module generators as quickly as possible. If in this situation the product $b_k \star x$ for any generators b_k in $RED(c)$ is not contained in $\langle B_{(\iota)_j} \rangle$ we will make the appropriate definition steps until it is for each of the generators which are summands of the reduct.

Eventually we will obtain $c \star x = \widetilde{c} \in \langle B_{(\iota)_{j+l}} \rangle_S$ and we know that $\widetilde{c}$ must be contained in the kernel of $\alpha_{(\iota)} : \Sigma_{(\iota)}/\Upsilon_{(\iota)} \longrightarrow\!\!\!\!\!\rightarrow \Theta$ as well. We will call a coincidence $\widetilde{c}$ which has been induced by another coincidence a **consequence**. We will show in Chapter 4 that the procedure of collecting the consequences of a coincidence and moreover the processing of coincidences is strictly terminating.

Suppose we have assigned possible S-module generators to the prefixes of $r_{(1)}, \ldots, r_{(\iota)}$. We obtain a generating set for $\mathcal{N}_{(\iota)}$ and we moreover suppose that we are in a state $(\iota)_j$. We introduce a new set of mappings $\tau_{(\iota)_k} : \mathcal{F} \longrightarrow \Sigma/\Upsilon_{(\iota)_k}$ such that a map $\tau_{(\iota)_j}$, which is defined on the generators of $\mathcal{F}_S$, takes into account the information gained from the set of relations $r_{(1)}, \ldots, r_{(\iota)}$, in particular the coincidences and consequences. We define $\tau_{(\iota)_j}$ by

$$\tau_{(\iota)_j}(y.w) := u_{(\iota)_j}\left(\gamma_{(\iota)_j}(y.w)\right)$$

for $y.w \in \mathcal{F}$. Accordingly whenever we have to replace a generator $b \in B_{(\iota+1)_0}$ by its undeleted image $u_{(\iota+1)}(b)$ at some stage of the procedure we will then want to adjust the map τ. Suppose $b = \tau_{(\iota)_j}(y.w)$ and that we have detected an applicable coincidence c with $HM(c) = b$. At that point when we apply the coincidence which leads to deleting the generator b, we will apply this information to the maps τ as well and we set $\tau_{(\iota+1)_0}(y.w) = r_b = HC(c)^{-1} \cdot RED(c)$. We denote the S-linear extension of the map $\tau_{(\iota)_j}$ by $\delta_{(\iota)_j}$, giving an A-module epimorphism

$$\delta_{(\iota)_j} : \mathcal{F} \longrightarrow \Sigma_{(\iota)_j}/\Upsilon_{(\iota)_j}.$$

Inapplicable Coincidences

So far we described the way in which the MGE-procedure handles applicable coincidences where we can replace the $HM(c)$ of a coincidence c by $HC(c)^{-1} \cdot RED(c)$. If $HC(c)$ however is not a unit of S then we certainly cannot conclude that the head monomial $HM(c)$ itself lies in the S-linear span of the generators in the reduct of c. We will call a coincidence c where $HC(c)$ is not a unit in S an **inapplicable coincidence**.

The MGE-procedure will deal with the inapplicable coincidences separately from the applicable coincidences (from which we can draw immediate conclusions). Whenever an inapplicable coincidence is detected, it will be stored in an ordered list. We will call this list the **torsion sequence** and we will denote it, depending on the stage (ι) of the procedure, by $L_{(\iota)}$. The letter "L" is induced by the fact that this list corresponds to a lattice as it is a list with ordered elements. In the same manner as in the case of applicable coincidences we consider the elements of L as elements of $\Sigma_{(\iota)}$.

The form of $L_{(\iota)}$ depends on the relations $r_{(1)}, \ldots, r_{(\iota)}$ which have already been investigated. The elements of the torsion sequence are ordered by the indices of their head monomials: let l_i, l_j be entries in $L_{(\iota)} = \{l_1, \ldots, l_t\}$. For correctness of the MGE-purpose we will always ensure that $HM(l_i) > HM(l_j)$ when $i < j$.

The elements of $L_{(\iota)}$ at a stage $(\iota)_k$ generate an S-submodule of Σ which we will denote by $\Lambda_{(\iota)}$. We will show in Chapter 4 that an arbitrary element

$l \in \Lambda_{(\iota)}$ must be inapplicable itself. Also in Chapter 4 we will describe in detail the handling of inapplicable coincidences: for instance the procedure of inserting inapplicable elements into the torsion sequence.

If at the point of termination $L_{(\nu)} \neq \emptyset$ then the elements of $L_{(\nu)}$ correspond to the generators of the torsion-submodule of $\Theta_{(\nu)}$, multiplied by their respective exponents. We will obtain $\Theta_{(\nu)}$ as the quotient-module of a certain finitely generated and free S-module Γ with generating set $B^u_{(\nu)}$ such that

$$\Theta = \Gamma/(\Lambda)_A.$$

2.5 Data accompanying the Computation

For the description of the MGE-procedure we will assign certain quadruples of data to every stage of the procedure. As described earlier, we have a series of stages accompanying the construction of a generating set of a module $\mathcal{N}_{(\iota+1)}$ and these stages depend on the relation $r \in Rels \backslash \{r_{(\iota)}, \ldots, r_{(\iota)}\}$ which gets investigated at that current state of the procedure, and on the prefixes of that relation. In order to describe these stages we introduced a further index, thus we have a set $\{(\iota)_0, \ldots, (\iota)_j, \ldots (\iota)_{t(\iota)}\}$ of indices, used in order to distinguish between the different forms of tools accompanying $\mathcal{N}_{(\iota)}$ such as for instance the modules $\Upsilon_{(\iota)_j}, \Upsilon_{(\iota)_{j+1}} \ldots \Upsilon_{(\iota)_{t(\iota)}}$.

We assume that relations $r_{(1)}, \ldots, r_{(\iota)}$ have been examined so far and that we have already traced j prefixes of the currently investigated relation r and we will describe the quadruple for this case. For the remaining part of the description of the quadruple we will omit the index $(\iota)_j$ whenever there is no ambiguity.

2.5.1 The S-Module Generating Set

The first part of the a tuple consists of the set B which is an approximation of the set of S-module generators for a finitely generated and free S-module Γ of which Θ is a quotient-module.

2.5.2 The Multiplication Table

We define the **Multiplication Table**, which will be denoted T, accompanying a submodule $\mathcal{N}_{(\iota)}$ (or in other words accompanying the construction of a generating set for $\mathcal{N}_{(\iota+1)}$) as a table in which we store certain information about the elements $b \in B$ contained in the set of possible generators of the S-module $\Theta_{(\nu)}$. The rows are indexed by an ordered set $B = \{b_1, \ldots b_{m(\iota)}\}$ and each row corresponds to a generator $b \in B$. We let the symbol $\perp$ denote "empty" or unknown. A row "b" of the table T contains the following information about a generator $b \in B$:

- A column del_b, which contains a flag which is either set to "**true**" or "**false**". If the flag in a row is set to "**true**", then this indicates that the accompanying generator b has been deleted; "**false**" that it has not been deleted.

- A column r_b which, in the case that the generator b corresponding to the row has been deleted, contains the possible replacement r_b. In case that $b \in B^u$ then r_b has not been defined and the entry in that column reads $\perp$.

- For every algebra generator $x \in X$ we have a column $\mathbf{prod}(b, x)$. A box in such a column either contains the product $b \star x$, or, in case that the free product $b.x$ is not congruent modulo Δ to an element of $\langle B \rangle_S$, the entry will read $\perp$.

- A column which, only if $del_b =$ **false**, contains the pre-image of $b \in B^u$ under the mapping $\rho : f \longmapsto b \in B^u$; otherwise the entry is "$\perp$".

Therefore, a table $T_{(\iota)}$ provides a description of the multiplication in an S-module which is isomorphic to $\mathcal{M}_{(\iota)} = \mathcal{F}/\mathcal{N}_{(\iota)}$. At the beginning of the procedure we will initialise the multiplication table $T_{(0)}$ which has rows corresponding to the set of S-module generators $B_{(0)} = \{b_1, \ldots, b_n\}$ which is in one-one relation to the set of module generators Y of $\mathcal{M}$. All rows of $T_{(0)}$ correspond to undeleted S-module generators and no boxes for the

action of $x \in X$ on $b \in B_{(0)}$ have been filled. Thus $T_{(0)}$ represents the free S-module $\langle B_{(0)}X^* \rangle = \Sigma_{(0)}$ which is isomorphic to $\mathcal{F}$.

From the pre-image contained in the table for $b \in B^u$ together with the undeleted image of $b \in B^d$ the mapping $\delta : \mathcal{F} \longrightarrow \langle B^u \rangle_S \subset \Sigma/(\Delta)_A/(\Omega)_A$ can be reconstructed.

By abuse of notation we will from now onwards not distinguish between the i-th row of the table and the S-module generator $b_i \in B$ corresponding to it.

Example 2.5.1 *Suppose that we have traced relations* $\{r_{(1)}, \ldots, r_{(\iota)}\} \in$ *Rels. A row in a multiplication table possibly describing such a situation is given by:*

	del_b	r_b	$\boldsymbol{prod}(b, x_1)$	...	$\boldsymbol{prod}(b, x_t)$	$\rho^{-1}(b)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_h	f	$\perp$	$\perp$	...	v	$y.w$
b_{h+1}	t	$b_7 - 3 \cdot b_4$	$\perp$	...	$\perp$	$\perp$
b_{h+2}	f	$\perp$	v'	...	v''	$y.\widetilde{w}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

In the table above, the row b_h *corresponds to the undeleted* S*-module generator with index* h*. The fact, that the generator* b_h *has not been deleted is indicated by the entry "*f*" in the column "*del_b*".*

The table describes the action of the algebra A*, which in this case has generators* $x_1, \ldots, x_t$*. The product* $b_h \star x_t$ *is contained in* $\langle B \rangle_S$ *and its undeleted image is a vector* $v = \sum_{i=1}^{m} \lambda_i \cdot b_i$*. Since the generator* b_h *is undeleted, the box with the replacement "*r_b*" has been filled with the symbol "*$\perp$*". Moreover, at this stage of the procedure there is no element of* $\langle B \rangle$ *known to be equal to* $b_h \star x_1$*, therefore the table-entry for the box of the product* $prod(b_h, x_1)$ *has been filled with the symbol "*$\perp$*" as well. All the information which is contained in the table has been obtained by tracing the prefixes of the finite subset* $\{r_{(1)}, \ldots r_{(\iota)}\} \subset$ *Rels.*

By the Schreier Theorem in Chapter 1 we know that, in the case that $\mathcal{M}$ is isomorphic to a finitely generated S-module, a finite subset of the set *Rels*

should suffice as generating set for the submodule $\mathcal{N}$ of $\mathcal{F}$. The multiplication table, or to be accurate, the choice of the S-module generators corresponding to its rows, has an impact on the choice of this subset of $Rels$: if we are investigating coincidences caused by an algebra-relation $r \in A$ then r will lead to an infinite number of module-relations $\{y.wr \mid y \in Y, w \in X^*\}$. We will however confine to those elements $y.w \in \mathcal{F}$ such that $\gamma(y.w) = b \in B^u$. We will ensure that we will apply every algebra-relation at a generator $b \in B^u$: this might also be called **pushing at** b.

2.5.3 The Coincidence Stack

In theory we interpret coincidences as generators of a certain S-submodule; the coincidences together with the set of generators of Δ gives rise to the S-module Υ. The product "$\star$" in the quotient-module Σ/Υ uses the undeleted image. Thus if an element $v \in \langle\Sigma\rangle_S$ contains a summand or the prefix of a summand with $b = HM(c)$ of an applicable coincidence c, then $v \notin \langle\Sigma^u\rangle_S$ and in fact there exists an element $\widetilde{v}$ which is congruent to v modulo Υ such that $\widetilde{v} \in \langle\Sigma^u\rangle_S$.

Here however we demand that all applicable coincidences have been processed and the so-obtained undeleted image has been applied to all elements or, in other words, that for all head terms b_c of applicable coincidences we have that $b_c \in B^d$. In practical terms this is not the case at every stage of the procedure. The next part of the tuple accompanying $\mathcal{N}_{(\iota)}$ consists of a tool used in the procedure in order to handle those coincidences of which the procedure has already become aware but which it was not able yet to examine and apply any further.

We call this the **coincidence stack** and we will denote it by Cp. The elements stored in Cp are ordered by the point of when they have been added to the stack: so elements which have been added last will be dealt with first. The coincidences contained in Cp are considered to be pending: when a coincidence c is found, it might not be dealt with immediately, for instance in the situation where the MGE-procedure is currently processing a different coincidence $\widetilde{c}$, which might lead, amongst other things, to the computation of the consequences of $\widetilde{c}$. Then c will first be added to the

stack: we set $Cp_{(\iota+1)_0} := Cp_{(\iota)_{t(\iota)}} \cup \{c\}$, where it is stored until the MGE-procedure, possibly at a later stage, will process c. Only then will the procedure evaluate if c is an applicable coincidence of not. If it is applicable then in the course of processing c all consequences $\widetilde{c}_1, \ldots, \widetilde{c}_l$ which are caused by c will be traced and added to the stack. Therefore the coincidence stack might contain coincidences which are non-applicable.

Moreover, since coincidences might be stored in $Cp_{(\iota)_j}$ over a few stages of the procedure there might be coincidences $c \in Cp_{(\iota)_j}$ such that $c \neq u_{(\iota)_j}(c)$. The reason for this is that the MGE-procedure will not update or check the coincidences while they are in the stack. Only at the point when $c \in Cp$ is chosen for processing will we replace c by the undeleted image $u(c)$ at that stage of the computation. This in means in particular that when a coincidence c is processed we will trace c completely, now as element of Σ/Υ and therefore using the product "$\star$".

2.5.4 The Torsion Sequence

If S is a domain but not a field we have seen before that the S-module Θ we wish to construct possibly contains torsion elements. If it does then we have to distinguish between applicable and inapplicable coincidences in the MGE-procedure. When the procedure has terminated the inapplicable coincidences, which are stored in the torsion sequence L, can be seen as generating set of a certain S-module Λ which is a submodule of a finitely generated and free S-module Γ, such that $\Theta = \Gamma/\Lambda$. In order to handle inapplicable coincidences we mainly need two procedures:

1. We must ensure at all times that no applicable coincidences are contained in the S-linear span of the inapplicable coincidences. Therefore we will store the inapplicable coincidences in a sequence L with elements which are strictly ordered by their head monomials. Therefore whenever an element gets inserted into L we must make sure that this ordering is maintained.

2. As the inapplicable coincidences $l \in L$ have also been obtained from A-module relations we must ensure that the S-module Λ generated by

the $l \in L$ equals its own A-module closure. We aim to close L with respect to action by the A-module generators $x \in X$.

In practical terms of the procedure, two separate lists will be used to store and handle the inapplicable coincidences:

1. *The Torsion Sequence L.*

2. *The List of inapplicable Coincidences I.*

These lists have identical elements. The elements of these lists are ordered in two different ways. We order the elements of the Torsion Sequence L by the index of their head monomial, thus we will always strictly ensure that for $i_1 < i_2$ we have that $HM(l_{i_1}) > HM(l_{i_2})$ for $l_{i_1}, l_{i_2} \in L$. The sequence I is used for the computation of the A-module closure of the elements which are stored in L. The elements of I are ordered on a "first in – first out" basis: the A-module closure of elements which have been inserted into I at an earlier point will be computed first.

Remark 2.5.2 *Contrary to the elements of Cp we will ensure that all $l \in L$ will be checked if they are affected whenever an applicable coincidence is processed that leads to the deletion of some $b \in B^u$. In the case that b is summand of $l \in L$ we will then replace l by its undeleted image. Moreover, if b is even the head monomial of some $l \in L$ then this l will be removed from the torsion sequence and we will add l to the coincidence stack where eventually it will be processed again. In this way we ensure that at every stage of the procedure only inapplicable coincidences are contained in a torsion sequence L and furthermore that all elements of L are contained in $\langle B^u \rangle_S$.*

We will complete this chapter with a short example of an MGE-procedure in terms of the data such as multiplication table, coincidence stack and torsion sequence used. Note that in this example we will use the technique of inserting inapplicable coincidences which will be described in detail in Chapter 4.

Example 2.5.3 *Let $\mathcal{M} = \langle y_1, y_2 \mid y_1.x^3 - y_2, 2 \cdot y_1.x - 6 \cdot y_1 \rangle_P$ and let $P = \langle x \mid x^2 - 2 \cdot x \rangle_{\mathbb{Z}}$. We begin with the generating set $B_{(0)} = \{b_1, b_2\}$ and*

accordingly initialise the multiplication table T as follows

	del_b	$\mathbf{prod}(b,x)$	$\rho^{-1}(b)$	r_b
b_1	f	$\perp$	y_1	$\perp$
b_2	f	$\perp$	y_2	$\perp$

We moreover set $Cp = \emptyset$ and $L = \emptyset$. We first examine the module relation $y_1.x^3 - y_2$ which leads to the definition steps $b_3 := \rho_{(0)_1}(y_1.x), b_4 := \rho_{(0)_2}(y_1.x^2)$ and $b_5 := \rho_{(0)_3}(y_1.x^3)$. The so-obtained applicable coincidence $b_5 - b_2$ does not have to be stored in Cp but can be processed immediately. Applying this information to the table gives

	del_b	$\mathbf{prod}(b,x)$	$\rho^{-1}(b)$	r_b
b_1	f	b_3	y_1	$\perp$
b_2	f	$\perp$	y_2	$\perp$
b_3	f	b_4	$y_1.x$	$\perp$
b_4	f	b_2	$y_1.x^2$	$\perp$
b_5	t	$\perp$	$\perp$	b_2

The coincidence induced by second module-relation $2 \cdot y_1.x - 6 \cdot y_1$ is without any further definition steps already contained in the S-linear span of the generators $B^u_{(1)} = \{b_1, b_2, b_3, b_4\}$ and in fact it is an inapplicable coincidence $2 \cdot b_3 - 6 \cdot b_1$ which we add to the torsion sequence: $L := [2 \cdot b_3 - 6 \cdot b_1]$.

Next we begin examining the relations that are implied by the relation $x^2 - 2 \cdot x$. Application of it at b_1 gives $b_1 \star x^2 - 2 \cdot b_1 \star x = b_4 - 2 \cdot b_3$; however, as $b_4 \star x \in \langle B \rangle$ this coincidence gives rise to a consequence and before we can delete b_4 and replace it by the replacement $2 \cdot b_3$ we have compute the consequence $\widetilde{c} = c \star x$. We obtain $\widetilde{c} = b_4 \star x - 2 \cdot b_3 \star x = b_2 - 2 \cdot b_4$ and since $\widetilde{c}$ cannot be processed immediately we add it to the coincidence stack: $Cp := \{b_2 - 2 \cdot b_4\}$, and now b_4 can be deleted.

Then we can process $\widetilde{c}$, as now $b_4 \in B^d$ we have to replace $\widetilde{c}$ by its undeleted image, we obtain an inapplicable coincidence $u(\widetilde{c}) = u(b_2 - 2 \cdot b_4) = b_2 - 4 \cdot b_3$ which we insert into L. We have that $HM(u(\widetilde{c})) = HM(l)$ for the element $l \in L$. As we must ensure that $HM(l_i) \neq HM(l_j)$, we replace $u(\widetilde{c})$ by $\widetilde{v} := 2 \cdot l + u(\widetilde{c}) = 2 \cdot (2 \cdot b_3 - 6 \cdot b_1) - 4 \cdot b_3 + b_2 = b_2 - 12 \cdot b_1$.

Since $\widetilde{v}$ is an applicable coincidence it will not be inserted into L. Moreover as $b_2 \star x \notin B$ no further consequences are induced and it can be processed

immediately. We will describe the general approach for the inserting of elements into the torsion sequence closely in Chapter 4. We now obtain the table:

	del_b	$\mathbf{prod}(b,x)$	$\rho^{-1}(b)$	r_b
b_1	f	b_3	y_1	$\perp$
b_2	t	$\perp$	$\perp$	$12 \cdot b_1$
b_3	f	$2 \cdot b_3$	$y_1.x$	$\perp$
b_4	t	$\perp$	$\perp$	$2 \cdot b_3$
b_5	t	$\perp$	$\perp$	b_2

and $Cp = \emptyset$ *and* $L = [2 \cdot b_3 - 6 \cdot b_1]$. *The A-module closure of* $l_1 \in L$ *gives* $l_1 \star x = 2 \cdot b_3 \star x - 6 \cdot b_1 \star x = -2 \cdot b_3$ *and we replace* l_1 *and* $l_1 \star x$ *by the elements* $v_1 := l_1 \star x + l_1 = -6 \cdot b_1$ *and* $v_2 := l_1 + v_1 = 2 \cdot b_3$ *and we obtain the torsion sequence* $L = [2 \cdot b_3, -6 \cdot b_1]$.

Since the application of an algebra relation at a generator which has already been deleted would not provide new information we will apply $x^2 - 2 \cdot x$ *at the next generator contained in* B^u. *We obtain the trivial coincidence* $b_3 \star x^2 - 2 \cdot b_3 \star x = 4 \cdot b_3 - 4 \cdot b_3$.

Therefore we obtain an S*-module* Θ *which is a quotient-module of the free module* $\langle b_1, b_3 \rangle_S$. *These generators correspond to the elements* y_1 *and* $y_1.x \in \mathcal{F}$. *The free rank of* Θ *is zero as both* b_1 *and* b_3 *are torsion elements,* b_1 *has the exponent* -6 *and* b_3 *has the exponent* 2. *The action of the generator* x *of* A *is described by the matrix*

$$x = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}$$

Chapter 3

Gröbner Bases and MGE-Procedure

In the following chapter we shall introduce Gröbner bases for S-modules and also prefix Gröbner bases in the case of A-modules which are given as the S-module closure of certain finitely generated S-modules. These methods shall be applied in subsequent chapters to the modules constructed in the course of an MGE-procedure and we shall use certain properties of such Gröbner bases in order to show correctness and termination of the MGE-procedure.
Section 3.1: We describe terminology such as ordering and reduction in the case of the S-modules for a Euclidean domain S and we specify S-module Gröbner bases. Certain properties of S-module Gröbner bases shall be established with regard to the reduction by elements which are contained in an S-module Gröbner basis.
Section 3.2: We describe prefix-reduction of elements of a free A-module. Prefix Gröbner bases are introduced and we shall discuss properties of modules which are generated by a prefix Gröbner basis. Thereafter we shall introduce the concept of prefix-closure. We show how prefix-closure can be used in certain cases in order to obtain a finite prefix Gröbner basis from a given S-module Gröbner basis.

3.1 Gröbner Bases of S-Modules

3.1.1 Ordering and Reduction on S-Modules

We introduce now the appropriate notation and language of ordering and reduction on elements of a module and we will explain the reduction techniques which we will use to simulate the MGE-procedure.

Definition 3.1.1 *Let $E = \{e_0, e_1, e_2, \dots\}$ be a set. We call a partial ordering $\succeq$ on the elements of E a* **well-founded ordering** *if the corresponding strict ordering $\succ$ allows no infinite descending chain $e_{i_1} \succ e_{i_2} \succ \dots$ for $e_{i_j} \in E$.*

A **reduction rule with respect to an ordering $\succeq$ on E** *is an irreflexive relation of a pair of elements (e_1, e_2) where $e_1 \succeq e_2$ and a reduction rule is written as*

$$e_1 \longrightarrow e_2.$$

We will call a reduction rule with respect to an ordering $\succeq$ on E **Noetherian**, *if no infinitely descending sequences of reductions*

$$e_0 \longrightarrow e_1 \longrightarrow e_2 \longrightarrow \cdots \text{ with } i \in \mathbb{N}$$

exist for the elements $e_i \in E$ where $e_i \neq e_{i+1}$.

Definition 3.1.2 *Let $\mathcal{H}$ denote a module with $h, h' \in \mathcal{H}$ and let $\mathcal{K}$ denote a submodule of $\mathcal{H}$. The module $\mathcal{K}$ defines a congruence relation " $\sim$ " on the elements of $\mathcal{H}$: we say that h and h' are* **congruent** *if $h - h' \in \mathcal{K}$. We define* **congruence classes** *on $\mathcal{H}$: the congruence class of $h \in \mathcal{H}$ by the (congruence) relation $\sim$, which we denote by $|h|_\sim$, is the set consisting of those elements $\widetilde{h} \in \mathcal{H}$ such that $h \sim \widetilde{h}$. We may also write $\sim_\mathcal{K}$ and $h \sim_\mathcal{K} h'$ if we want to stress that the congruence is generated by $\mathcal{K}$.*

Let $|h|_\sim$ denote a congruence class of elements of a module $\mathcal{H}$ and let " $\succeq$ " denote an ordering on the elements of $\mathcal{H}$. We will call an element $\overline{h} \in \mathcal{H}$ **minimal** *in its class $|h|_\sim$ if there is no $h' \in |h|_\sim$, $h' \neq \overline{h}$, such that $\overline{h} \succeq h'$.*

We will now discuss the terms of ordering and reduction in the case of S-modules. Thus let S be an ordered Euclidean domain. It should be stressed at this point that not every Euclidean domain is ordered. For instance the Gaussian integers, as a subring of the complex numbers, form a domain that cannot be ordered: there does not exist a total ordering for the elements of the Gaussian integers.

We furthermore assume that the algebra A is a finitely generated monoid-algebra over S that is generated by the finite set X. We will denote by $\mathcal{F} = \langle Y \rangle_A$ a free and finitely generated A-module. Moreover, we define Σ as the A-module closure of a finitely generated S-module $\langle B \rangle_S$, where B is an ordered set $B = \{b_1, \ldots, b_m\}$; thus $\Sigma = \langle BX^* \rangle_S$.

Definition 3.1.3 *We denote by $\mathfrak{P} \subset S$ a subset of elements of S such that the following holds:*

1. *If $\lambda_1, \lambda_2 \in \mathfrak{P}$, then $\lambda_1 + \lambda_2 \in \mathfrak{P}$ and also $\lambda_1 \cdot \lambda_2 \in \mathfrak{P}$;*
2. *for $\lambda \in S$ one of $\lambda \in \mathfrak{P}$, $-\lambda \in \mathfrak{P}$, or $\lambda = 0$ holds.*

The set $\mathfrak{P}$ is called the set of **positive elements** *of S.*

We obtain a total ordering $>_S$ on elements of S: Let $\lambda_1, \lambda_2 \in S$, we set

$$\lambda_1 >_S \lambda_2 \Longleftrightarrow \lambda_1 - \lambda_2 \in \mathfrak{P}.$$

For $\lambda \in S$ we set

$$|\lambda| = \begin{cases} \lambda, \text{ if } \lambda \in \mathfrak{P} \text{ or } \lambda = 0; \\ -\lambda, \text{ otherwise.} \end{cases}$$

We can extend the ordering on S in order to obtain a total ordering "$\succ$" on the elements of $\langle B \rangle_S$. Let $v_1 = \sum_{j=1}^{m_1} \lambda_j \cdot b_j$, with $HM(v_1) = b_{m_1}$, and $v_2 = \sum_{j=1}^{m_2} \kappa_j \cdot b_j$ with $HM(v_2) = b_{m_2}$. We set

$$v_1 \succ v_2 \Longleftrightarrow \begin{cases} m_1 > m_2, \text{ or} \\ m_1 = m_2 \text{ and } \kappa_{m_1} >_S \lambda_{m_2}, \text{ or} \\ m_1 = m_2 \text{ and } \kappa_{m_1} = \lambda_{m_2} \text{ and } RED(v_1) \succ RED(v_2). \end{cases}$$

An element $v \in \Sigma$ is of the form

$$v = \sum_{j=1}^{m} \sum_{k=1}^{t(j)} \lambda_{jk} \cdot b_j.w_{jk}, \quad \text{where } w_{jk} \in X^* \text{ and } \lambda_{jk} \in S.$$

Since Σ, as the A-module closure of a free S-module, is free itself, this linear combination of the elements $b.w$, where $b \in B$ and $w \in X^*$, is unique for every $v \in \Sigma$. We extend the given ordering on $\langle B \rangle$ by defining an ordering on the elements of Σ. This ordering is induced by the maximal length of words of the monoid X^* occurring as summands of the module element:

Definition 3.1.4 *Let $w = x_{i_1} x_{i_2} \cdots x_{i_t} \in X^*$, we define the* **length of** *w as*

$$|w| := t.$$

For $v \in \Sigma$ where $v = \sum_{j=1}^{m} \sum_{k=1}^{t(j)} \lambda_{jk} \cdot b_j.w_{jk}$, we then define the **weight of** *v, denoted by $Wei(v)$ as*

$$Wei(v) := \textbf{\textit{max}}\{|w_{jk}| : \lambda_{jk} \cdot b_j.w_{jk} \text{ summand of } v \text{ with } \lambda_{jk} \neq 0\}.$$

Let $b_s.w$ and $b_t.w'$ be generators of Σ_S, then

$$b_s.w \succ_{wei} b_t.w' \iff \begin{cases} |w| > |w'|, \text{ or} \\ |w| = |w'| \text{ and } s > t. \end{cases}$$

Accordingly, we define an **ordering by weight** *"$\succ_{wei}$" on the elements of Σ as follows: let $v_1, v_2 \in \Sigma$ with head terms $HT(v_1) = \kappa \cdot b_s.w$ and $HT(v_2) = \lambda \cdot b_t.w'$, then*

$$v_1 \succ_{wei} v_2 \iff \begin{cases} Wei(v_1) > Wei(v_2), or \\ Wei(v_1) = Wei(v_2) \text{ and } s > t, or \\ Wei(v_1) = Wei(v_2) \text{ and } s = t \text{ and } \kappa >_S \lambda. \end{cases}$$

The set B is bounded below in the given situation and the weight of elements of Σ is bounded below by 0 as well. If we assume that there does not exist an infinite descending sequence of elements of the ring S then we can conclude that there cannot exist any infinite sequences

$$|v_1| \succ_{wei} |v_2| \succ_{wei} |v_3| \succ_{wei} \cdots$$

of elements of Σ in the case of ordering by weight in the setting given. In the further procedure we shall assume that there are no infinite sequences of elements of S. We will now introduce reduction on the elements of Σ.

Definition 3.1.5 *Let $v_1, v_2 \in \Sigma$ and let $H = \{h_1, \ldots, h_t\} \subset \Sigma$. We say that H S-**module reduces** v_1 **to** v_2 **in one step**, denoted by $v_1 \xrightarrow[S]{H} v_2$, if*

$$v_2 = v_1 - (\kappa_1 \cdot h_1 + \cdots + \kappa_t \cdot h_t)$$

where $\kappa_i \in S$ such that $\kappa_i \neq 0$ for at least one $i \in \{1, \ldots, t\}$. For $h_j \in H$ with $\kappa_j \neq 0$ the following conditions have to hold:

1. *$HM(h_j) = b.w$ for a summand $\lambda \cdot b.w$ of v_1.*
2. *Let λ denote the coefficient of the summand $b.w$. We demand that there are $\kappa, \kappa' \in S$ with $\lambda = \kappa \cdot HC(h_j) + \kappa'$ where*
   (a) *$|\kappa \cdot HC(h_j)| \leq_S |\lambda|$; and*
   (b) *$|\kappa'| <_S |HC(h_j)|$.*

*We say that H S-**module reduces** v_1 **to** v_2, denoted by $v_1 \xrightarrow[S]{H}{}^{*} v_2$, if there exists a sequence of S-module reductions*

$$v_1 \xrightarrow[S]{H} \widetilde{v}_1 \xrightarrow[S]{H} \cdots \xrightarrow[S]{H} \widetilde{v}_k \xrightarrow[S]{H} v_2$$

with $\widetilde{v}_i \in \Sigma$ for $1 \leq i \leq k$. We call an element $v \in \Sigma$ **minimal with respect to** *H if it cannot be S-module reduced by $H \subset \Sigma$. We call a set H* **inter-reduced** *if every $h_i \in H$ is minimal with respect to $H \backslash \{h_i\}$.*

3.1.2 S-Module Gröbner Bases

Let H denote a finite set of elements of Σ, generating a submodule $\Xi \subset \Sigma$. We are interested to see that the reduction by elements of H leads to a minimal element which is canonical up to multiplication by a unit of S. Let $h_1, h_2 \in H$ such that $HM(h_1) = HM(h_2)$ and $|HC(h_1)| \geq_S |HC(h_2)|$ and let $v \in \Sigma$ be S-module reducible by h_1 and h_2, suppose with the respective

coefficients $\lambda_1, \lambda_2 \in S$. We have

$$\begin{array}{ccc} v & \xrightarrow[S]{h_1} & v_1 := v - \lambda_1 \cdot h_1 \\ {\scriptstyle h_2}\downarrow{\scriptstyle S} & & \\ v_2 := v - \lambda_2 \cdot h_2 & & \end{array}$$

Suppose that $v_1 \neq v_2$ and that v_1 cannot be obtained from v_2 by multiplication with a unit of S. Then if there is no element $\overline{v} \in \Sigma$ with accompanying sequences of reduction $v_1 \xrightarrow[S]{H}{}^{*} \overline{v}$ and $v_2 \xrightarrow[S]{H}{}^{*} \overline{v}$, then the S-module reduction by elements of H does not lead to a canonical result. In the literature of Gröbner bases a set H which does lead to a canonical minimal element is called **confluent**.

Moreover we want to be able to determine if an element v is in minimal form with respect to a set H, or if it is further reducible, by comparing $HT(v)$ with the head terms of elements of H. We want to obtain a generating set H' such that all elements contained in the S-linear span $\langle H' \rangle_S$ have as their minimal form 0.

For $h_1, h_2 \in H$ as above, as $HC(h_1)$ and $HC(h_2)$ are elements of the Euclidean domain S, the extended greatest common divisor provides elements $\kappa_1, \kappa_2 \in S$ such that

$$\kappa_1 \cdot HC(h_1) = \kappa_2 \cdot HC(h_2),$$

namely where $\kappa_i \cdot HC(h_i)$ is the least common multiple of $HC(h_1)$ and $HC(h_2)$ for $i \in \{1, 2\}$.

If we set $\widetilde{v} := \kappa_1 \cdot h_1 - \kappa_2 \cdot h_2$, then $\widetilde{v}$ lies in the S-linear span of h_1 and h_2. In the case that there is no element $h' \in H \backslash \{h_1, h_2\}$ with $HM(\widetilde{v}) = HM(h')$ such that also $|HC(h')| \leq_S |HC(\widetilde{v})|$, the element $\widetilde{v}$ is minimal with respect to H despite the fact that it is contained in the S-linear span of H.

In literature on Gröbner bases a pair of elements such as $h_1, h_2 \in H$ is called a **critical pair**. It can be shown that there is a close connection between the property of a set H being confluent and that all elements contained in the S-linear span have minimal form zero, respectively, with the property that there are no critical pairs contained in H.

Let $H = \{h_1, \ldots, h_t\}$ be a set of elements of Σ. For the set of head monomials of a set H we define

$$HM(H) := \{HM(h_i) \mid h_i \in H\};$$

and in the same way for the head terms, $HT(h) = HC(h) \cdot HM(h)$, we set $HT(H) := \{HT(h_i) \mid h_i \in H\}$.

In order to obtain a confluent set $G \subset \Xi$ such that for all v in the S-linear span of G we have that $HT(v) \in \langle HT(G) \rangle$, B. Buchberger developed the theory of Gröbner bases for the generating sets of ideals in polynomial rings $k[x_1, \ldots, x_n]$, where k is a field, see for instance [6, 7]. Buchberger proved that the property of a set G being confluent can be traced back to certain properties of so-called $\mathfrak{s}$-polynomials constructed from the elements of G. This can be seen as the motivation of the algorithm developed by Buchberger for the construction of Gröbner bases. The theory of Gröbner bases can be translated into the setting of modules over certain types of rings, see for instance [1]. We will now give the definition of an $\mathfrak{s}$-polynomial for elements of a free S-module and also the definition of an S-module Gröbner basis.

Definition 3.1.6 *Let $h_1, h_2 \in \Sigma$ such that $HM(h_1) = HM(h_2)$ and let $\lambda_1, \lambda_2 \in S$ such that $\lambda_1 \cdot HC(h_1) = \lambda_2 \cdot HC(h_2)$. We define an* **$\mathfrak{s}$-polynomial of h_1 and h_2** *as follows:*

$$\mathfrak{s}\text{-}pol(h_1, h_2) := \lambda_1 \cdot h_1 - \lambda_2 \cdot h_2.$$

So the $\mathfrak{s}$-polynomial is a tool in order to construct an element which is contained in the linear span of elements h_1, h_2 but which has a head monomial that is smaller than the head monomials of h_1 and h_2. This is achieved by multiplying h_1 and h_2 respectively by coefficients λ_1, λ_2 such that $\lambda_i \cdot HC(h_i)$ for $i \in \{1, 2\}$ is equal to, or a multiple of the least common multiple of $HC(h_1)$ and $HC(h_2)$.

In the case where head coefficients are elements of a field, an $\mathfrak{s}$-polynomial can be obtained by multiplying with the respective multiplicative inverses of the head coefficients. Also in the case of fields, Buchberger proved that

reduction by a set H must be confluent if each $\mathfrak{s}$-polynomial of elements of H can be reduced to 0 by H. However, in the case where the head coefficients are elements of a ring and thus are not necessarily invertible, we must take the head coefficients themselves into account as well when we are investigating if reduction by a set is confluent.

Suppose for instance the case where $h_1, h_2 \in H$ such that $HM(h_1) = HM(h_2)$ but where the set H does not contain an element h' such that $HM(h') = HM(h_1)$ and $HC(h') = \mu := GCD(HC(h_1), HC(h_2))$. There exist $\kappa_1, \kappa_2 \in S$ such that $\mu = \kappa_1 \cdot HC(h_1) + \kappa_2 \cdot HC(h_2)$. If $\mu <_S HC(h_1)$ and $\mu <_S HC(h_2)$ then $\widetilde{v} = \kappa_1 \cdot h_1 + \kappa_2 \cdot h_2$ is contained in the linear span of H although it is not guaranteed that $\widetilde{v}$ can be S-module reduced any further by elements of H. In order to handle this situation, a further tool has been introduced in the setting of Gröbner bases where the coefficients are elements of a ring. We shall follow the notation used in [5] by T. Becker and V. Weispfenning:

Definition 3.1.7 *Let $h_1, h_2 \in \Sigma$ such that $HM(h_1) = HM(h_2)$ and let $\kappa_1, \kappa_2 \in S$ such that $GCD(HC(h_1), HC(h_2)) = \kappa_1 \cdot HC(h_1) + \kappa_2 \cdot HC(h_2)$. We define a* **$\mathfrak{g}$-polynomial of h_1 and h_2** *as follows:*

$$\mathfrak{g}\text{-}pol(h_1, h_2) := \kappa_1 \cdot h_1 + \kappa_2 \cdot h_2.$$

Lemma 3.1.8 *Let $v \in \Sigma$ and let $H \subset \Sigma$ denote a finite set such that*

$$\mathfrak{g}\text{-}pol(h, h') \xrightarrow[S]{H}{}^{*} 0$$

for all $h, h' \in H$. If $v \xrightarrow[S]{H}{}^{*} 0$ then there exist $h'' \in H$ and $\kappa \in S$ such that $HM(h'') = HM(v)$ and $HC(v) = \kappa \cdot HC(h'')$.

Proof. If $v \xrightarrow[S]{H}{}^{*} 0$ then $v = \sum_{i=1}^{t+k} \lambda_i \cdot h_i$, where we suppose that we have chosen the h_i in such a way that $HM(v) = HM(h_i)$ for exactly $i \in \{1, \ldots, t\}$ and where moreover $|HC(h_1)| \geq_S |HC(h_2)| \geq_S \cdots \geq_S |HC(h_t)|$ for all $1 \leq i \leq t$.

We certainly have that $HT(v) = \sum_{i=1}^{t} \lambda_i \cdot HT(h_i)$ and $|HC(h_i)| \leq_S |HC(v)|$ for all $1 \leq i \leq t$. Furthermore we assume that we have chosen this

reduction of v such that the respective norms of the head coefficients of the h_i for $i \in \{1, \ldots, t\}$ are as small as possible. In particular we demand that there is no other representation of v which contains an h' with $HM(h') = HM(h_i)$ and $|HC(h')| <_S |HC(h_t)|$.

The claim is certainly satisfied if $t = 1$. Also if $t > 1$ and $HC(h_1) = HC(h_t)$ it follows that $HC(v)$ must be a multiple of $HC(h_1)$. So we assume that $t > 1$ and $|HC(h_1)| >_S |HC(h_t)|$. By assumption on the set H we know that $\mathfrak{g}\text{-pol}(h_1, h_t) \xrightarrow[S]{H}{}^{*} 0$ for all such $\mathfrak{g}$-polynomials. So there must exist $\widetilde{h}_1, \ldots, \widetilde{h}_m \in H$ such that

$$\widetilde{g} := \mathfrak{g}\text{-pol}(h_1, h_t) = \sum_{j=1}^{m} \nu_j \cdot \widetilde{h}_j$$

We have formed $\widetilde{g} = s_1 \cdot h_1 + s_2 \cdot h_t$, where $s_1, s_2 \in S$ such that $s_1 \cdot HC(h_1) + s_2 \cdot HC(h_t) = \mathrm{GCD}(HC(h_1), HC(h_t))$, so $\widetilde{g}$ is contained in the S-module $\langle h_1, h_t \rangle_S$.

However, $v = \sum_{i=1}^{t+k} \lambda_i \cdot h_i$ can also be written as

$$v = (\lambda_1 - s_1) \cdot h_1 + \sum_{i=2}^{t-1} \lambda_i \cdot h_i + (\lambda_t - s_2) \cdot h_t + \sum_{j=t+1}^{t+k} \lambda_j \cdot h_j + \sum_{\iota=1}^{m} \nu_\iota \cdot \widetilde{h}_\iota.$$

The summands on the right hand side of this equation provide a valid reduction sequence of v to 0 as well.

Now suppose that $|HC(\widetilde{g})| <_S |HC(h_t)|$. It follows that $|HC(\widetilde{h}_j)| <_S |HC(h_t)|$ for all $\widetilde{h}_j$ which reduce $\widetilde{g}$. However, this is a contradiction to the assumption that the reduction had been chosen in a way such that the norms of the head coefficients of the h_i with $1 \leq i \leq t$ are as small as possible with respect to the ordering $\leq_S$.

Therefore we can conclude that $HC(\widetilde{g}) = HC(h_t)$ and this implies that $HC(h_1)$ is a multiple of $HC(h_t)$. This argument can be applied to all h_i with $i \in \{1, \ldots, t-1\}$, and it follows that $HC(v)$ must be a multiple of $HC(h_t)$. □

Lemma 3.1.9 *Let $H \subset \Sigma$ be a finite set such that for every pair of elements $h, h' \in H$ it is ensured that $\mathfrak{g}\text{-pol}(h, h') \xrightarrow[S]{H}{}^{*} 0$. Let $v \in \Sigma, v \neq 0$, if*

v is minimal with respect to H then no summand $\lambda \cdot b.w$ of v is contained in the S-module $\langle HT(H)\rangle_S$.

Proof. Suppose there is a summand $\lambda \cdot b.w \neq 0$ of v which is contained in $\langle HT(H)\rangle_S$. Then

$$\lambda \cdot b.w = \lambda_1 \cdot HT(h_1) + \cdots + \lambda_t \cdot HT(h_t).$$

We shall prove the claim by induction on the number t of summands of the sum above. Suppose $t = 1$, then $\lambda \cdot b.w = \lambda_1 \cdot HT(h_1)$ and the claim follows.

Let $t = 2$, then $\lambda \cdot b.w = \lambda_1 \cdot HT(h_1) + \lambda_2 \cdot HT(h_2)$. We know that every $\mathfrak{g}$-polynomial of h_1 and h_2 must be S-module reducible to 0. Let $\widetilde{g} = \mathfrak{g}\text{-pol}(h_1, h_2) = \kappa_1 \cdot h_1 + \kappa_2 \cdot h_2$ with $\kappa_1, \kappa_2 \in S$. Since $HC(\widetilde{g}) = GCD(HC(h_1), HC(h_2))$ there exist $\mu_1, \mu_2 \in S$ with $HC(h_i) = \mu_i \cdot HC(\widetilde{g})$ for $i \in \{1, 2\}$. Accordingly $\lambda \cdot b.w = (\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot HT(\widetilde{g})$. Since $\widetilde{g}$ is S-module reducible to 0 by H it follows that $\lambda \cdot b.w$ must be S-module reducible by H as well.

So suppose that the assumption has been shown for $t = n - 1$; we set $t = n$. Therefore $\lambda \cdot b.w = \sum_{i=1}^{n} \lambda_i \cdot HT(h_i)$. Without loss of generality we form a $\mathfrak{g}$-polynomial of h_1 and h_2:

$$\widetilde{g} := \mathfrak{g}\text{-pol}(h_1, h_2) = s_1 \cdot h_1 + s_2 \cdot h_2;$$

By assumption, $\widetilde{g} \xrightarrow[S]{H}{}^{*} 0$ and we can conclude that $\widetilde{h} \in H$ and $\kappa \in S$ exist such that $HC(\widetilde{g}) = \kappa \cdot HC(\widetilde{h})$. Moreover there are $\mu_1, \mu_2 \in S$ with $HC(h_i) = \mu_i \cdot HC(\widetilde{g}) = \mu_i \cdot \kappa \cdot HC(\widetilde{h})$ for $i \in \{1, 2\}$.

So

$$\lambda \cdot b.w = \sum_{i=1}^{n} \lambda_i \cdot HT(h_i) = \sum_{i=1}^{n-1} \alpha_i \cdot HT(\widetilde{h}_i)$$

where

- $\alpha_1 := (\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot \kappa$ for $i \in \{1, 2\}$;
- $\alpha_i := \lambda_{i+1}$ for $2 \leq i \leq n - 1$;
- $\widetilde{h}_1 := \widetilde{h}$ and $\widetilde{h}_i := h_{i+1}$ for $2 \leq i \leq n - 1$;

and so the claim follows by induction. □

The converse of the Lemma above is only true in a modified form. By definition, an element $v_1 \in \Sigma$ can be S-module reduced by an element h if two conditions are satisfied: firstly we demand that there is a summand $\lambda \cdot b.w$ of v_1 such that $HM(h) = b.w$; secondly we must have that $|HC(h)| \leq_S |\lambda|$. This second condition does not necessarily require that the coefficient λ at the summand of v_1 is a multiple of $HC(h)$. Therefore if h S-module reduces v_1 to an element v_2 then it is possible that the term $b.w$ is a summand of v_2 as well, then with a coefficient $|\kappa'| <_S |\lambda|$ such that $\lambda = \kappa \cdot HC(h) + \kappa'$ where $|\kappa'| <_S |HC(h)|$.

Corollary 3.1.10 *Let $H \subset \Sigma$ be a finite set such that $\mathfrak{g}$-pol$(h, h') \xrightarrow[S]{H}{}^{*} 0$ for all $h, h' \in H$. Let $v \in \Sigma$, $v \neq 0$; suppose that for any summand $\lambda \cdot b.w$ of v for which $b.w \in HM(H)$ there exists no $\lambda' \in S$ with $|\lambda'| \leq_S |\lambda|$ and $\lambda' \cdot b.w \in \langle HT(H) \rangle_S$. Then v is minimal with respect to H.*

We now give the definition of an S-module Gröbner basis and we shall proceed by investigating certain properties of such Gröbner bases.

Definition 3.1.11 *Let Ξ be a submodule of the S-module Σ. We call a set of elements $G = \{g_1, \ldots, g_t\} \subset \Xi$ an* **S-module Gröbner basis of Ξ** *if for every $v \in \Xi, v \neq 0$, there exists an element $g_i \in G$ such that:*

1. *$HM(v) = HM(g_i)$, and*
2. *$|HC(v)| \geq_S |HC(g_i)|$ such that there are $\kappa, \kappa' \in S$ with $HC(v) = \kappa \cdot HC(g_i) + \kappa'$ such that*
   - *(a) $|\kappa \cdot HC(g_i)| \leq_S |HC(v)|$, and*
   - *(b) $|\kappa'| <_S |HC(g_i)|$.*

Lemma 3.1.12 *Let $G = \{g_1, \ldots, g_t\} \subset \Xi$ be an S-module Gröbner basis of Ξ_S. Then G generates Ξ.*

Proof. Let $v \in \Xi, v \neq 0$, there exists a sequence of reductions

$$v \xrightarrow[S]{G} \widetilde{v}_1 \xrightarrow[S]{G} \cdots \xrightarrow[S]{G} \widetilde{v}_k \xrightarrow[S]{G} \overline{v}$$

such that $\overline{v}$ is minimal with respect to G. Then $v - \overline{v}$ is contained in the S-linear span of G and, as $G \subset \Xi$, also $\overline{v} \in \Xi$. The set G is an S-module Gröbner basis for Ξ_S, it follows that $\overline{v} = 0$ and therefore v must be contained in the S-linear span of G. □

Lemma 3.1.13 *Let Ξ be a submodule of Σ and let $H = \{h_1, \ldots, h_t\}$ be a set of elements of Σ which generates Ξ. Then the following are equivalent:*

1. *The set H is an S-module Gröbner basis for Ξ.*
2. *Let $v \in \Sigma$ and $v \neq 0$, then $v \in \Xi$ if and only if $v \xrightarrow[S]{H}{}^{*} 0$.*

Proof. " 1. $\Longrightarrow$ 2. ": Suppose that $v \in \Xi$ such that $v \neq 0$. Then v can be reduced by H to an element $\overline{v}$ that is minimal with respect to H. Since $v - \overline{v} = \lambda_1 \cdot h_{i_1} + \cdots + \lambda_m \cdot h_{i_m} \in \Xi$ it follows that $\overline{v} \in \Xi$ as well. Then $\overline{v}$ cannot be further reduced by the S-module Gröbner basis H and it follows that $\overline{v} = 0$.

Now suppose that $v \xrightarrow[S]{H}{}^{*} 0$. Then there exists a sequence of reductions

$$v \xrightarrow[S]{H} \widetilde{v}_1 \xrightarrow[S]{H} \cdots \xrightarrow[S]{H} \widetilde{v}_k \xrightarrow[S]{H} 0,$$

and therefore v must lie in the S-linear span of H. It follows that $v \in \Xi$.

" 2. $\Longrightarrow$ 1. ": Let $v \in \Xi$ and $v \neq 0$. By assumption $v \xrightarrow[S]{H}{}^{*} 0$, induced by this reduction sequence there exist $\lambda_1, \ldots, \lambda_t \in S$ such that

$$v = \lambda_1 \cdot h_1 + \cdots + \lambda_t \cdot h_t$$

where we must have $|HM(h_i)| \leq_S |HM(v)|$ for all h_i with $\lambda_i \neq 0$. As v gets reduced to 0 there must exist a non-empty subset $\{h_{i_1}, \ldots, h_{i_m}\} \subset H$ which reduces $HT(v)$. Therefore $HM(h_{i_j}) = HM(v)$ for h_{i_j} with $1 \leq j \leq m$. Again it follows from the argument that the h_{i_j} are S-module reducing v that $|HC(h_{i_j})| \leq_S |HC(v)|$. We can conclude that H is an S-module Gröbner basis. □

Corollary 3.1.14 *Let Ξ be a submodule of a free S-module Σ which is generated by a finite S-module Gröbner basis G and let $v \in \Xi$ which can be S-module reduced by G to an element $\overline{v}$ that is minimal with respect to G. Then $\overline{v} = 0$.*

Corollary 3.1.15 *Let Ξ be a submodule of a free S-module Σ which is generated by the finite set G. If G is an S-module Gröbner basis then for all $\mathfrak{s}$-polynomials $\mathfrak{s}$-pol (g_1, g_2) of elements $g_1, g_2 \in G$ we have that*

$$\mathfrak{s}\text{-}pol(g_1, g_2) \xrightarrow[S]{G}{}^{*} 0.$$

Proof. Suppose there is $v := \mathfrak{s}$-pol $(g_1, g_2) \neq 0$ which cannot be S-module reduced to 0 by G. Then v is an element of Ξ which is minimal with respect to G. It follows that there is no $g \in G$ such that $HM(v) = HM(g)$ and also $|HC(v)| \geq_S |HC(g)|$. This is a contradiction to the assumption that G is a Gröbner basis and therefore we must have $v = 0$. □

Corollary 3.1.16 *Let Ξ be a submodule of a free S-module Σ which is generated by the finite set G. If G is an S-module Gröbner basis then for all $\mathfrak{g}$-polynomials $\mathfrak{g}$-pol (g_1, g_2) of elements $g_1, g_2 \in G$ we have that*

$$\mathfrak{g}\text{-}pol(g_1, g_2) \xrightarrow[S]{G}{}^{*} 0.$$

We shall now present a theorem which, in a different setting, was proved by Buchberger in the case of polynomial rings $k[x_1, \ldots, x_n]$ where k is a field. We translate this theorem to the setting of finitely generated modules over a Euclidean domain S and the proof here follows the ideas of the proof of the Buchberger Theorem as it has been presented by T. Becker and V. Weispfenning in [5]. This theorem shows that it can be seen directly if a set H is an S-module Gröbner basis from the property of $\mathfrak{s}$-polynomials and $\mathfrak{g}$-polynomials of $h, h' \in H$ of being S-module reducible by H.

Theorem 3.1.17 [Buchberger's Theorem in [5], p. 457] *Let Ξ be a submodule of the free S-module Σ and let H be a finite generating set*

of Ξ *such that for all* $h, h' \in H$ *we have* $\mathfrak{s}$*-pol*$(h, h') \xrightarrow[S]{H}{}^{*} 0$ *and also* $\mathfrak{g}$*-pol*$(h, h') \xrightarrow[S]{H}{}^{*} 0$. *Then* H *forms an* S*-module Gröbner basis of* Ξ.

Proof. Let $v \in \Xi, v \neq 0$, since H generates Ξ, v can be written as a linear combination of elements of H. We shall assume that v cannot be S-module reduced to 0. We shall divide the proof into two parts. In the first part we shall suppose that $v = \sum_{i=1}^{m} \lambda_i \cdot h_i$ where $HM(v) = \max_{1 \leq i \leq t}\{HM(h_i)\}$ but that $|HC(v)| <_S |HC(h_i)|$ for all $i \in \{1, \ldots, t\}$. In the second part we shall assume that the head monomials of the summands h_i cancel so that $HM(v) < \max\{HM(h_i)\}$.

(1) : We proceed by induction on the number of summands h_i of v with $HM(h_i) = HM(v)$. There is nothing to show if $n = 1$, so we begin with the case $n = 2$ and without loss of generality we suppose that the summands are ordered such that $HM(v) = HM(h_1) = HM(h_2)$. By assumption, $\widetilde{g} := \mathfrak{g}$-pol$(h_1 h_2) \xrightarrow[S]{H}{}^{*} 0$. It follows from Lemma 3.1.8 that there exist $\widetilde{h} \in H$ and $\kappa, \mu_1, \mu_2 \in S$ such that $HM(\widetilde{h}) = HM(\widetilde{g})$ and $\kappa \cdot HC(\widetilde{h}) = HC(\widetilde{g})$, and $\mu_i \cdot HC(\widetilde{h}) = HC(h_i)$ for $i \in \{1, 2\}$.

It follows that $HM(\mu_i \cdot \widetilde{h} - h_i) < HM(h_i)$ and the element $(\mu_i \cdot \widetilde{h} - h_i)$ for $i \in \{1, 2\}$ is of the form of an $\mathfrak{s}$-polynomial of $\widetilde{h}$ with h_1 and h_2 respectively. By assumption we have that all such $\mathfrak{s}$-polynomials must reduce to 0,

$$\mathfrak{s}\text{-pol}(\widetilde{h}, h_i) \xrightarrow[S]{H}{}^{*} 0,$$

and as $HM(\mu_i \cdot \widetilde{h} - h_i) < HM(h_i)$ for $i \in \{1, 2\}$ we also must have that

$$\mathfrak{s}\text{-pol}(\widetilde{h}, h_i) \xrightarrow[S]{H \setminus \{h_1, h_2\}}{}^{*} 0.$$

Therefore we can write $\mu_1 \cdot \widetilde{h} - h_1 = \sum_{j=1}^{l} \nu_j \cdot h'_j$ and $\mu_2 \cdot \widetilde{h} - h_2 = \sum_{j'=1}^{l'} \nu'_{j'} \cdot h''_{j'}$ where $HM(h'_j) < HM(h_1)$ and $HM(h''_{j'}) < HM(h_2)$ for all summands h'_j and $h''_{j'}$. We obtain

$$v = \lambda_1 \cdot (\mu_1 \cdot \widetilde{h} - \sum_{j=1}^{l} \nu_j \cdot h'_j) + \lambda_2 \cdot (\mu_2 \cdot \widetilde{h} - \sum_{j'=1}^{l'} \nu'_{j'} \cdot h''_{j'}) + \sum_{i=3}^{m} \lambda_i \cdot h_i =$$

$$(\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot \widetilde{h} - \lambda_1 \cdot (\sum_{j=1}^{l} \nu_j \cdot h'_j) - \lambda_2 \cdot (\sum_{j'=1}^{l'} \nu'_{j'} \cdot h''_{j'}) + \sum_{i=3}^{m} \lambda_i \cdot h_i.$$

So the only summand which has a head monomial equal to $HM(v)$ remaining on the right hand side is $\widetilde{h}$. It follows that $HC(v) = (\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot HC(\widetilde{h})$. Therefore $HM(v) = HM(\widetilde{h})$ and $|HC(\widetilde{h})| \leq_S |HC(v)|$ and it follows that v is S-module reducible by H.

By induction hypothesis, the assumption holds for $n = t-1$, so if we have $h_1, \ldots, h_{t-1}$, where $t-1 \leq m$, such that $HM(h_i) = HM(v)$ for $1 \leq i \leq t-1$ then there is $\widetilde{h}$ with $HM(\widetilde{h}) = HM(v)$ and $|HC(\widetilde{h})| \leq_S |HC(v)|$.

So let $n = t$: we set $v = \sum_{i=1}^{m} \lambda_i \cdot h_i$ and without loss of generality we order the sum such that $HM(h_i) = HM(v)$ for $i \in \{1, \ldots, t\}$ where $t \leq m$. Again, $\mathfrak{g}\text{-pol}(h_j, h_k) \xrightarrow[S]{H}{}^{*} 0$ for all respective $\mathfrak{g}$-polynomials of all $h_j, h_k \in H$. We set $\widetilde{g} := \mathfrak{g}\text{-pol}(h_1, h_2)$, since $\widetilde{g}$ can be S-module reduced to 0 by H it follows from Lemma 3.1.8 that an element $\widetilde{h} \in H$ exists such that $HC(\widetilde{g}) = \kappa \cdot HC(\widetilde{h})$ with $\kappa \in S$. We can proceed similar to the case of $n = 2$ and obtain $\mu_1, \mu_2 \in S$ with $\mu_1 \cdot HC(\widetilde{h}) = HC(h_1)$ and $\mu_2 \cdot HC(\widetilde{h}) = HC(h_2)$. So again we have $v = \sum_{i=1}^{t} \lambda_i \cdot h_i + \sum_{t+1}^{m} \lambda_i \cdot h_i$. This is equal to

$$\lambda_1 \cdot (\mu_1 \cdot \widetilde{h} - \sum_{j=1}^{l} \nu_j \cdot h'_j) + \lambda_2 \cdot (\mu_2 \cdot \widetilde{h} - \sum_{j'=1}^{l'} \nu'_{j'} \cdot h''_{j'}) + \sum_{i=3}^{t} \lambda_i \cdot h_i + \sum_{t+1}^{m} \lambda_i \cdot h_i;$$

and the last expression can be written as follows

$$(\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot \widetilde{h} + \sum_{i=3}^{t} \lambda_i \cdot h_i - \lambda_1 \cdot (\sum_{j=1}^{l} \nu_j \cdot h'_j) - \lambda_2 \cdot (\sum_{j'=1}^{l'} \nu'_{j'} \cdot h''_{j'}) + \sum_{t+1}^{m} \lambda_i \cdot h_i.$$

Accordingly we obtain a sum with $t-1$ summands which have $HM(v)$ as their respective head monomial, namely $\widetilde{h}$ and the summands of $\sum_{i=3}^{t} \lambda_i \cdot h_i$. Therefore we can apply the induction hypothesis and the assumption follows.

(2) : We shall now construct a contradiction by assuming that head monomials of the summands $h_i \in H$ cancel. So let again

$$v = \sum_{i=1}^{m} \lambda_i \cdot h_i;$$

and we suppose that $HM(v) \neq \max\{HM(h_i) \mid 1 \leq i \leq m\}$. We set

$$b_{max} := \max\{HM(h_i) \mid 1 \leq i \leq m\}$$

as minimal among the maximal head monomials of all such representations of v, we have $HM(v) < b_{max}$. In order to construct a contradiction we shall produce a representation

$$v = \sum_{j=1}^{t} \kappa_j \cdot \widetilde{h}_j$$

such that $b'_{max} := \max\{HM(\widetilde{h}_j) \mid 1 \leq j \leq t\} < b_{max}$.

We proceed by induction on the number n of indices i with $b_{max} = HM(h_i)$. The case $n = 1$ is not possible in the case that the head monomials cancel. So let $n = 2$, without loss of generality we assume that $HM(h_1) = HM(h_2) = b_{max}$. Then we must have $\kappa_1 \cdot HC(h_1) = -\kappa_2 \cdot HC(h_2)$ with $\kappa_1, \kappa_2 \in S$ and so there must exist $\mu \in S$ such that

$$\mu \cdot LCM((HC(h_1), HC(h_2)) = \kappa_1 \cdot HC(h_1) = -\kappa_2 \cdot HC(h_2).$$

It follows that

$$\kappa_1 \cdot h_1 + \kappa_2 \cdot h_2 = \mu \cdot \mathfrak{s}\text{-pol}(h_1, h_2)$$

for some $\mathfrak{s}$-polynomial $\mathfrak{s}$-pol(h_1, h_2) of h_1 and h_2.

By assumption on the set H, every $\mathfrak{s}$-polynomial can be S-module reduced to 0 by H and so we must have

$$\mathfrak{s}\text{-pol}(h_1, h_2) = \sum_{\iota=1}^{l} \widetilde{\lambda}_\iota \cdot h_\iota.$$

Accordingly we can write v as follows:

$$v = \sum_{i=3}^{m} \lambda_i \cdot h_i + \mu \cdot (\sum_{\iota=1}^{l} \widetilde{\lambda}_\iota \cdot h_\iota).$$

The maximum of the head monomials occuring in the first sum is smaller than b_{max}, this follows from the assumption that $n = 2$. The maximum $\widetilde{b}_{\max}$ of the head monomials in the second sum satisfies $\widetilde{b}_{max} < b_{max}$ and we see that the maximum b'_{max} of the summands of both sums must satisfy $b'_{max} < b_{max}$, therefore this is the representation of v we were looking for.

Now let $n > 2$. We assume without loss of generality that $HM(h_1) = HM(h_2) = b_{max}$. We set $\widetilde{g} := \mathfrak{g}\text{-pol}(h_1, h_2)$ for some $\mathfrak{g}$-polynomial of h_1 and

h_2. Since $\widetilde{g} \xrightarrow[S]{H}{}^{*} 0$, there exists $\widetilde{h} \in H$ such that $HM(\widetilde{h}) = HM(h_1) = HM(h_2)$ and $HC(\widetilde{g})$ is a multiple of $HC(\widetilde{h})$.

Since $b_{max} = HM(h_1) = HM(h_2)$ we also have that $HM(\widetilde{h}) = b_{max}$, moreover there must exist $\nu_1, \nu_2 \in S$ such that $HT(h_1) = \nu_1 \cdot HT(\widetilde{h})$ and $HT(h_2) = \nu_2 \cdot HT(\widetilde{h})$. We can modify the representation of v as follows:

$$v = \lambda_1 \cdot (h_1 - \nu_1 \cdot \widetilde{h}) + \lambda_2 \cdot (h_2 - \nu_2 \cdot \widetilde{h}) + (\lambda_1 \cdot \nu_1 + \lambda_2 \cdot \nu_2) \cdot \widetilde{h} + \sum_{i=3}^{m} \lambda_i \cdot h_i.$$

The head monomials of h_1 and $\widetilde{h}$ cancel, and so do the head monomials of h_2 and $\widetilde{h}$, so in these terms the maximal head monomial must be smaller than b_{max}. In the remaining $m-1$ summands, the highest head monomial b_{max} occurs at most $n-1$ times: there are exactly $n-2$ occurances in $\sum_{i=3}^{m} \lambda_i \cdot h_i$, and the summand $(\lambda_1 \cdot \nu_1 + \lambda_2 \cdot \nu_2) \cdot \widetilde{h}$ contributes at most one occurance. So we can apply the induction hypothesis and we have a representation of v, such as $v = \sum_{j=1}^{t} \kappa_j \cdot \widetilde{h}_j$, where $b'_{max} = \max\{HM(\widetilde{h}_i) \mid 1 \leq j \leq t\} < b_{max}$. □

Lemma 3.1.18 *Let Ξ be a submodule of the free S-module Σ and let $H = \{h_1, \ldots, h_t\}$ be an S-module Gröbner basis of Ξ. Then there is an equality of S-modules*

$$\langle HT(H) \rangle_S = \langle HT(\Xi) \rangle_S.$$

Proof. The set H generates Ξ, therefore for $v \in \Xi$ with $v \neq 0$ we have $v = \sum_{i=1}^{t} \lambda_i \cdot h_i$, then $v \xrightarrow[S]{H}{}^{*} 0$. Therefore we can apply Lemma 3.1.8 and it follows that there is $h \in H$ and $\kappa \in S$ such that $HM(h) = HM(v)$ and $HC(v) = \kappa \cdot HC(h)$. Therefore $HT(v) \in HT(H)$.

On the other hand, the set H generates the module Ξ, thus $H \subset \Xi$. Hence we can conclude that $HT(H) \subset HT(\Xi)$ and the equality of the respective S-modules follows. □

Corollary 3.1.19 *Let $H = \{h_1, \ldots, h_t\}$ be an inter-reduced set generating the S-module $\Xi \subset \Sigma$. Then H is an S-module Gröbner basis of Ξ.*

Proof. Let $v \in \Xi$ with $v \neq 0$, then $v = \sum_{i=1}^{t} \lambda_i \cdot h_i$. As the head monomials of the elements of H cannot cancel each other we must have $HM(v) = \max\{HM(h_i) \mid \lambda_i \neq 0\}$. Set $h_k \in H$ such that $HM(h_k) = \max\{HM(h_i) \mid \lambda_i \neq 0\}$. Then $HC(v) = \lambda_k \cdot HC(h_k)$ and by Definition 3.1.11 H is an S-module Gröbner basis of Ξ. □

Proposition 3.1.20 *If there exists an S-module Gröbner basis for a submodule Ξ of the free S-module Σ then there also exists an S-module Gröbner basis of Ξ that is inter-reduced.*

Proof. Let G denote the S-module Gröbner basis, suppose that $b_m \in HM(G)$ and let n denote the greatest number of $g \in G$ with $HM(g) = b_m$ for all $g \in G$.

In the case that $n = 1$ there is nothing to show; so let $n = 2$. Let $g_1, g_2 \in G$ with $HM(g_1) = HM(g_2) = b_m$, without loss of generality we suppose that $|HC(g_1)| \leq_S |HC(g_2)|$. Since G is an S-module Gröbner basis we know for all $\mathfrak{g}$-polynomials of g_1 and g_2 that $\mathfrak{g}\text{-pol}(g_1, g_2) \xrightarrow[S]{G}{}^{*} 0$. We abbreviate $\widetilde{g} := \mathfrak{g}\text{-pol}(g_1, g_2)$ for one such $\mathfrak{g}$-polynomial. Then $HC(\widetilde{g}) = GCD(HC(g_1), HC(g_2))$, and as $\widetilde{g} \xrightarrow[S]{G}{}^{*} 0$ there exist $g' \in G$ and $\kappa \in S$ such that $HM(g') = HM(\widetilde{g})$ and $HC(\widetilde{g}) = \kappa \cdot HC(g')$. Since there are exactly two elements $g_1, g_2 \in G$ with $HM(g_1) = HM(g_2) = b_m$ it follows that $g' = g_1$ and $\kappa = 1$. Therefore $HC(g_2)$ must be a multiple of $HC(g_1)$, so there exists $\mu \in S$ with $\mu \cdot HC(g_1) = HC(g_2)$. It follows that $HM(g_2 - \mu \cdot g_1) < HM(g_2)$ and since G is a Gröbner basis, $g_2 - \mu \cdot g_1 \xrightarrow[S]{G}{}^{*} 0$ and accordingly $g_2 - \mu \cdot g_1 \xrightarrow[S]{G\setminus\{g_2\}}{}^{*} 0$. Therefore $g_2 - \mu \cdot g_1$ is contained in the S-module $\langle G\setminus\{g_2\}\rangle_S$, since $g_1 \in \langle G\setminus\{g_2\}\rangle$ as well it follows that

$$g_2 \in \langle G\setminus\{g_2\}\rangle_S.$$

Moreover, $g_2 \xrightarrow{g_1} g_2 - \mu \cdot g_2 \xrightarrow{G\setminus\{g_2\}} 0$ and this implies that $G\setminus\{g_2\}$ is an S-module Gröbner basis of Ξ as well.

We suppose that an inter-reduced S-module Gröbner basis can be obtained from an S-module Gröbner basis where there are at most $n = t - 1$ elements $g_i \in G$ with $HM(g_1) = \cdots = HM(g_{t-1}) = b_m$.

So let $n = t$, there are $g_1, \ldots g_t \in G$ with $HM(g_i) = b_m$ for all $i \in \{1, \ldots, t\}$ and $b_m \in HM(G)$. Without loss of generality we assume again that $|HC(g_1)| \leq_S |HC(g_2)|$, again we set $\widetilde{g} := \mathfrak{g}\text{-pol}(g_1, g_2)$. Since $\widetilde{g} \xrightarrow[S]{G}{}^{*} 0$ there exists $g' \in G, \kappa \in S$ with $HM(g') = HM(\widetilde{g})$ and $HC(\widetilde{g}) = \kappa \cdot HC(g')$. Since $HC(g_2)$ is a multiple of $HC(\widetilde{g})$ there must then also exist a $\mu \in S$ such that $HC(g_2) = \mu \cdot HC(g')$. Again, $HM(g_2 - \mu \cdot g_1) < HM(g_2)$ and $g_2 - \mu \cdot g' \xrightarrow{G\setminus\{g_2\}}{}^{*}_{S} 0$.

Again we can conclude that g_2 is contained in the S-module $\langle G\setminus\{g_2\}\rangle_S$ and from $g_2 - \mu \cdot g' \xrightarrow{G\setminus\{g_2\}}{}^{*}_{S} 0$ it follows $g_2 \xrightarrow{G\setminus\{g_2\}}{}^{*}_{S} 0$ as well. So we obtain a set $G\setminus\{g_2\}$ which has the same S-linear span as G and which is an S-module Gröbner basis where there are only $n = t - 1$ elements $g_i \in G$ with $HM(g_i) = b_m$ and so the claim follows. □

Theorem 3.1.21 *Let Ξ be a finitely generated submodule of the free S-module Σ. Then there exists a finite S-module Gröbner basis for Ξ.*

Proof. By assumption the ring S is a Euclidean domain and therefore in particular it is a principal ideal domain (PID). It is a general theorem (see for instance [19]) that a finitely generated and torsion-free S-module is a free S-module if S is a PID.

Since Ξ is a submodule of a free S-module Σ it follows that Ξ must be torsion-free and therefore, as Ξ is finitely generated by assumption, Ξ is free. Let $b = \{b_1, \ldots, b_n\}$ be a basis of Ξ and let $H = \{h_i\}_{i \in I}$ be a basis of Σ. Then $b_j = \sum_{i \in I} \lambda_{ij} \cdot h_i$ where $\lambda_{ij} \in S$ and where we have $\lambda_{ij} \neq 0$ only for finitely many λ_{ij}. We take all $h_i \in H$ which are a summand of some $b_j \in B$ such that $\lambda_{ij} \neq 0$. This gives a finite set $\{h_1, \ldots, h_t\}$ and we set $\Phi := \langle h_1, \ldots, h_t\rangle_S$ as the S-module generated by this set.

Since $b_j \in \Phi$ for all $b_j \in B$ we have that Ξ is a submodule of Φ. Also, the set $HT(\Xi)$ is contained in Φ and therefore the S-module $\langle HT(\Xi)\rangle_S$ is a submodule of Φ. Being a submodule of a finitely generated module over a Euclidean domain, $\langle HT(\Xi)\rangle_S$ is finitely generated itself, so there exists a finite set of elements of Φ, $E = \{e_1, \ldots, e_m\} \subset HT(\Xi)$ such that $\langle E\rangle_S = \langle HT(\Xi)\rangle_S$.

As S-module reduction of an element $e \in E$ by elements $e_i \in E\backslash\{e\}$ does not change the S-linear span of the set E, we can choose instead an inter-reduced set $E' = \{e'_1, \ldots, e'_\mu\}$. Then for $e' \in E'$ we have that $e' = e - (\lambda_1 \cdot e_1 + \ldots \lambda_m \cdot e_m) = HT(v) - (\lambda_1 \cdot HT(v_1) + \ldots \lambda_m \cdot HT(v_m))$ for $v, v_i \in \Xi$. Since Φ is free, $e' = HT(v')$ for some element $v' \in \Xi$ and we can choose a set $G = \{g_1, \ldots, g_\mu\}$ of elements of Ξ such that $HT(g_i) = e'_i$ for all $g_i \in G$.

Let $v \in \Xi, v \neq 0$, then $HT(v) \in \langle HT(G)\rangle_S$ and since G is inter-reduced there must exist $g \in G$ and $\lambda \in S$ such that $HM(v) = HM(g)$ and $HC(v) = \lambda \cdot HC(g)$. It follows from Definition 3.1.11 that the set G forms a finite S-module Gröbner basis for Ξ. □

3.2 Prefix Gröbner Bases of A-Modules

We shall describe prefix Gröbner bases for free A-modules. Eventually we shall establish relationships between these kinds of prefix Gröbner bases and certain routines of the MGE-procedure. Connections between Gröbner bases and the Todd-Coxeter algorithm have been described by B. Reinert in [36] and by B. Reinert, T. Mora, and K. Madlener in [37, 38]. Prefix Gröbner bases in the case of monoid and groups rings have been extensively studied by B. Reinert et. al. in [34, 35].

3.2.1 Prefix Reduction

As before we denote by A a finitely generated and free S-algebra. Therefore A, regarded as S-module, is generated by the elements of a finitely generated and free monoid X^*. The free S-module $\Sigma = \langle BX^*\rangle$ can be considered as the A-module closure of the finitely generated S-module $\langle B\rangle$, so it has an A-module structure as well. We will again use ordering by weight on the elements of Σ.

Definition 3.2.1 *Let $v_1, v_2 \in \Sigma$ and let $H = \{h_1, \ldots, h_t\} \subset \Sigma$. We say*

that H **prefix-reduces** v_1 **to** v_2 **in one step**, *denoted by* $v_1 \xrightarrow[p]{H} v_2$, *if*

$$v_2 = v_1 - (\kappa_1 \cdot h_1.w_1 + \cdots + \kappa_t \cdot h_t.w_t),$$

where $w_i \in X^*, \kappa_i \in S$ *and* $\kappa_i \neq 0$ *for at least one* $i \in \{1, \ldots, t\}$. *For* $h_j \in H$ *with* $\kappa_j \neq 0$ *the following conditions have to hold:*

1. $HM(h_j.w_j) = b.w$ *for a summand* $\lambda \cdot b.w$ *of* v_1.
2. *Let* λ *denote the coefficient of the summand* $b.w$. *We demand that there are* $\kappa, \kappa' \in S$ *with* $\lambda = \kappa \cdot HC(h_j) + \kappa'$ *where*
   (a) $|\kappa \cdot HC(h_j.w_j)| \leq_S |\lambda|$; *and*
   (b) $|\kappa'| <_S |HC(h_j)|$.

We say that H **prefix-reduces** v_1 **to** v_2, *denoted by* $v_1 \xrightarrow[p]{H}{}^* v_2$, *if there exists a sequence of reductions*

$$v_1 \xrightarrow[p]{H} \widetilde{v}_1 \xrightarrow[p]{H} \ldots \xrightarrow[p]{H} \widetilde{v}_k \xrightarrow[p]{H} v_2$$

with $\widetilde{v}_i \in \Sigma$. *We call an element* v **prefix-minimal** *with respect to the set* H *if* v *cannot be prefix-reduced by* H. *We call a set* H **prefix inter-reduced** *if every* $h_i \in H$ *is prefix-minimal with respect to* $H \setminus \{h_i\}$.

Lemma 3.2.2 *Let* $v_1, v_2, h \in \Sigma$. *If* v_1 *can be prefix-reduced by* h *to* v_2 *then* $v_1 \succ_{wei} v_2$.

Proof. Certainly $HT(h) \succ_{wei} RED(h)$ and, as Σ is free, $HT(h.w) = HT(h).w \succ_{wei} RED(h).w = RED(h.w)$. Therefore

$$v_2 = v_1 - \kappa \cdot h.w = v_1 - \kappa \cdot HT(h.w) + \kappa \cdot RED(h.w)$$

and it follows that $v_1 \succ_{wei} v_2$. □

3.2.2 Prefix Gröbner Bases

Definition 3.2.3 *Let $h_1, h_2 \in \Sigma$ and $w_1, w_2 \in X^*$ such that $HM(h_1).w_1 = HM(h_2).w_2$ and $\lambda_1 \cdot HC(h_1) = \lambda_2 \cdot HC(h_2)$ for $\lambda_1, \lambda_2 \in S$. We define a* **prefix $\mathfrak{s}$-polynomial of h_1 and h_2** *as follows:*

$$\mathfrak{s}\text{-}pol(h_1, h_2, w_1, w_2) := \lambda_1 \cdot h_1.w_1 - \lambda_2 \cdot h_2.w_2.$$

Definition 3.2.4 *Let $h_1, h_2 \in \Sigma$ and $w_1, w_2 \in X^*$ such that $HM(h_1).w_1 = HM(h_2).w_2$ and let $\kappa_1, \kappa_2 \in S$ such that $GCD(HC(h_1), HC(h_2)) = \kappa_1 \cdot h_1 + \kappa_2 \cdot h_2$. We define a* **prefix $\mathfrak{g}$-polynomial of h_1 and h_2** *as follows:*

$$\mathfrak{g}\text{-}pol(h_1, h_2, w_1, w_2) := \kappa_1 \cdot h_1.w_1 + \kappa_2 \cdot h_2.w_2.$$

Remark 3.2.5 *Since we are working with modules that are free we only need to consider those cases where $w_i = \varepsilon$ for at least one $i \in \{1, 2\}$.*

Lemma 3.2.6 *Let $v \in \Sigma$ and let $H \subset \Sigma$ denote a finite set such that*

$$\mathfrak{g}\text{-}pol(h, h', w_1, w_2) \xrightarrow[p]{H}{}^{*} 0$$

for all respective $\mathfrak{g}$-polynomials of all $h, h' \in H$. If $v \xrightarrow[p]{H}{}^{*} 0$ then there exist $h'' \in H$ and $\kappa \in S$ such that $HM(h'') = p]_{HM(v)}$ and $HC(v) = \kappa \cdot HC(h'')$.

Proof. The proof of this lemma essentially follows the proof of Lemma 3.1.8. Let $v \in \Upsilon$ and $v \neq 0$. If $v \xrightarrow[p]{H}{}^{*} 0$ then

$$v = \sum_{i=1}^{m} h_i \cdot \sum_{j=1}^{k(i)} \lambda_{ji}.w_{ji}$$

and $HM(v) = \max\{HM(h_i.w_{ji}) \mid 1 \leq i \leq m, 1 \leq j_i \leq k(i)\}$. Since v can be prefix reduced to 0 by H there must be a subset of all summands $h_i.w_{ji}$ for which we have that $HM(v) = HM(h_i.w_{ji})$. We denote these elements by $\mathfrak{E} = \{\mathfrak{e}_1, \ldots, \mathfrak{e}_t\}$; so $HM(\mathfrak{e}_\iota) = HM(v)$ for all $\mathfrak{e}_\iota \in \mathfrak{E}$. Note, since Σ is a free module, that each h_i can appear at most once as the prefix of some element $\mathfrak{e}_\iota$ in the set $\mathfrak{E}$.

We can write

$$v = \sum_{\iota=1}^{t} \kappa_\iota \cdot \mathfrak{e}_\iota + \sum_{i'=1}^{m'} h_{i'} \cdot \sum_{j'=1}^{k'(i')} \lambda_{j'i'}.w_{j'i'}$$

where the κ_ι are equal to the respective coefficients λ_{ji} in the representation of v further above, and where we have removed those summands $\lambda_{ji} \cdot h_i.w_{ji}$ that are equal to some $\mathfrak{e}_\iota$. Without loss of generality we suppose that the $\mathfrak{e}_\iota$ have been arranged such that

$$|HC(\mathfrak{e}_1)| \geq_S |HC(\mathfrak{e}_2)| \geq_S \cdots \geq_S |HC(\mathfrak{e}_t)|.$$

Furthermore we assume that this representation of v in terms of elements of H has been chosen in a way that the norms of the head coefficients of $\mathfrak{e}_\iota \in \mathfrak{E}$ are minimal. In particular we demand that there is no other representation of v which contains $h' \in H$ with $HM(h'.w_{ji}) = HM(v)$ and $|HC(h')| <_S |HC(\mathfrak{e}_t)|$.

We suppose again that $t > 1$ and $|HC(\mathfrak{e}_1)| >_S |HC(\mathfrak{e}_t)|$; let

$$\widetilde{g} := \mathfrak{g}\text{-pol}(\mathfrak{e}_1, \mathfrak{e}_t, w, w')$$

for some prefix $\mathfrak{g}$-polynomial of $\mathfrak{e}_1$ and $\mathfrak{e}_t$. Since $HM(\mathfrak{e}_1) = HM(\mathfrak{e}_t)$ we can choose $\widetilde{g}$ such that $w = w' = \varepsilon$. The assumption on H implies that $\widetilde{g} \xrightarrow[p]{H}{}^{*} 0$, so there must exist $\widetilde{h}_1, \ldots, \widetilde{h}_l \in H$ with

$$\widetilde{g} = \sum_{d=1}^{l} \widetilde{h}_d \cdot \sum_{\sigma=1}^{\tau(d)} \mu_{\sigma d}.w_{\sigma d}$$

The $\mathfrak{g}$-polynomial $\widetilde{g}$ has been formed as $s_1 \cdot \mathfrak{e}_1 + s_2 \cdot \mathfrak{e}_t$ where $s_1 \cdot HC(\mathfrak{e}_1) + s_2 \cdot HC(\mathfrak{e}_t) = GCD(HC(\mathfrak{e}_1), HC(\mathfrak{e}_t))$. Accordigly, v is equal to the following sum:

$$(\kappa_1 - s_1)\cdot\mathfrak{e}_1 + \sum_{\iota=2}^{t-1} \kappa_\iota \cdot \mathfrak{e}_\iota + (\kappa_t - s_2)\cdot\mathfrak{e}_t + \sum_{i'=1}^{m'} h_{i'} \cdot \sum_{j'=1}^{k'(i')} \lambda_{j'i'}.w_{j'i'} + \sum_{d=1}^{l} \widetilde{h}_d \cdot \sum_{\sigma=1}^{\tau(d)} \mu_{\sigma d}.w_{\sigma d}$$

Similar to the proof of Lemma 3.1.8 we can now conclude that $HC(\widetilde{g}) = HC(\mathfrak{e}_t)$ and that we must have $HC(\widetilde{g}_i) = HC(\mathfrak{e}_t)$ for all such $\mathfrak{g}$-polynomials

$\widetilde{g}_i = \mathfrak{g}\text{-pol}(\mathfrak{e}_i, \mathfrak{e}_t, w, w')$. Therefore it follows that $HC(v)$ must be a multiple of $HC(\mathfrak{e}_t)$. □

Lemma 3.2.7 *Let $H \subset \Sigma$ be a finite set such that for every pair of elements $h, h' \in H$ it is ensured that $\mathfrak{g}\text{-pol}(h, h', w_1, w_2) \xrightarrow[p]{H}{}^{*} 0$. Let $v \in \Sigma, v \neq 0$, if v is prefix-minimal with respect to H then no summand of v is contained in the A-module closure $(\langle HT(H)\rangle)_A$ of the S-module generated by the head terms of H.*

The proof of this lemma follows the same concept as the proof of Lemma 3.1.9 where we replace S-module reduction by prefix reduction.

Corollary 3.2.8 *Let $v \in \Sigma$ and let $H \subset \Sigma$. If v is prefix-minimal with respect to the set H then it is minimal with respect to H as well.*

Definition 3.2.9 *Let $G = \{g_1, \ldots, g_t\}$ be a set of elements of Σ and let $\Upsilon \subset \Sigma$ denote the A- module closure of a finitely generated submodule Ξ_S of Σ. We call G a* **prefix Gröbner basis** *of Υ if for every $v \in \Upsilon$, $v \neq 0$, there exists a prefix $p]_{HM(v)}$ of $HM(v)$, and an element $g_i \in G$ such that*

1. *$p]_{HM(v)} = HM(g_i)$, and*
2. *$|HC(v)| \geq |HC(g_i)|$ such there are $\kappa, \kappa' \in S$ with $HC(v) = \kappa \cdot HC(g_i) + \kappa'$ such that*
   (a) *$|\kappa \cdot HC(g_i)| \leq_S |HC(v)|$, and*
   (b) *$|\kappa'| <_S |HC(g_i)|$.*

Lemma 3.2.10 *Let $G = \{g_1, \ldots, g_t\} \subset \Upsilon := (\Xi)_A$ be a prefix Gröbner basis of the A-module closure Υ of an S-module Ξ. Then G generates Υ.*

The proof of this Lemma follows the proof of Lemma 3.1.12. We now choose an element $v \in \Upsilon, v \neq 0$, and we replace S-module reduction by prefix reduction.

Lemma 3.2.11 *Let Ξ_S be a finitely generated submodule of Σ, generated by the set $H = \{h_1, \ldots, h_t\}$, and let Υ denote the A-module closure of Ξ. Then the following are equivalent:*

1. *The set H is a prefix Gröbner basis for Υ.*
2. *Let $v \in \Sigma$ and $v \neq 0$, then $v \in \Upsilon$ if and only if $v \xrightarrow[p]{H}{}^{*} 0$.*

The proof of this lemma follows the same idea as the proof of Lemma 3.1.13. Again we replace the terminology of S-module reduction and S-module Gröbner bases with that of prefix reduction and prefix Gröbner bases.

Corollary 3.2.12 *Let Υ denote the A-module closure of $\Xi_S \subset \Sigma$. We suppose that Υ is generated by a finite prefix Gröbner basis G. Let $v \in \Upsilon, v \neq 0$, if v can be prefix reduced by G to an element $\overline{v}$ that is prefix minimal with respect to G then $\overline{v} = 0$.*

Corollary 3.2.13 *Let Ξ_S be a submodule of Σ that is generated by a finite set G. If the A-linear span of G forms a prefix Gröbner basis of $\Upsilon := (\Xi)_A$, then*

$$\mathfrak{s}\text{-}pol\ (g_1, g_2, w_1, w_2) \xrightarrow[p]{G}{}^{*} 0.$$

for all $\mathfrak{s}$-polynomials of $g_1, g_2 \in G$ and words $w_1, w_2 \in X^*$.

Corollary 3.2.14 *Let Ξ_S be a submodule of Σ that is generated by a finite set G. If the A-linear span of G forms a prefix Gröbner basis of $\Upsilon := (\Xi)_A$, then*

$$\mathfrak{g}\text{-}pol\ (g_1, g_2, w_1, w_2) \xrightarrow[p]{G}{}^{*} 0.$$

for all $\mathfrak{g}$-polynomials of $g_1, g_2 \in G$ and words $w_1, w_2 \in X^*$.

Theorem 3.2.15 [Buchberger's Theorem] *Let Ξ_S be a submodule of Σ that is generated by a finite set H and let Υ denote the A-linear span of Ξ_S. We suppose that $\mathfrak{s}\text{-}pol(h, h', w_1, w_2) \xrightarrow[p]{H}{}^{*} 0$ and $\mathfrak{g}\text{-}pol(h, h', w_1, w_2) \xrightarrow[p]{H}{}^{*} 0$ for all $h, h' \in H$ and $w_1, w_2 \in X^*$. Then the set H forms a prefix Gröbner basis of Υ.*

Proof. The proof of this Theorem is similar to the proof of Theorem 3.1.17, we follow again the proof given by T. Becker and V. Weispfenning in [5]. Let $v \in \Upsilon$, $v \neq 0$, as H is an A-module generating set of Υ, we have

$$v = \sum_{i=1}^{m} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji}.$$

We shall assume that v cannot be prefix reduced to 0 by elements of H. We again divide the proof into two parts, in the first part we assume that $HM(v) = \max\{HM(h_i).w_{ji} \mid 1 \leq i \leq m, 1 \leq j_i \leq z(i)\}$ but that $|HC(v)| <_S |HC(h_i.w_{ji})|$ for all such $h_i.w_{ji}$. In the second part we shall assume that the head monomials cancel so that

$$HM(v) < \max\{HM(h_i).w_{ji} \mid 1 \leq i \leq m, 1 \leq j_i \leq z(i)\}.$$

Note that if two head monomials cancel as summands of v than one head monomial must have been a prefix of the other.

(1) : We use induction on the number n of those $h_i.w_{ji}$ that are non-zero as summand of v such that $HM(h_i.w_{ji}) = HM(v)$. Let $n = 2$; without loss of generality we assume that $HM(h_1).w_{1,1} = HM(h_2).w_{1,2} = HM(v)$. We set $\mathfrak{e}_1 := h_1.w_{1,1}$ and $\mathfrak{e}_2 := h_2.w_{1,2}$. Let $\widetilde{g} := \mathfrak{g}\text{-pol}(\mathfrak{e}_1, \mathfrak{e}_2, \varepsilon, \varepsilon)$ for some prefix $\mathfrak{g}$-polynomial of $\mathfrak{e}_1$ and $\mathfrak{e}_2$. Since $\widetilde{g} = \mathfrak{g}\text{-pol}(h_1, h_2, w_{1,1}, w_{2,1})$ for some prefix $\mathfrak{g}$-polynomial of h_1 and h_2, it follows from the assumption on the set H that $\widetilde{g} \xrightarrow[p]{H}{}^{*} 0$. Therefore there exist $\widetilde{h} \in H$ and $\kappa, \mu_1, \mu_2 \in S$ and $\widetilde{w} \in X^*$ such that $HM(\widetilde{h}).\widetilde{w} = HM(\widetilde{g})$(where certainly $HM(\widetilde{g}) = HM(\mathfrak{e}_1) = HM(\mathfrak{e}_2)$); and moreover $\kappa \cdot HC(\widetilde{h}) = HC(\widetilde{g})$, $\mu_1 \cdot HC(\widetilde{h}) = HC(\mathfrak{e}_1)$, and $\mu_2 \cdot HC(\widetilde{h}) = HC(\mathfrak{e}_2)$.

Accordingly, $HM(\mu_i \cdot \widetilde{h}.\widetilde{w} - \mathfrak{e}_i) < HM(\mathfrak{e}_i)$ for $i \in \{1, 2\}$, and $(\mu_i \cdot \widetilde{h}.\widetilde{w} - \mathfrak{e}_i)$ is of the form of a prefix $\mathfrak{s}$-polynomial of $\widetilde{h}$ with $\mathfrak{e}_1$ and $\mathfrak{e}_2$, respectively. Again by assumption on H, all prefix $\mathfrak{s}$-polynomials of elements of H must be prefix reducible to 0 by H. Therefore we can write the respective elements as sums

- $\mu_1 \cdot \widetilde{h}.\widetilde{w} - \mathfrak{e}_1 = \sum_{d=1}^{l} h'_d \cdot \sum_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d}$, and
- $\mu_2 \cdot \widetilde{h}.\widetilde{w} - \mathfrak{e}_2 = \sum_{d'=1}^{l'} h'_{d'} \cdot \sum_{\varphi'=1}^{k'(d')} \nu_{\varphi' d'}.w_{\varphi' d'}$.

We can insert the above into the representations of v, thus

$$\begin{aligned} v &= \lambda_1 \cdot \big(\mu_1 \cdot \widetilde{h}.w - \sum\nolimits_{d=1}^{l} h'_d \cdot \sum\nolimits_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d} + h_1 \sum\nolimits_{j_1=2}^{z(1)} \lambda_{j_1}.w_{j_1}\big) \\ &\quad + \lambda_2 \cdot \big(\mu_2 \cdot \widetilde{h}.w - \sum\nolimits_{d'=1}^{l'} h''_{d'} \cdot \sum\nolimits_{\varphi'=1}^{k'(d')} \nu_{\varphi' d'}.w_{\varphi' d'} + h_2 \sum\nolimits_{j_2=2}^{z(2)} \lambda_{j_2}.w_{j_2}\big) \\ &\quad + \sum\nolimits_{i=3}^{m} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \\ &= (\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot \widetilde{h}.w - \lambda_1 \cdot \big(\sum\nolimits_{d=1}^{l} h'_d \cdot \sum\nolimits_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d}\big) \\ &\quad - \lambda_2 \cdot \big(\sum\nolimits_{d'=1}^{l'} h''_{d'} \cdot \sum\nolimits_{\varphi'=1}^{k'(d')} \nu_{\varphi' d'}.w_{\varphi' d'}\big) + \lambda_1 \cdot h_1 \sum\nolimits_{j_1=2}^{m(1)} \lambda_{j_1}.w_{j_1} \\ &\quad + \lambda_2 \cdot h_2 \sum\nolimits_{j_2=2}^{m(2)} \lambda_{j_2}.w_{j_2} + \sum\nolimits_{i=3}^{m} h_i \sum\nolimits_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \end{aligned}$$

So $\widetilde{h}.w$ must be the only summand such that $HM(\widetilde{h}.w) = HM(v)$, accordingly we have found $\widetilde{h} \in H$ with $HM(\widetilde{h}) = p]_{HM(v)}$ and $|HC(\widetilde{h})| \leq_S |HC(v)|$.

By induction there are $t-1$ summands in the representation of v with $HM(v) = HM(h_1.w_{1,1}) = HM(h_2.w_{1,2}) = \cdots = HM(h_{t-1}.w_{1,t-1})$ and there does exist $\widetilde{h} \in H$ with $HM(\widetilde{h}) = p]_{HM(v)}$ and $|HC(\widetilde{h})| \leq_S |HC(v)|$.

So let $n = t$: we have

$$v = \sum_{i=1}^{m} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji},$$

and without loss of generality we suppose that the sum is ordered such that $HM(h_1.w_{1,1}) = HM(h_2.w_{1,2}) = \cdots = HM(h_t.w_{1,t}) = HM(v)$; again we set $\mathfrak{e}_i := h_i.w_{1,i}$. We choose $h_1.w_{1,1}$ and $h_2.w_{1,2}$ and we set $\widetilde{g} :=$ $\mathfrak{g}$-pol$(h_1, h_2, w_{1,1}, w_{1,2})$ for a prefix $\mathfrak{g}$-polynomial of h_1 and h_2. As $\widetilde{g} \xrightarrow[p]{H}{}^{*} 0$ there exist $\widetilde{h} \in H$ and $\kappa \in S$ with $HM(\widetilde{h}) = p]_{HM(\widetilde{g})}$ and $HC(\widetilde{g}) = \kappa \cdot HC(\widetilde{h})$.

We proceed similar to the case $n = 2$, thus we let $\mu_1, \mu_2 \in S$ such that $\mu_i \cdot HC(\widetilde{h}) = HC(h_i)$ for $i \in \{1, 2\}$. We can write

$$\begin{aligned}
v &= \sum_{i=1}^{t} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} + \sum_{i=t+1}^{m} h_i \cdot \sum_{i=t+1}^{m} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \\
&= \lambda_1 \cdot \big(\mu_1 \cdot \widetilde{h}.w - \sum_{d=1}^{l} h'_d \cdot \sum_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d} + h_1 \sum_{j_1=2}^{z(1)} \lambda_{j_1}.w_{j_1}\big) \\
&\quad + \lambda_2 \cdot \big(\mu_2 \cdot \widetilde{h}.w - \sum_{d'=1}^{l'} h''_{d'} \cdot \sum_{\varphi'=1}^{k'(d')} \nu_{\varphi' d'}.w_{\varphi' d'} + h_2 \sum_{j_2=2}^{z(2)} \lambda_{j_2}.w_{j_2}\big) \\
&\quad + \sum_{i=3}^{t} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \sum_{i=t+1}^{m} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \\
&= (\lambda_1 \cdot \mu_1 + \lambda_2 \cdot \mu_2) \cdot \widetilde{h}.w - \lambda_1 \cdot \big(\sum_{d=1}^{l} h'_d \cdot \sum_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d}\big) \\
&\quad - \lambda_2 \cdot \big(\sum_{d'=1}^{l'} h''_{d'} \cdot \sum_{\varphi'=1}^{k'(d')} \nu_{\varphi' d'}.w_{\varphi' d'}\big) + \lambda_1 \cdot h_1 \sum_{j_1=2}^{m_1} \lambda_{j_1}.w_{j_1} \\
&\quad + \lambda_2 \cdot h_2 \sum_{j_2=2}^{m_2} \lambda_{j_2}.w_{j_2} + \sum_{i=3}^{m} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji}
\end{aligned}$$

Since Σ is free, we can have at most one j in a sum $h_i.\sum_{j_i=1}^{z_i} \lambda_{j_i}.w_{j_i}$ such that $HM(h_i.w_{j_i}) = HM(v)$ for each $1 \leq i \leq t$. It follows that therefore no such summands can be contained in $h_1.\sum_{j_1=2}^{z(1)} \lambda_{j_1}.w_{j_1}$ and in $h_2.\sum_{j_2=2}^{z(2)} \lambda_{j_2}.w_{j_2}$.

Moreover, the representation of v has been chosen such that no summand of $\sum_{i=t+1}^{m} h_i.\sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji}$ contains such a head monomial, and as $\sum_{d=1}^{l} h'_d \sum_{\varphi=1}^{k(d)} \nu_{\varphi d} w_{\varphi d}$ and $\sum_{d'=1}^{l'} h''_{d'} \sum_{\varphi'=1}^{k'(d')} \nu_{\varphi' d'}.w_{\varphi' d'}$ are representations of prefix $\mathfrak{s}$-polynomials of $\widetilde{h}.w$ with $\mathfrak{e}_1$ and $\mathfrak{e}_2$, respectively, it follows that the maximal head monomials of any summands of these two sums must be smaller that $HM(v)$.

We can conclude that exactly $t - 1$ summands remain in this representation of v which are equal to $HM(v)$, and therefore the assumption follows by induction.

(2): We shall now construct a contradiction by assuming that some of the head monomials of summands of v cancel, such that we then obtain $HM(v) < \max\{HM(h_i.w_{ij}) \mid 1 \leq i \leq m, 1 \leq j_i \leq z(i)\}$. So suppose that

$HM(v) \neq \max\{HM(h_i.w_{ji})\}$ and we set

$$c_{max} := \max\{HM(h_i.w_{ji})\}.$$

We choose c_{max} as the minimal element among the maximal head monomials of all possible representations of v in terms of h_i, and we assume that $HM(v) < c_{max}$. We aim to construct a contradiction by producing a representation

$$v = \sum_{i'=1}^{m'} h'_{i'} \cdot \sum_{j'=1}^{z'(i')} \lambda'_{j'i'}.w'_{j'i'}$$

so that $c'_{max} := \max\{HM(h'_{i'}.w'_{j'i'})\} < c_{max}$.

We again proceed by induction on the number n of summands $h_i.w_{ji}$ with $HM(h_i.w_{ji}) = c_{max}$; so let $n = 2$. Without loss of generality we assume $HM(h_1.w_{1_1}) = HM(h_2.w_{1_2}) = c_{max}$. It follows that we must have $\lambda_{1_1} \cdot HC(h_1) = -\lambda_{1_2} \cdot HC(h_2)$ and also $HM(h_1.w_{1_1}) = HM(h_2.w_{1_2})$.

Accordingly, $\lambda_{1_1} \cdot HC(h_1)$ and $\lambda_{1_2} \cdot HC(h_2)$ must be multiples of the least common multiple of $HC(h_1)$ and $HC(h_2)$, say by a coefficient $\mu \in S$. We obtain a prefix $\mathfrak{s}$-polynomial $\widetilde{s}$ of $h_1.w_{1_1}$ and $h_2.w_{1_2}$:

$$\widetilde{s} := \lambda_{1_1} \cdot h_1.w_{1_1} + \lambda_{1_2} \cdot h_2.w_{1_2} = \mu \cdot \mathfrak{s}\text{-pol}(h_1.w_{1_1}, h_2.w_{1_2}, \varepsilon, \varepsilon).$$

Certainly we can choose a prefix $\mathfrak{s}$-polynomial of h_1 and h_2 such that $\widetilde{s} = \mu \cdot \mathfrak{s}\text{-pol}(h_1, h_2, w_{1_1}, w_{1_2})$, and by assumption on the set H we can prefix-reduce $\widetilde{s}$ to 0 by H, thus

$$\widetilde{s} = \mu \cdot \sum_{d=1}^{l} h'_d \cdot \sum_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d}.$$

Accordingly, we can write

$$\begin{aligned} v &= \textstyle\sum_{i=1}^{m} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \\ &= h_1 \cdot \textstyle\sum_{j_1=2}^{z(1)} \lambda_{j_1}.w_{j_1} + h_2 \cdot \sum_{j_2=2}^{z(2)} \lambda_{j_2}.w_{j_2} \\ &\quad + \textstyle\sum_{i=3}^{m} h_i \cdot \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} + \mu \cdot \sum_{d=1}^{l} h'_d \sum_{\varphi=1}^{k(d)} \nu_{\varphi d} w_{\varphi d} \end{aligned}$$

Since $h_1.w_{1_1} = h_2.w_{1_2} = c_{max}$ we must have that the maximal head monomials of the first two sums (so where $i = 1$ and $i = 2$) must be smaller than c_{max}. Also we did assume that there were exactly two such maximal head monomials and it follows that

$$\max\{HM(h_i.w_{j_i}) \mid 3 \leq i \leq m, 1 \leq j_i \leq z(i)\} < c_{max}.$$

There only remains $\mu \cdot \sum_{d=1}^{l} h'_d \sum_{\varphi=1}^{k(d)} \nu_{\varphi d}.w_{\varphi d}$, however, since this term has been constructed as the multiple of a prefix $\mathfrak{s}$-polynomial of $h_1.w_{1_1}$ and $h_2.w_{1_2}$, it follows that the maximal head monomial of all summands of this sum must be smaller than c_{max}. We can conclude that we have found a representation of v which has a maximal head monomial c'_{max} smaller than c_{max} as was intended.

Now let $n > 2$, again we assume without loss of generality that $c_{max} = HM(h_1.w_{1_1}) = HM(h_2.w_{1_2})$. We set $\widetilde{g} := \mathfrak{g}\text{-pol}(h_1.w_{1_1}, h_2.w_{1_2}, \varepsilon, \varepsilon)$ as a prefix $\mathfrak{g}$-polynomial of $h_1.w_{1_1}$ and $h_2.w_{1_2}$. As $\widetilde{g}$ is equal to a prefix $\mathfrak{g}$-polynomal $\mathfrak{g}\text{-pol}(h_1, h_2, w_{1_1}, w_{1_2})$, we know that $\widetilde{g} \xrightarrow[p]{H}{}^{*} 0$, and therefore there exist $\widetilde{h} \in H$, $w \in X^*$ and $\kappa \in S$ such that $HM(\widetilde{h}.w) = HM(h_1.w_{1_1}) = HM(h_2.w_{1_2})$ and $HC(\widetilde{g}) = \kappa \cdot HC(\widetilde{h})$.

Since $c_{max} = HM(h_1.w_{1_1}) = HM(h_2.w_{1_2})$ we also have that $HM(h.w) = c_{max}$, moreover there must exist $\mu_1, \mu_2 \in S$ with $HT(h_i.w_{1_i}) = \mu_i \cdot HT(\widetilde{h}.w)$ for $i \in \{1, 2\}$. We again modify the representation of v:

$$\begin{aligned}
v &= \sum_{i=1}^{m} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \\
&= h_1.\lambda_{1_1}.w_{1_1} + h_2.\lambda_{1_2}.w_{1_2} + h_1 \sum_{j_1=2}^{z(1)} \lambda_{j_1}.w_{j_1} \\
&\quad + h_2 \sum_{j_2=2}^{z(2)} \lambda_{j_2}.w_{j_2} + \sum_{i=3}^{m} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji} \\
&= \lambda_{1_1} \cdot (h_1.w_{1_1} - \mu_1 \cdot \widetilde{h}.w) + \lambda_{1_2} \cdot (h_2.w_{1_2} - \mu_2 \cdot \widetilde{h}.w) \\
&\quad + (\lambda_{1_1} \cdot \mu_1 + \lambda_{1_2} \cdot \mu_2) \cdot \widetilde{h}.w + \sum_{i=3}^{m} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji}
\end{aligned}$$

As $HT(h_i.w_{1_i}) = HT(\mu_i.\widetilde{h}.w)$ for $i = 1$ and $i = 2$, the head monomials of the first two terms, and the head monomials of the third and fourth summands

respectively, cancel each other. In the remaining sum $\sum_{i=3}^{m} h_i \sum_{j=1}^{z(i)} \lambda_{ji}.w_{ji}$ the maximal head monomial c_{max} can occur at most $n-2$ times, and the term $(\lambda_{1_1} \cdot \mu_1 + \lambda_{1_2} \cdot \mu_2) \cdot \widetilde{h}.w$ provides at most one summand equal to c_{max}. It follows that we can apply the induction hypothesis, and we can write v as

$$v = \sum_{i'=1}^{m'} \widetilde{h}_{i'} \cdot \sum_{j'}^{z'(i')} \kappa_{j'i'}.w'_{j'i'}$$

where we have a maximal head monomial

$$c'_{max} = \max\{HM(\widetilde{h}_{i'}.w'_{j'i'}) \mid 1 \leq i' \leq m', 1 \leq j'_{i'} \leq z'(i')\} < c_{max}.$$

□

3.2.3 Generator Prefix-Closure

Definition 3.2.16 *Let $H = \{h_1, \ldots, h_t\} \subset \Sigma$ be a finite set, suppose that there are $h_{k_1}, h_{k_2} \in H$ and $w \in X^*$ such that for their head monomials $HM(h_{k_1}).w = HM(h_{k_2})$ holds. We call the element $h_{k_1}.w$ the* **prefix-closure of h_{k_1} and h_{k_2}**. *We say that a set H is* **prefix-closed** *if for every pair $h_{k_1}, h_{k_2} \in H$ the prefix-closure is already contained in H.*

Lemma 3.2.17 *Let H be a finite set of the free S-module Σ. The process of prefix-closing H ends after a finite number of steps and the so obtained prefix-closed set must be finite as well.*

Proof. We suppose that for all $h \in H$ we have that $Wei(h) \leq n$. We will denote by $H_i := \{h_{j_1}, \ldots, h_{j_t}\}$ those subsets of H such that $Wei(h_{j_k}) = i$ for all $h_{j_k} \in H_i$.

We begin by adding the prefix-closure for all $h \in H$ with $Wei(h) \leq 1$. Suppose that there is a set $\{\widetilde{h}_{j_1}, \ldots \widetilde{h}_{j_l}\} \subset H_0$ such that $HM(\widetilde{h}_{j_k}).x = HM(h)$ for some $h \in H_1$ and $x \in X$. Accordingly, we will add elements $\widetilde{h}_{j_k}.x$ to H. By assumption on the given ordering, and since Σ is free, we have $HM(h_{j_k}).x = HM(h_{j_k}.x)$. Therefore the newly added elements do not lead to any further prefix-closures with elements of H_0. As H is finite

by assumption there can only be a finite number of such closures. After adding a finite number of elements we obtain a prefix-closed and finite set $\widetilde{H}_1 := H_0 \cup H_1$.

Suppose we are given a prefix-closed finite set $\widetilde{H}_{n-1} := H_0 \cup H_1 \cdots \cup H_{n-1}$. Let $\{h_{j_1}, \ldots, h_{j_m}\} \subset H_n$ be the subset (not necessarily proper) of elements of H_n such that for h_{j_k} there exist elements $h \in \widetilde{H}_{n-1}$ with $HM(h).w = HM(h_{j_k})$. As Σ is a free module such a word w is unique, so again we add a finite number of elements $h.w$ which yields a finite and prefix-closed set $\widetilde{H}_n$. □

Suppose that H is the finite generating set of a submodule Ξ of Σ and let $\widetilde{H}$ denote the set obtained by prefix-closing H. Generally, the S-modules generated by H and $\widetilde{H}$ are not equal. We can however show that the A-module closures of the respective S-modules are the same:

Lemma 3.2.18 *Let H be a finite set of elements of Σ and let $\widetilde{H}$ denote the set we obtain by prefix-closing H. Then $\langle H \rangle_A = \langle \widetilde{H} \rangle_A$.*

Proof. Since $H \subset \widetilde{H}$ it follows that $\langle H \rangle_A \subset \langle \widetilde{H} \rangle_A$. On the other hand, let $\widetilde{h} \in \widetilde{H} \setminus H$. Then $\widetilde{h} = h_k.w$ for some $h_k \in H$ and $w \in X^*$, therefore $\widetilde{h} \in \langle H \rangle_A$. □

Proposition 3.2.19 *Let Ξ be a finitely generated S-submodule of Σ. Then an S-module Gröbner basis which is also prefix-closed for the S-module Ξ' with $(\Xi)_A = (\Xi')_A$ can be obtained by a finite number of steps.*

Proof. Let H denote the generating set of Ξ and we set $\widetilde{h} \in H$ as that element of H such that

$$HM(\widetilde{h}) := \max\{HM(h) \mid h \in H\}.$$

Constructing an $\mathfrak{s}$-polynomial of elements $h_1, h_2 \in H$ possibly leads to extending the set H by an element h'. However, such an element h' has a head monomial which is always smaller than the respective head monomials of h_1 and h_2, but never greater. Thus at no point of adding elements in

order to obtain an S-module Gröbner basis will we add an element h' with $HM(h') > HM(\widetilde{h})$. Therefore we never exceed the given upper bound and it follows from Lemma 3.2.17 that the respective adding of prefix-closure elements must all be finite.

Certainly, the computing of an S-module Gröbner basis does not change the A-linear span of the given set; similarly, prefix-closure does not change the A-linear span. Therefore after a finite number of steps we will obtain a prefix closed S-module Gröbner basis $\widetilde{H}$ such that $(\langle \widetilde{H} \rangle)_A = (\Xi)_A$. □

Theorem 3.2.20 *Let H be a finite set of elements of Σ generating a submodule $\Xi \subset \Sigma$. If H is an S-module Gröbner basis for Ξ which is prefix-closed then H also is a prefix Gröbner basis for $(\Xi)_A$.*

Proof. Suppose that H is a prefix-closed S-module Gröbner basis which is not a prefix Gröbner basis for $(\Xi)_A$. It follows from Theorem 3.2.15 that there is either at least one prefix $\mathfrak{s}$-polynomial h' or at least one $\mathfrak{g}$-polynomial $\widetilde{h}$ of elements of H such that h' or $\widetilde{h}$ cannot be prefix-reduced to 0 by elements of H.

We shall first assume that there is such an $\mathfrak{s}$-polynomial and we set $h' := \mathfrak{s}\text{-pol}(h_1, h_2, w_1, w_2)$ for $h_1, h_2 \in$. As $(\Xi)_A$ is free, we can choose the $\mathfrak{s}$-polynomial so that at least one of the w_i is the empty word ε. Moreover, from the assumption that H is a prefix-closed set it even follows that $w_1 = w_2 = \varepsilon$. Otherwise, since $HM(h_i.w) = HM(h_i).w$ for all $h_i \in H$ and $w \in X^*$, the head monomial of one element must have been the prefix of the head monomial of the other. However, if $w_1 = w_2 = \varepsilon$, then the prefix $\mathfrak{s}$-polynomial above is in fact an S-module $\mathfrak{s}$-polynomial.

The same argument holds for a prefix $\mathfrak{g}$-polynomial $\widetilde{h}$ that cannot be prefix-reduced to 0. In both cases we obtain a contradiction to the assumption that H is an S-module Gröbner basis of Ξ. □

Corollary 3.2.21 *Let Ξ be a submodule of Σ and suppose that Ξ is finitely generated by an inter-reduced and prefix-closed set $H \subset \Sigma$. Then H is a prefix Gröbner basis of $(\Xi)_A$.*

Chapter 4

Correctness of the Procedures

In this chapter we will show the correctness of the MGE-procedure and of all the respective sub-routines needed. The chapter is divided into the following two sections.

Section 4.1: We give a brief outline of the procedure putting the emphasis on the technical side of the MGE-procedure. Thereafter we give descriptions in pseudo-code of the main procedures and routines used. We first give a description of those procedures which lead to definitions of S-module generators, then we explain those procedures which are concerned with the processing of the different cases of coincidences and finally we give a description of the main procedure.

Section 4.2: We show correctness of the respective procedures. We demonstrate how the multiplication table and the coincidences can be interpreted as generating sets of certain S-modules; to these generating sets, Gröbner basis techniques, as were introduced in Chapter 3, can be applied and we can deduce from these the correctness of the routines used.

4.1 Description of the Procedure

We shall describe the MGE-procedure again for a finitely generated P-module $\mathcal{M}$, generated by $Y' = \{y'_1, \ldots, y'_n\}$ with relations $U \subset \mathcal{F}_A$ and

where $P = \langle X \mid R \rangle$ is a finitely presented S-algebra with generating set $X = \{x_1 \ldots, x_t\}$.

Recall that we wish to construct a concrete finitely generated S-module $\Theta = \Theta_{(\nu)}$ which is compatible with the action of elements of X such that it is a P-module which is isomorphic to $\mathcal{M}$. As the MGE-procedure follows the ideas of the Todd-Coxeter procedure we aim to obtain information about the module Θ from the relations of $\mathcal{M}$.

The information about the action of the algebra-generators on the module generators $b \in B^u$ of Θ then will be stored in a multiplication table T. In the course of the procedure we will form a set of finitely generated free S-modules $\langle B^u \rangle_S$ together with mappings $\gamma : \mathcal{F} \longrightarrow \Sigma/(\Delta)_A$ and $\delta : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \Sigma/\Upsilon$. We shall assume in the following that $B = \{b_1, \ldots, b_m\}$. We construct Θ as a quotient-module of Σ by the submodule Υ. As before we will denote the product on Θ by the elements of X by "$\star$".

We will consider $\mathcal{M}$ as an A-module throughout the procedure, so the relations $Rels$ of $\mathcal{M}$ are elements of $\mathcal{F}$. The image $\delta(r) \in \langle B^u \rangle$ of an element $r \in Rels$, which must certainly be 0 as element of $\mathcal{M}$, provides the information that $\delta(r)$ must be 0 in Θ. Such elements $\delta(r)$ will be called *coincidences* and in the MGE-procedure we will store these in a stack. If however the ring S is not a field then the elements of S are not generally invertible. This possibly leads to coincidences which cannot be applied in the usual way. We shall store these so-called inapplicable coincidences in a sequence L, separate from the applicable coincidences which can be applied to the entries of the multiplication table immediately. We will use two different orderings on the elements of L. These specific orderings are needed for certain sub-routines of the MGE-procedure. We shall now give a description of the different routines in pseudo-code.

Before we describe the main-routine in pseudo-code we shall introduce subroutines needed and we shall give their respective descriptions in pseudo-code.

4.1.1 Definition Procedures

In the following procedure we are computing the image of an element $f.a$ for $f \in \mathcal{F}$ and $a \in A$ under $\delta : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \Sigma/\Upsilon$ such that $\delta(f.a) = \delta(f) \star a$ is contained in the finitely generated submodule $\langle B \rangle_S$ of Σ. We refer to an assignment of a new S-module-generator $b' \notin B$ to a product $b \star x$ as a *definition step* and, in terms of the actual procedure, such a step leads to an additional entry in the multiplication table T.

IMAGE1

We will begin with the simplest case, namely where $\delta(f) = b \in B^u$ and $a = x \in X$. In the case that $b \star x \notin \langle B \rangle_S$ this will lead to the definition of a new S-module generator $b' \notin B$. The input of the procedure includes a boolean variable *flag*. This variable indicates if we are allowed to deduce from $v = b \star x$ that $b = v \star x'$ and vice versa in the case that algebra-relations $xx' - 1$ and $x'x - 1$ are contained in the set R of algebra relations.

Image1 corresponds to an actual definition step of an S-module generator $b \in B^u$ with the algebra generator $x \in X$. As Image1 manipulates a multiplication table T, we will present the product "$b \star x$", when considered as an entry of the table, by prod(b, x). We suppose that the table is of length m at the begin of the routine Image1.

Input: $b \in B^u$, $x \in X$, *flag* $\in \{$*true, false*$\}$;
Output: prod$(b, x) = v \in \langle B^u \rangle_S$;

```
Begin
If prod(b, x) = ṽ ∈ ⟨B⟩ then        * prod(b, x) has been defined already *
   Return u(ṽ) ∈ ⟨B^u⟩_S;             * Replace ṽ by its undeleted image *
Else                                  * Extend the table by row m + 1 *
   v := b_{m+1};                                  * B := B ∪ {b_{m+1}} *
   T[m + 1] := Record(deleted = false, images = [ ],
         define := γ^{-1}(b_{m+1}));
   prod(b, x) := v;
   If flag then
      prod(b_{m+1}, x^{-1}) := b;
```

```
      Return v;
   Fi;
Fi;
End.
```

Remark 4.1.1 *A component of the record T which represents the table is the entry denoted by " define". This entry gives the preimage of the newly defined S-module generator b_{m+1} under the homomorphism γ. This preimage is an element of $\mathcal{F}$. We assume here that elements of the A-module $\mathcal{F}$ can be stored and represented by the computer. We will describe the handling of elements of $\mathcal{F}$ in the case of the implementation in GAP in greater detail in Chapter 7.*

IMAGE2

The routine Image2 has as input an element $v = \sum_{i=1}^{m} \lambda_i \cdot b_i$ where we assume that $\lambda_i \neq 0$ only if $b_i \in B^u$ such that $v \in \langle B^u \rangle_S$. We want to identify the product of v with $x \in X$ and Image2 can therefore lead to definition steps for more than one summand.

Input: $v = \sum_{i=1}^{m} \lambda_i \cdot b_i \in \langle B^u \rangle, x \in X$, *flag* $\in \{$*true, false*$\}$;
Output: $v' = v \star x$;
Begin
$v' := 0$;
For i such that b_i is summand of v with $\lambda_i \neq 0$ do
  $v_i :=$ IMAGE1$(b_i, x, flag)$;
  $v' := v' + v_i$;
Od;
Return v';
End.

Remark 4.1.2 *Note that in certain situations the procedure* IMAGE2 *for $v \star x$ will be called where "flag" is set to "false" even if x is invertible in the sense that there is $x' \in X$ together with algebra-relations $x.x' - 1$ and $x'.x - 1$. We suppose that a consequence $\widetilde{c}$ of a coincidence $c \in \langle B^u \rangle$ is being traced where $\widetilde{c} = c \star x$. In this situation we already must have for all*

summands b of $\widetilde{c}$ that $b \star x' \in \langle B^u \rangle$ and in fact $\widetilde{c} \star x'$ must be equal to the coincidence c. Therefore in this case the deduction $\widetilde{c} \star x'$ would not provide any new information.

IMAGE MODULE RELATION

The following routine computes the image under δ in Σ/Υ for a module relation $\omega \in U \subset \mathcal{F}$. Since $\omega = \sum_{i=1}^{n} \sum_{j=1}^{t} \lambda_{ij} \cdot y_i.w_{ij}$, we do not compute the product by $x \in X$ but by sums of words $w \in X^*$. As elements are replaced by the respective undeleted images, the output will consist of $\widetilde{v} \in \langle B^u \rangle$ such that $\widetilde{v} = \delta(\omega)$.

Input: $\omega \in U$;
Output: $\widetilde{v} \in \langle B^u \rangle$;

```
Begin
For ω ∈ U do                                   * ω = Σ_{i=1}^{n} Σ_{j=1}^{t} λ_ij · y_i.w_ij *
   ṽ := 0;
   For summand λ_ij · y_i.w_ij, λ_ij ≠ 0 do
      v_i := u(b_i);                           * b_i = γ(y_i) for y_i ∈ Y *
      For k ∈ [1..., l] do                     * Suppose w_ij = x_1 ... x_l *
         v_i := IMAGE2(v_i, x_k, flag);
      Od;
      ṽ := ṽ + v_i;
   Od;
Return ṽ;
End.
```

4.1.2 Coincidence Procedure

Coincidences represent relations of $\mathcal{M}$ in the terminology of S-modules. When a coincidence is being processed this means that information of possible S-linear dependencies of elements of Σ will be applied to the entries of the multiplication table T and possibly to the entries of the torsion sequence L as well. Since in the course of the procedure it might not be possible to process a coincidence immediately, coincidences, irrespective of

whether they are applicable or inapplicable, are stored in the coincidence stack Cp.

CLEARING COINCIDENCES

At certain stages of the main routine, CLEARING COINCIDENCES will be called: this procedure will process the coincidences pending in Cp and it will return when $Cp = \emptyset$.

Input: Cp;
Begin
While $Cp \neq \emptyset$ do
  Choose c from Cp;
  $Cp := Cp \backslash \{c\}$;
  $c := u(c)$;
  If $c \neq 0$ then
    PROCESSING A COINCIDENCE(c);
  Fi;
Od;
End

Remark 4.1.3 *Contrary to the elements contained in the torsion sequence L (if L has been initialised and is not empty) which are ordered by their respective head monomials, the elements of Cp are ordered only by the point of when they have been added to Cp. The elements of Cp are stored and processed by a "last–in, first–out" principle.*

In fact, the elements of L are coincidences which have already been processed and which have been found to be inapplicable. If a coincidence c cannot be processed by the MGE-procedure immediately after it has been detected then it is inserted into Cp directly without being investigated any further. While a coincidence is stored in Cp it will not be replaced by its undeleted image and as a consequence the list Cp possibly contains elements $c \notin \langle B^u \rangle$ or might also contain c_1, c_2 such that $u(c_1) = u(c_2)$. Accordingly it is possible that the undeleted image of a coincidence, while it is stored in Cp, actually becomes 0.

PROCESSING A COINCIDENCE (PRC)

A coincidence $c \in Cp$ has been chosen for processing. Depending on whether c is applicable or not, the procedure will either collect all possible consequences, which will be added to Cp, and apply the information contained in c to the elements of L (with APPLY COINCIDENCE TO TORSION SEQUENCE), or it will call the sub-procedure HANDLE INAPPLICABLE COINCIDENCE in order to deal with the inapplicable coincidence c and possibly insert it into L.

Input: A coincidence c, the table T, the torsion sequence L;

```
Begin
Let b_{m'} = HM(c);                          * c = sum_{i=1}^{m'} λ_i · b_i ∈ ⟨B^u⟩ *
If HC(c) is not unit of Ring S then
   HANDLE INAPPLICABLE COINCIDENCE(c);
Fi;
For x ∈ X do
   If prod(b_m, x) ∈ ⟨B⟩ then
      v := u(prod(b_m, x));
      ṽ :=IMAGE2(RED(c), x, false);
      c̃ := v − ṽ;
      If c̃ ≠ 0 then        * A consequence c̃ of c has been found *
         Cp := Cp ∪ {c̃};
      Fi;
   Fi;
Od;
B^d := B^d ∪ {b_{m'}}, B^u := B^u\{b_{m'}};
Replace b_{m'} by r_{b_{m'}} = HC(c)^{-1} · RED(c);
APPLY COINCIDENCE TO TORSION SEQUENCE(c);
Return;
End.
```

Remark 4.1.4 *The presented routines resemble the routines as they are implemented in GAP. The procedure* PROCESSING A COINCIDENCE *does not search the table T for entries $v = prod(b, x)$ which contain $b_{m'}$ as a summand*

in order to replace these immediately by their undeleted image. Instead, only if an entry v is subsequently used in the course of the computation will v be traced again and only then will it be replaced by its undeleted image $u(v)$. Towards the end of an MGE-computation when all necessary coincidences have been processed the table will be checked and every element which is not in its undeleted form will be updated. Therefore, whenever the procedure uses elements in a computation these will be in the desired minimal form.

HANDLE INAPPLICABLE COINCIDENCES (HIC)

This procedure is called when an inapplicable coincidence c has been found by the procedure PROCESSING A COINCIDENCE. With respect to the process of inserting inapplicable coincidences we order the elements of L by the index of their head monomials. In order to avoid oversights of any applicable coincidences possibly contained in the S-linear span of elements of $L = \{l_1, \ldots, l_k\}$, we shall maintain the elements of L in strict pivot form such that $HM(l_i) > HM(l_j)$ if $j > i$.

Therefore, if an inapplicable coincidence c has to get inserted into L, where $HM(c) = HM(l_i)$, we replace c and l_i by elements v_1, v_2 such that the S-linear span of c and l_i is the same as that of v_1 and v_2 but where $HM(v_1) \neq HM(v_2)$. For this we use the extended greatest common divisor which provides, in addition to the greatest common divisor $\mu = GCD(HC(l_i), HC(c))$, elements s_1, s_2 and t_1, t_2 such that $s_1 \cdot HC(l_i) + s_2 \cdot HC(c) = \mu$ and $t_1 \cdot HC(l_i) + t_2 \cdot HC(c) = 0$. We set

$$v_1 := s_1 \cdot l_i + s_2 \cdot c.$$

If $HC(v_1)$ is not a unit it will replace the entry l_i of L. Otherwise we will add v_1 to Cp and remove l_i from L. We set

$$v_2 := t_1 \cdot l_i + t_2 \cdot c.$$

Note that $HM(v_2) < HM(c)$. If $HC(v_2)$ is a unit then we will add v_2 to Cp, otherwise we will insert v_2 into L using the same procedure as before. Certainly $v_1, v_2 \in \langle B^u \rangle$ and we shall show in Lemma 4.2.8 that for the modules generated by the respective elements we have that

$$\langle v_1, v_2 \rangle_S = \langle l_i, c \rangle_S.$$

Input: An inapplicable coincidence v, L and Cp;
Output: $\widetilde{L}$ and $\widetilde{C}p$ such that $\langle L, Cp, v\rangle_S = \langle \widetilde{L}, \widetilde{C}p\rangle_S$;

```
Begin
v := u(v);                                   * Let v = Σ_{i=1}^{m} λ_i · b_i *
b_m = HM(v);
λ_m = HC(v);
C̃p := Cp;
If λ_m < 0 then
   v := −v;
Fi;
j := 1;
While j ≤ Length(L) do                       * Begin of Main-routine of HIC *
   If HM(L[j]) < b_m then
      Insert v into L at position j;
      Return;
   Elif HM(L[j]) = b_m then
      μ := GCD (HC(L[j]), λ_m);
      v_1 := s_1 · L[j] + s_2 · v;           * s_i : s_1 · HC(L[j]) + s_2 · λ_m = μ *
      v_2 := t_1 · L[j] + t_2 · v;           * t_i : t_1 · HC(L[j]) + t_2 · λ_m = 0 *
      If HC(v_1) is unit of S then
         C̃p := C̃p ∪ {v_1};
         L := L\{L[j]};
      Else
         L[j] := v_1;
         j := j + 1;
      Fi;
      v := v_2;                              * Begin routine for v_2 *
      If v = 0 then
         Return;
      Fi;
      b_m' := HM(v);
      If HC(v) is unit of S then
         C̃p := C̃p ∪ {v};
```

```
        Return;
    Fi;
Od;                                   * End of Main-routine *
Append v to L;
```
$\widetilde{L} := L;$
```
End.
```

Remark 4.1.5 *For the handling of the inapplicable coincidences, so firstly the insertion of new inapplicable elements into L and secondly, to close L with respect to the action of algebra-generators $x \in X$, we use two separate orderings on the elements of L. The ordering by head monomials of elements becomes necessary for the inserting of elements into L, as described above.*

For the procedure CLOSE TORSION SEQUENCE, *which ensures the A-module closure of elements of L, we need a seperate ordering. It has been found that applying* CLOSE TORSION SEQUENCE *to L using the ordering given by the head monomials might lead to infinite loops. The reason for this is that necessary information might be overseen since new entries with greater head monomials are added to the beginning of the list. This then might lead to the procedure dealing only with entries of L which are A-linearly dependent.*

This situation corresponds to a violation of the Mendelsohn Condition in Coset Enumeration; for a discussion on this condition see for instance [30] or [32]. Another discussion of this will be given in Section 7.1.

CLOSE TORSION SEQUENCE

Since the torsion elements are induced by A-module relations we know that under the action of A-module generators we must again obtain a torsion element. This procedure therefore adds for every $l \in L$ which has been contained in L at the beginning of the routine the A-module closure $l \star x$ to the coincidence stack Cp. In order to ensure correctness we apply this routine to the sequence I. This sequence contains exactly the same elements as L, however the elements of I are ordered by the point of when they have been inserted and will be dealt with by CLOSE TORSION SEQUENCE in a "first in

– first out" way.

Input: I;
Begin
$n :=$ Length(I);
For $j \in [1, \ldots n]$ do
  If not $I[j]$ closed with respect to "$\star$" for all $x \in X$ then
    For $x \in X$ do
      $v :=$ IMAGE2$(I[j], x, false)$;
      $Cp := Cp \cup \{v\}$;
    Od;
    CLEAR COINCIDENCES(Cp);
  Fi;
Od;
End.

CLEAN TORSION SEQUENCE

The following procedure uses the information on the torsion of elements of a module $\Theta_{(\iota)}$ in order to bring elements of L into a minimal form. Elements of L possibly consist of more than one summand. If $j > i$ then $HM(L[i]) > HM(L[j])$. If $RED(L[i])$ contains a summand $\lambda \cdot b$ such that $b = HM(L[j])$ where moreover $\lambda > HC(L[j])$ then we can replace the summand $\lambda \cdot b$ by the Euclidean remainder by $HT(L[j])$. In the case that $RED(L[j]) \neq 0$ this implies corresponding adjustments to other summands of $RED(L[i])$.

Input: L;
Begin
$n :=$ Length(L);
For $i := n - 1$ to 1 do * *Clean by cleaned elements* *
  For $j := i + 1$ to n do
    $q :=$EUCLIDEAN QUOTIENT$\big(HC(L[i]), HC(L[j])\big)$;
    If $q \neq 0$ then
      $L[i] := L[i] - q \cdot L[j]$;
    Fi;

```
   Od;
Od;
End.
```

APPLY COINCIDENCE TO TORSION SEQUENCE

The following routine is being called by PROCESSING A COINCIDENCE: when a coincidence $c \in Cp$ is processed it will be removed from Cp. We suppose that c is an applicable coincidence such that $c := u(c) \neq 0$ and let $b_m = HM(c)$; then c leads to deletion of $b_m \in B^u$. In order to ensure that we maintain the condition that $l \in \langle B^u \rangle$ for all $l \in L$ we check if b_m is contained as a summand of any $l \in L$ and then possibly replace such a l by its undeleted image $u(l)$.

Input: An applicable coincidence c, Cp and L;
$\widetilde{L}$ and $\widetilde{Cp}$ are produced such that $\widetilde{L} \subset \langle B^u \rangle_S$ and $\langle L, Cp \rangle_S = \langle \widetilde{L}, \widetilde{Cp} \rangle_S$;

```
Begin
For l ∈ L do
   If HM(c) is summand of l then
      If HM(l) = HM(c) then
         L̃ := L \ {l};
         C̃p := Cp ∪ {l};
      Else
         L̃ := (L\{l}) ∪ {u(l)};
      Fi;
   Fi;
Od;
End.
```

4.1.3 Main Procedure

The input of the main routine consists of finite descriptions of the module $\mathcal{M}_P$ and the algebra P and of an empty multiplication table $T_{(0)}$ which is of length n, the number of module generators of $\mathcal{M}_P$. At every stage of the

procedure the multiplication table gives a description of the S-module $\Theta_{(\iota)}$ which has been constructed so far and of its product "$\star$". The initial table corresponds to the free S-module with n generators.

Suppose that this main procedure terminates, say in a state (ν), and that the table has been closed. Then the output will consist of a finite number of generators $b \in B^u_{(\nu)}$ together with a multiplication table $T_{(\nu)}$, containing the product $b \star x \in \langle B^u \rangle_S$ for every pair $b \in B^u_{(\nu)}, x \in X$. The multiplication table then describes the action of the algebra-generators $x \in X$ on the S-module generators of the S-module $\Theta_{(\nu)} \cong \mathcal{M}$. Moreover, the sequence $L_{(\nu)}$ describes the torsion of $\Theta_{(\nu)}$ and we shall see that the elements of $L_{(\nu)}$ can be considered as a generating set of a submodule $\Lambda \subset \langle B^u \rangle$ and that $\Theta_{(\nu)} \cong \langle B^u \rangle_S / (\Lambda)_A$.

MAIN ROUTINE

Input: $\mathcal{M}, P_S$, a table $T_{(0)}$, $Cp_{(0)} = \emptyset$, if S not a field then $L_{(0)} := [\,]$;
Output: A table $T_{(\nu)}$, if S not a field then also a torsion sequence $L_{(\nu)}$;

```
Begin
For module-relations ω ∈ U do
   v := IMAGE MODULE RELATIONS(ω, flag);
   Cp := Cp ∪ {v};
   CLEAR COINCIDENCES(Cp);
Od;
i := 1;
While i ≤ Length(T) do
   If T[i].deleted = true then          * indicates that b_i ∈ B^d *
      i := i + 1;
   Else
      For r ∈ R do
         c := IMAGE2(b_i, r, flag);
         Cp := Cp ∪ {c};
      Od;
      CLEAR COINCIDENCES;
      If L ≠ ∅ then
```

```
            CLOSE TORSION SEQUENCE(L);
            CLEAN TORSION SEQUENCE(L);
        Fi;
        i := i + 1;
    Fi;
Od;
If L is not empty then
    While L ≠ ∅ do
        CLOSE TORSION SEQUENCE(L);
    Od;
CLEAN TORSION SEQUENCE(L);
Return T and L;
End.
```

4.2 Correctness of the Procedures

We will show correctness of the MGE-procedures by applying the Gröbner basis techniques which we developed in Chapter 3 to the S-modules and their A-module closures that will be constructed in the course of an MGE-procedure. We remind ourselves that we want to construct a P-module $\Theta_{(\nu)}$ that is finitely generated as S-module and that is P-module isomorphic to the given module $\mathcal{M}_P$. We aim to construct $\Theta_{(\nu)}$ as the quotient-module of the free module $\Sigma_{(\nu)}$ by a certain submodule $\Upsilon_{(\nu)}$. As before, we denote by Δ the submodule of Σ that is generated by those elements $b.x - b'$ which are induced by the definition steps of an MGE-procedure.

In the procedures themselves we are interested in coincidences $c \in \Sigma/\Upsilon$ such that we can be certain that $c = u(c)$. In order to relate the coincidences process in the theoretical description to reduction as it has been described in Chapter 3, we will consider coincidences as elements of $\Sigma/(\Delta)_A$. Thus we have that $c = \gamma(r)$ for some $r \in \mathit{Rels} \subset \mathcal{F}$ and $c \in \langle B^u \rangle$ does not have to hold necessarily. To such an element $c \in \Sigma/(\Delta)_A$ we assign an element $k \in \Sigma$ that is contained in the preimage of c under the canonical map

$\pi : \Sigma \longrightarrow\!\!\!\!\!\rightarrow \Sigma/(\Delta)_A$. Generally the choice of such a $k \in \Sigma$ is not canonical. We will now describe how we can in fact choose a mapping from $\Sigma/(\Delta)_A$ to Σ in a canonical way in the given situation.

Lemma 4.2.1 *Let H denote the finite generating set of Δ. The set H is a prefix inter-reduced prefix Gröbner basis of $(\Delta)_A$.*

Proof. By construction, the set H consists only of elements $h \doteq b.x - b'$ where $b, b' \in B$, so $HT(h) = b.x$, $RED(h) = b'$ and therefore $Wei\big(HT(h)\big) = 1$ and $Wei\big(RED(h)\big) = 0$. The head monomials of the elements of H are pair-wise different. It follows from the definition of elements contained in H that the head monomial of one element $h \in H$ cannot be a prefix of the head monomial or the reduct of another element $\widetilde{h} \in H\backslash\{h\}$ as this, in the first case, would imply that $Wei\big(HT(\widetilde{h})\big) > 1$, and in the second case that $Wei\big(RED(\widetilde{h})\big) > 0$. Thus the set H is prefix inter-reduced and in particular inter-reduced.

It follows from Corollary 3.1.19 that H is an S-module Gröbner basis for Δ which, for trivial reasons, is also prefix-closed. We can deduce from Theorem 3.2.20 that H is a prefix Gröbner basis for $(\Delta)_A$. □

As prefix-reduction of $v \in \Sigma$ by the elements of a prefix Gröbner basis leads to a canonical minimal element $\overline{v}$, we can assign to every congruence class $|v|$ modulo $(\Delta)_A$ in Σ a canonical representative minimal with respect to the ordering " $\succ_{wei}$ ". Accordingly, we can map every element $v + (\Delta)_A \in \Sigma/(\Delta)_A$ to the canonical representative $\overline{v} \in \Sigma$. This yields a map

$$\zeta : \Sigma/(\Delta)_A \longrightarrow \Sigma,$$

$$v + (\Delta)_A \overset{\zeta}{\longmapsto} \overline{v}.$$

Lemma 4.2.2 *The map $\zeta : \Sigma/(\Delta)_A \longrightarrow \Sigma$ is an S-module monomorphism.*

Proof. Since $HC(h_i) = 1$ for all $h_i \in H$, we have that $\zeta(\lambda \cdot (v + (\Delta)_A)) = \lambda \cdot \overline{v} = \lambda \cdot \zeta\big(v + (\Delta)_A\big)$. For the same reason it follows that $\overline{v}_1 + \overline{v}_2 = \overline{\overline{v_1} + \overline{v_2}}$, therefore $\zeta\big(v_1 + v_2 + (\Delta)_A\big) = \overline{\overline{v_1} + \overline{v_2}} = \overline{v}_1 + \overline{v}_2 = \zeta\big(v_1 + (\Delta)_A\big) + \zeta\big(v_2 + (\Delta)_A\big)$.

The homomorphism ζ is injective: if the canonical representative of a class is 0 then this class must consist of elements contained in $(\Delta)_A$. □

At any given stage of the procedure, the generating set of Δ is of the stated form and therefore is an S-module Gröbner basis, so we can define a homomorphism $\zeta_{(\iota)_j}$ for all stages $(\iota)_j$. We will furthermore define χ as the composition of the maps $\gamma : \mathcal{F} \longrightarrow \Sigma/(\Delta)_A$ and $\zeta : \Sigma/(\Delta)_A \longrightarrow \Sigma$, providing an S-module monomorphism

$$\chi : \mathcal{F} \longrightarrow \Sigma.$$

Notation 4.2.3 *We introduced in Chapter 2 the stack of pending coincidences Cp. Accordingly we will denote the set of applicable coincidences which have been already processed by Ca. Thus the information obtained from $c \in Ca$ has already been applied to the elements stored in the multiplication table T and the torsion sequence L. Note that the set Ca only has a theoretical meaning. The elements of Ca have already been processed and information evaluated; therefore the MGE-procedure does not need to access the elements of Ca again.*

Remark 4.2.4 *Whereas in the description of the MGE-procedure in practical terms in Chapter 2 we gave a description of the effect of coincidences $c = \delta(r) \in \Sigma/\Upsilon$, we will investigate the effect of the relations $r \in Rels$ when they are considered as elements of Σ. We will interpret the image of relations under χ as elements contained in the generating set of the module Υ. By abuse of notation we will refer from now onwards to the images under ζ of the applicable coincidences Ca (inapplicable coincidences Cp) as applicable (or inapplicable) coincidences as well.*

In Section 2.4.1 we introduced Υ as the A-module closure of the S-module that is generated by elements induced by the definition steps and also by elements $k \in \Sigma$ which have been induced by the coincidences of an MGE-procedure. We also defined a product " $\star$ " in the quotient-module Σ/Υ which takes into consideration the undeleted image of elements with

respect to the coincidences contained in Ca. In Section 2.5.3, the stack of pending coincidences Cp was introduced.

As the undeleted image can only take into consideration those coincidences which have already been processed, and so are contained in Ca, there will be a discrepancy between the set B^d and that subset of S-module generators which should actually be deleted when the A-linear span of Cp is not zero. Moreover, in the case that S is not a field we possibly have a non-trivial the set of inapplicable coincidences L. These and the pending coincidences have to be factored out from Σ as well in order to eventually obtain a module that is P-module isomorphic to $\mathcal{M}$.

We define a set of S-modules $\Pi_{(\iota)_j}$, for $(0)_1 \leq (\iota)_j \leq (\nu)_0$, together with the respective A-module closure $\Psi_{(\iota)_j}$. The generating set of $\Pi_{(\iota)_j}$ consists of the following elements of $\Sigma_{(\iota)_j}$:

- The set $h \in H$ induced by the definition steps of the MGE-procedure, so $h = b.x - b'$ and in particular $HC(h) = 1$, $Wei\big(HM(h)\big) = 1$ and $Wei\big(RED(h)\big) = 0$ for all $h \in H$.

- The following elements which all are of weight 0 :

  - The set $\{\zeta(c_1), \ldots, \zeta(c_t)\}$ of coincidences in $Ca \in \Sigma$;
  - the set of elements $L \in \Sigma$ which are induced by the inapplicable coincidences;
  - the set of elements which are induced by the coincidences Cp pending in the coincidence stack.

We will now show how certain properties of the generating set of such a module Π can be interpreted in terms of the MGE-procedure and for instance its setting of the multiplication table and the coincidence stack.

Lemma 4.2.5 *Let T denote the multiplication table of an MGE-procedure in stage (ι), where we are given the torsion sequence L and the coincidence stack Cp. Then the information stored in T, Cp and L defines the S-module Π and the multiplication "$\star$".*

Proof. It is clear that the elements of Cp and L correspond to the respective generators of Π. Every row b of the table T corresponds to an element $b \in B$, where B is the set of all possible S-module generators at the stage (ι).

For every undeleted generator $b \in B^u$ and every $x \in X$ there exists a box $\mathrm{prod}(b, x)$. If the box has been filled it contains an element $b \star x = v \in \langle B^u \rangle$. Otherwise, if the entry reads "$\perp$", no definition step for the action of x on b has taken place and the product "$\star$" of b and x is the free product $b.x$ If $\mathrm{prod}(b, x)$ has a non-trivial entry, then it contains either

- $b' \in B^u$ and the entry of $\mathrm{prod}(b, x)$ has, since the point of definition, not been altered; or
- $v \in \langle B^u \rangle_S$ such that $v = u(b') = b' - \lambda_1 \cdot c_1 - \ldots \lambda_t \cdot c_t$ for $c_i \in Ca$.

In the first case, the entry $\mathrm{prod}(b, x)$ of the row b corresponds to a generator $h = b.x - b'$ of Δ. The second case can be translated into a generator $h = b.x - b'$ of Δ such that $b' = RED(h) = HM(c)$ for $c \in Ca$. As $c \in Ca$, c must is an applicable coincidence and therefore $HC(c)$ must be a unit. Then in the course of the procedure b' has been replaced by the respective undeleted images (which are the reducts of $c_{i_j} \in Ca$) leading to a sequence of S-module reductions

$$b' \xrightarrow{c_{i_1}} \widetilde{v} \longrightarrow \ldots \xrightarrow{c_{i_m}} \mathrm{prod}(b, x)$$

by $\{c_{i_1}, \ldots, c_{i_m}\} \subset Ca$.

For every deleted generator $b \in B^d$ we have that $b = HM(c)$ for some applicable coincidence $c \in Ca$, and b has been replaced by $r_b = HC(c)^{-1} \cdot RED(c)$, so that $c = b - r_b$. In this sense we can consider the elements contained in T as a generating set and we have

$$\langle T \rangle_S \subset \langle H \cup Ca \rangle_S.$$

On the other hand, whenever a new definition $h = b.x - b'$ has taken place, leading to $\Pi_{(\iota)_{j+1}} = \Pi_{(\iota)_j} + \langle h \rangle_S$, the table T is extended by another row $b' \in B^u$, where at first $\mathrm{prod}(b', x) = \perp$ for all $x \in X$. Also, if a coincidence c with $HM(c) = b \in B^u$ is added to Ca this implies that $B^d := B^d \cup \{b\}$.

All possible consequences are added to Cp and we delete the row "b" in the table and replace it by $r_b = RED(c)$, hence $\langle H \cup Ca \rangle_S \subset \langle T \rangle_S$. □

Accordingly, a multiplication table T induces a set, which we shall denote by $\widetilde{T}$, containing the following elements of Σ :

- $b.x - v$ for all rows $b \in B^u$ of T and every entry $\text{prod}(b, x) = v$;
- $b - r_b$ for all rows $b \in B^d$ of T with replacement r_b.

We will now proceed to show that the procedure HANDLING INAPPLICABLE COINCIDENCES (HIC) computes the correct results. We need the following definition for torsion sequences:

Definition 4.2.6 *Let $L = \{l_1, \ldots, l_t\}$. We say that a torsion sequence L is in* **pivot form**, *if $HM(l_i) > HM(l_{i+1})$ for all $1 \leq i \leq t-1$. Moreover, we will call a torsion sequence* **reduced** *if $HC(l_i)$ is not a unit of S for all $l_i \in L$.*

Lemma 4.2.7 [26] *Let L be a torsion sequence which is in pivot form and reduced. The S-linear span Λ of the elements of L does not contain any applicable coincidences.*

Proof. Let $L = \{l_1, \ldots, l_t\}$ and $HM(l_i) > HM(l_{i+1})$ for all $1 \leq i \leq t-1$ and let $c \in \Lambda$ such that $c = \sum_{i=1}^{t} \lambda_i \cdot l_i$ with $HM(c) = b \in B$. In fact, as it is ensured that an element of L is replaced by its undeleted image immediately we must have $l_i = u(l_i)$ and it follows that $b \in B^u$.

Let k be the maximal index of entries of L such that $HM(l_k) \geq b$. As L is in pivot form, the entries of L are ordered by their head monomials and we conclude that $\lambda_i = 0$ for all $i < k$. If these coefficients were unequal to zero then there would be an entry l_i such that $HM(l_i)$ was a non-trivial summand of l. This would imply that $HM(l_i) > b = HM(c)$.

On the other hand we have that $b > HM(l_{k+1}) > HM(l_{k+2}) > \cdots > HM(l_t)$. Therefore for all $i > k$, the S-module generator b cannot be contained as a summand with coefficient $\lambda_i \neq 0$ in any of the entries l_i. It

follows that b can be contained as a non-zero summand only in the summand l_k. Therefore $HC(c)$ must be a multiple of $HC(l_k)$ and therefore $HC(c) = \lambda_k \cdot HC(l_k)$. By assumption, the torsion sequence is reduced which implies that $HC(l_k)$ is not a unit of S. It follows that $HC(c)$ cannot be a unit of S either. □

Lemma 4.2.8 *Suppose we are given a reduced torsion sequence L in pivot form into which we insert an inapplicable coincidence c with the procedure HIC. Let L' denote the torsion sequence returned by the procedure and let $\{c_1, \ldots, c_n\}$ denote the set of those coincidences which were added to the coincidence stack Cp in the course of the procedure. Then*

$$\langle L', c_1, \ldots, c_n \rangle_S = \langle L, c \rangle_S.$$

Proof. Suppose that $L = \{l_1, \ldots, l_t\}$ and let $c = \sum_{i=1}^{m} \lambda_i \cdot b_i$. Suppose that $HM(c) \neq HM(l_j)$ for all $1 \leq j \leq t$ and suppose that $HM(l_k) > HM(c) > HM(l_{k+1})$. Then we will insert c into L at position $k+1$ and obtain $L' = l_1, \ldots, l_k, \widetilde{l}_{k+1}, \ldots, \widetilde{l}_{t+1}$ where $\widetilde{l}_{k+1} = c$ and $\widetilde{l}_{k+j+1} = l_{k+j}$ for $1 \leq j \leq t-k$. Clearly, no further coincidences are produced in this case and $\langle L \cup C \rangle_S = \langle L' \rangle_S$.

Therefore we suppose there is $l_k \in L$ such that $HM(l_k) = HM(c)$. We set $\mu := GCD(HC(c), HC(l_k))$ as the greatest common divisor of $HC(c)$ and $HC(l_k)$. Then there exist elements $s_1, s_2 \in S$ such that

$$s_1 \cdot HC(c) + s_2 \cdot HC(l_k) = \mu.$$

and also $t_1, t_2 \in S$ with $s_1 \cdot t_1 + s_2 \cdot t_2 = 1$, namely $t_1 = HC(c)/\mu$ and $t_2 = HC(l_k)/\mu$ and therefore

$$t_2 \cdot HC(c) - t_1 \cdot HC(l_k) = 0.$$

In the procedure HIC, c and l_k get replaced by v_1 and v_2 such that $v_1 := s_1 \cdot c + s_2 \cdot l_k$ and $v_2 := t_2 \cdot c - t_1 \cdot l_k$.

By definition, v_1 and v_2 are contained in the S-linear span of c and l_k. On the other hand,

$$c = (s_1 \cdot t_1 + s_2 \cdot t_2) \cdot c = s_1 \cdot t_1 \cdot c + s_2 \cdot t_1 \cdot l_k + s_2 \cdot t_2 \cdot c - s_2 \cdot t_1 \cdot l_k = \\ t_1 \cdot (s_1 \cdot c + s_2 \cdot l_k) + s_2 \cdot (t_2 \cdot c - t_1 \cdot l_k) = t_1 \cdot v_1 + s_2 \cdot v_2$$

and similarly $l_k = t_2 \cdot v_1 - s_1 \cdot v_2$. It follows that we obtain an equality of the S-modules generated by the respective elements:

$$\langle v_1, v_2 \rangle_S = \langle c, l_k \rangle_S.$$

Depending on whether v_1 and v_2 are applicable or not they will either be inserted into L (starting a new loop with the element v_2 which has $HM(v_2) < HM(v_1)$) or, if they are applicable, into the coincidence stack. As every coincidence added to Cp in the procedure HIC has been produced as either v_1 and v_2, the claim follows. □

Remark 4.2.9 *Let $l_i \in L$ and suppose we aim to insert an inapplicable coincidence v such that $HM(l_i) = HM(v)$ into L. Then the element v_1 which is formed in the course of the HIC-procedure resembles the S-module $\mathfrak{g}$-polynomial of l_i and v and v_2 corresponds the $\mathfrak{s}$-polynomial of l_i and v.*

Lemma 4.2.10 [26] *Let L be a torsion sequence which is reduced and in pivot form. If we insert an inapplicable coincidence c into L, then the torsion sequence L' produced by* HIC *will be reduced and in pivot form as well.*

Proof. Suppose that we have entered the main loop of HIC for the j-th time with an element v and let $L = \{l_1, \ldots, l_t\}$. Then for all $1 \leq i < j$ we have that $HM(l_i) > HM(v)$. Before having entered for the j-th time, the following can have happened:

1. The element v is the coincidence with which we intially entered the procedure HIC. In this case the torsion sequence L has not been altered and nothing needs to be shown.

2. There has been an element $v' \neq v$ which was supposed to be inserted into L. An element $l_i \in L$ was found with $HM(v') = HM(l_i)$ for $l_i \in L$ where $i < j$. Then v has been defined as $v := v_2$ where $v_2 = t_2 \cdot v' - t_1 \cdot l_i$. We set $v_1 := s_1 \cdot v' + s_2 \cdot l_i$ and remove the entry l_i from L.

   (a) If v_1 is applicable we set $l_k := l_{k+1}$ for all $i \leq k < t$. We add v_1 to the coincidence stack and we will pursue in the procedure HIC with inserting the element $v = v_2$. The head monomial of v is strictly smaller than the head monomial of v_1. We pursue the insertion of v at position i in order to compare $HM(v)$ with the head monomial of the new i-th entry of $L := L \backslash \{l_i\}$.

   (b) If v_1 is inapplicable, then it will get inserted into $L \backslash \{l_i\}$, namely at position i. Since $HM(v_1) = HM(l_i)$ and L had been reduced and in pivot form, it follows that $L := (L \backslash \{l_i\}) \cup \{v_1\}$ must be reduced and in pivot form as well.

   Thus in both cases we aim to insert $v = v_2$ into a reduced torsion sequence in pivot form. As we are entering the loop for the j-th time it follows that $HM(l_i) > HM(v)$ for all $i < j$. □

We will now show that the procedure PROCESSING A COINCIDENCE (PRC) is terminating. For this we will show that PRC essentially resembles prefix reduction of elements of $\widetilde{T}$ and L by the coincidence which is being processed and that the possible computation of consequences resembles prefix-closure.

Proposition 4.2.11 *Let $c \in Cp$ be an applicable coincidence c. The procedure PRC applied to c corresponds to prefix reduction of the entries of $\widetilde{T}$ and L by the element c. The computation of consequences, if there are any, corresponds to the prefix-closure of c with $b.x - b'$ for the affected $x \in X$.*

Proof. Let $b_h = HM(c)$. As $HC(c)$ is a unit of S, the procedure PRC replaces the row b_h in the table T by $r_{b_h} = HC(c)^{-1} \cdot RED(c)$, and the respective row b_h of T gets deleted. Accordingly, for every $v = \mathrm{prod}(b_i, x_j)$

in the table which contains b_h as a summand, suppose with coefficient λ_h, the computing of the new undeleted image of v resembles a reduction by c:

$$v \xrightarrow{c} v - \lambda_h \cdot HC(c)^{-1} \cdot c = \widetilde{v}$$

where $\widetilde{v}$ is an element which is minimal with respect to the other entries of T, thus elements of the form $b.x - v'$ with $b \in B^u$ and $v' \in \langle B^u \rangle_S$. Similarly, the subprocedure APPLY COINCIDENCE TO TORSION SEQUENCE leads to reductions of elements $l \in L$.

Now suppose that a consequence needs to be computed. Thus the product $b_h \star x$ with at least one $x \in X$ has been defined, so there is at least one entry $\mathrm{prod}(b_h, x)$ contained in the row b_h of T which has been filled with $v = b_h \star x$. However, in order to compute such a consequence $\widetilde{c} := c \star x$, PRC possibly leads to a finite number of definition steps, namely for each summand b_k of $RED(c)$ for which $b_k \star x \notin \langle B \rangle_S$ so the box $\mathrm{prod}(b_k, x)$ has not been filled. These definition steps can be interpreted as enlarging the generating set of the module Δ by elements $h_k = b_k.x - b'_k$. The element $c.x$ is the prefix-closure of $c = b_h - RED(c)$ and $h' = b_h.x - v$. In the case that the product $b_k \star x$ has been defined for all summands b_k of $RED(c)$, there exists an S-module reduction-sequence

$$c.x \xrightarrow{h'} v + RED(c).x \xrightarrow{h_{j_1}} \ldots \xrightarrow{h_{j_m}} \widetilde{c}$$

reducing the prefix-closure $c.x$ to the element $\widetilde{c} \in \langle B^u \rangle_S$ which is a consequence of c. □

Corollary 4.2.12 *The procedure PRC terminates.*

Proof. There are a finite number of elements contained in $\widetilde{T}$ and L, accordingly reduction of these elements by a coincidence c must be a finite process. Moreover it follows from Lemma 3.2.17 that prefix-closing a finite set is a finite process. Therefore we can conclude that the computation of potential consequences must be finite and it follows that PRC must terminate. □

Remark 4.2.13 *Since the tracing of a coincidence c in the MGE-procedure uses the undeleted image (as defined in Definition 2.4.7), it follows that a coincidence must be minimal with respect to the coincidences contained in Ca at the point when it gets applied.*

Definition 4.2.14 *We will call a generating set G of a submodule Ψ of Σ an* **MGE-basis** *if G is a prefix inter-reduced prefix Gröbner basis such that for all $g \in G$ either*

- $Wei\big(HM(g)\big) = 1, HC(g) = 1$ *and* $Wei\big(RED(g)\big) = 0$, *or*
- $Wei(g) = 0$.

Lemma 4.2.15 *Let $Cp = \emptyset$ and suppose that L is a torsion sequence in pivot form and reduced. Then the set $\widetilde{T} \cup L$ is an MGE-basis of $\Psi = (\langle \widetilde{T}, L \rangle_S)_A$.*

Proof. The elements contained in $\widetilde{T}$ are either elements $h' = b.x - v \in \Sigma^u$ such that $Wei(HM(h')) = 1$ and $Wei(RED(h')) = 0$, or they correspond to coincidences $c \in Ca$ for which $RED(c) \in \langle B^u \rangle$. The set $\widetilde{T} \cup L$ is prefix-closed. Indeed the procedure PROCESSING A COINCIDENCE ensures that all possible consequences of the coincidence which is being processed have been captured. Since $Cp = \emptyset$ it follows that every such consequence must now be contained in either $\widetilde{T}$ or L. Moreover, the procedure TORSION CLOSURE leads to adding $l \star x$ to Cp for every pair of $l \in L$ and $x \in X$. Such an element $l \star x$ is obtained from the prefix-closure element $l.x$ by S-module reduction of elements of weight 1 contained in $\widetilde{T}$. Again, as $Cp = \emptyset$, we must have $l \star x \in \widetilde{T} \cup L$.

By assumption on L there are no applicable coincidences contained in L. As it is ensured that we have $l = u(l)$ for $l \in L$ it follows that the elements of L, which itself is an inter-reduced set, must be minimal with respect to Ca. On the other hand, the set Ca must be inter-reduced: this follows from using its undeleted image when a coincidence is being processed. Also, as there are no applicable coincidences contained in L, the head terms of the elements of Ca are minimal with respect to L. A finite number of reductions

of reducts of elements of Ca by elements of L leads to an inter-reduced set $\widetilde{T} \cup L$ and it follows from Corollary 3.1.19 that $\widetilde{T} \cup L$ forms an S-module Gröbner basis for the S-module it generates. As the set is prefix-closed as well, Theorem 3.2.20 implies that $\widetilde{T} \cup L$ must be a prefix Gröbner basis for the A-module closure Ψ. Certainly, all the elements of $\widetilde{T}$ and L are of the demanded form and the claim follows. □

Corollary 4.2.16 *Suppose that $\langle Cp \rangle_A \subset \langle Ca \cup L \rangle_A$ and suppose that the torsion sequence L is in pivot form and reduced. Then $\widetilde{T} \cup L$ is an MGE-basis of $\Psi = (\Pi)_A$.*

Proof. We described in Lemma 4.2.5 how the elements of Ca can be found as entries of T, thus $Ca \subset \widetilde{T}$. In Lemma 4.2.15 it was explained that the set $Ca \cup L$ is inter-reduced and, since $Wei(v) = 0$ for all $v \in Ca \cup L$, it is prefix inter-reduced for trivial reasons. Therefore, every element $v \in \langle Ca \cup L \rangle_A$ can be prefix-reduced to 0. It follows in particular that for every $c \in Cp$,

$$c \xrightarrow[S]{Ca \cup L} 0$$

and this implies that $u(c) = 0$ or $u(c) \in \Lambda = \langle L \rangle_S$. Since, whenever a pending coincidence c gets processed its undeleted image is being computed, it follows that the coincidences $c \in Cp$ cannot lead to any further prefix-reductions of elements of $\widetilde{T} \cup L$. □

We will now introduce a property for the table T which is needed in order to be able to draw conclusions from a given generating set $G = \widetilde{T} \cup Cp \cup L$ to the elements contained in the set of pending coincidences Cp.

Definition 4.2.17 *We will call a multiplication table T* **connected** *if we have for every row $b \in B^u$ one of the following:*

- *At least one of the boxes $prod(b, x)$ for $x \in X$ has been filled, or*
- *b is contained as summand of at least one $prod(b', x) = v \in \langle B^u \rangle_S$ for $x \in X$ and a generator $b' \in B^u$.*

Example 4.2.18 *Suppose we are given the P-module $\mathcal{M} = \langle y_1, y_2 \mid y_1.x_1^3 - y_1, y_2 - 2 \cdot y_1 \rangle_P$ where $P = \langle x_1, x_2 \mid x_1x_2 - x_2x_1 \rangle_{\mathbb{Z}}$. After computing of the coincidence obtained from the first module-relation we obtain the table:*

	$prod(b, x_1)$	$prod(b, x_2)$	r_b	$\gamma^{-1}(\pi(b))$
b_1	b_3	$\perp$	$\perp$	y_1
b_2	$\perp$	$\perp$	$\perp$	y_2
b_3	b_4	$\perp$	$\perp$	$y_1.x_1$
b_4	b_5	$\perp$	$\perp$	$y_1.x_1^2$
b_5	$\perp$	$\perp$	b_1	$\perp$

Suppose now that we have added the coincidence $b_2 - 2 \cdot b_1$ to the coincidence stack but that it has not been processed yet. Then $Cp = \{b_2 - 2 \cdot b_1\}$. No definitions have taken place for the S-submodule generator b_2, nor can it be found in the replacement of a coincidence, therefore the table above is not connected.

The generating set $G = \widetilde{T} \cup Cp \cup L$ which we obtain at this point of the computation then consists of the following elements: $G = \{b_1.x_1 - b_3, b_3.x_1 - b_4, b_4.x_1 - b_1, b_5 - b_1, b_2 - 2 \cdot b_1\}$ and since G is prefix inter-reduced it follows that G is an MGE-basis. This however can only be the case if the pending coincidence does not lead to prefix-reductions for any elements of G as its head monomial b_2 is not contained in any entry of the multiplication table.

The condition on the multiplication table to be connected is necessary in order for the assertion of the following Lemma to be true:

Lemma 4.2.19 *Let Π be a finitely generated S-module with generating set $G = \widetilde{T} \cup Cp \cup L$ where we suppose that the set $\widetilde{T}$ corresponds to a connected multiplication table T. If G is an MGE-basis, then $\langle Cp \rangle_A \subset \langle \widetilde{T} \cup L \rangle_A$.*

Proof. Suppose that the A-linear span of Cp is not contained in the A-linear span of $\widetilde{T} \cup L$. Then there exists $v \in \langle Cp \rangle_A$ such that $v \neq 0$. Without loss of generality we can choose v prefix-minimal with respect to the set $\widetilde{T} \cup L$; then in particular $u(v) \neq 0$. It follows that $v \in \langle Cp \rangle_A \cap \Sigma^u$ and $v = \sum_{j=1}^{t} \lambda_j \cdot c_j.w_j$ for $c_j \in Cp$. We will distinguish between the following two cases:

1. There exists $c \in Cp$ such that $HM(c) = p]_{HM(v)}$ and $HC(c) \leq HC(v)$. Since $v = u(v)$ it follows that $HM(c) \in B^u$.

By assumption, $\widetilde{T}$ corresponds to a connected table, therefore $HM(c)$ can be found in the multiplication table as a summand of a $\mathrm{prod}(b, x)$ or as a row $b \in B^u$. It follows that $HM(c)$ is a summand or a prefix of an element of $\widetilde{T}$ which is a contradiction to the assumption that the set G is prefix inter-reduced.

2. There exists no $c \in Cp$ such that both $HM(c) = p]_{HM(v)}$ and $HC(c) \leq HC(v)$ hold. Therefore $v \neq 0$ must be prefix-minimal with respect to the elements of Cp. Since v however was chosen to be prefix-minimal with respect to $\widetilde{T} \cup L$, it follows that v must be prefix-minimal with respect to G. As $v \neq 0$ it follows that G cannot be a prefix Gröbner basis of $\Psi = (\Pi)_A$ and in particular it cannot be an MGE-basis either. □

Proposition 4.2.20 *Suppose that the S-submodule Π of Σ is finitely generated by the finite set $\widetilde{T} \cup L \cup Cp$. A finite MGE-basis $G = \widetilde{T}' \cup L' \subset \Sigma'$ can be computed such that $\Sigma \subset \Sigma'$, $\Psi \subset \langle G \rangle_A$ and $\Sigma/(\Pi)_A \cong \Sigma'/\langle G \rangle_A$.*

Proof. It follows from Lemma 3.1.21 and Lemma 3.2.17 that we can obtain an S-module Gröbner basis and a prefix-closed set from a finite generating set. Thus we can compute a finite set G with $\langle G \rangle_A = \langle \widetilde{T} \cup L \cup Cp \rangle_A$ such that G is inter-reduced, prefix-closed and an S-module Gröbner basis. For achieving this we need to compute a finite number of $\mathfrak{s}$-polynomials, we need to add a finite number of prefix-closures and need to carry out a finite number of S-module reductions. However, the elements added for prefix-closure might not be in the appropriate form for G to be an MGE-basis: for each $c.x$ added for prefix-closure we know that $Wei(c.x) = 1$. In the case that every $c.x$ can be reduced by $\widetilde{T}$ such that $c.x \xrightarrow{\widetilde{T}_S} q$ with $Wei(q) = 0$, the assumption follows immediately.

Now suppose that there is a set of elements $c.x$, caused by prefix-closure, which cannot be reduced by elements of $\widetilde{T}$ to an element of weight 0. Then we obtain by reduction $c.x \xrightarrow[S]{\widetilde{T}}{}^{*} p$ an element p that is minimal with respect to $\widetilde{T}$ but where $Wei(p) = 1$. In this situation we need to make definition steps

and therefore have to add for each summand $b.x$ of p with $b.x \notin HM(\widetilde{T})$ an element $h' = b.x - b' = b.x - \text{prod}(b, x)$ to the set $\widetilde{T}$.

A finite number of such elements $h' := b.x - b'$ is being added such that the respective b' have greater index than the elements that have already been contained in the set of S-module generators B of Σ. We set $\Sigma' = \langle B'X^* \rangle_S$, where $B' = B \cup \{b'_1, \ldots b'_m\}$. Moreover, we set $\widetilde{T}' := \widetilde{T} \cup \{h'_1 \ldots, h'_m\}$ and now for all $c.x$ we can reduce $c.x \xrightarrow[S]{\widetilde{T}'}{}^{*} q$ such that $Wei(q) = 0$.

Suppose that we have to add a prefix-closure element for such an element $q \in \langle B' \rangle_S$. Then there is $h'_i \in \widetilde{T}'$ and an element $x \in X$ such that

$$HM(q).x = HM(h'_i).$$

Since we were only able to obtain q by reduction by $\widetilde{T}'$, but not by $\widetilde{T}$, it follows that $HM(q) = b' \in B' \backslash B$ where b' must be the reduct of some $h'_j \in \widetilde{T}' \setminus \widetilde{T}$.

Now if $b' = RED(h'_j)$ is the prefix of $HM(h'_i)$ then there must have been a summand of one of the elements which we did obtain by reducing the elements of the form $c.x$, and this summand is just $b'.x$. Since h'_j with $RED(h'_j) = b'$ had only been added to $\widetilde{T}$ in that course of reduction of some element $c.x$ it follows that we must have started initially with an element $c.x$ with $Wei(c.x) > 1$. However, this is a contradiction as $c.x$ is the prefix-closure of an element of weight 0 with an element that has weight 1. So $Wei(c.x) \leq 1$. We conclude that h'_j must have already been contained in $\widetilde{T}$.

Therefore, after adding a finite number of prefix-closure elements $c.x$ and possibly a finite number of elements $h' = b.x - b'$, which then will lead to a finite number of S-module reductions in order to obtain elements $\widetilde{c}$ of weight 0, we will obtain a prefix-closed set G of the demanded form. An element $g \in G$ then has to be minimal with respect to $G \setminus \{g\}$. Therefore G is inter-reduced and it follows that G is an S-module Gröbner basis such that for every $g \in G$ we either have that

- $g \in G$ with $HC(g) = 1, Wei\big(HM(g)\big) = 1$ and $Wei(RED(g)) = 0$; or
- $g \in G$ such that $Wei(g) = 0$.

Certainly, as the elements added are of the form $b.x - \text{prod}(b, x)$, which is just an element $b.x - b' \in \Delta$, we must have that $\Sigma/\Psi \cong \Sigma'/\langle G \rangle_A$. □

Lemma 4.2.21 *The procedure* CLEARING COINCIDENCES *terminates.*

Proof. The procedure CLEARING COINCIDENCES chooses a coincidence $c \in Cp$, and if the undeleted image of c is unequal to 0, then the procedure PRC is called for c. In the case that c is inapplicable, the subroutine HIC is called. The routine HIC essentially computes an inter-reduced Gröbner basis from the set $L \cup \{c\}$ (L denotes the torsion sequence).

If $HM(c)$ is different to the head monomials of elements contained in L, c can be inserted immediately into L. In the case that there is an $l \in L$ with $HM(l) = HM(c)$, an element v_1 replaces the entry l of L; v_1 is equal to a $\mathfrak{g}$-polynomial of l and c. We then aim to insert an element v_2 into L; v_2 has been formed as an $\mathfrak{s}$-polynomial of l and c and therefore has a strictly smaller head monomial than c and l. It follows that this routine must terminate.

If c is applicable it has been shown in Lemma 4.2.11 that the procedure PRC applied to a coincidence c corresponds to prefix-reduction of $\widetilde{T}$ and L by c. Moreover, in the case that consequences need to be computed, the computation of these consequences corresponds to adding the prefix-closure $c.x$ of c with an element $b.x - b' \in \widetilde{T}$, where b' is a summand of the reduct of c.

In order to obtain a consequence $\widetilde{c} = c \star x$, thus an element of weight 0, it is possible that a finite number of definitions need to be made. This corresponds to adding a finite number of elements to the set $\widetilde{T}$ and it follows from Proposition 4.2.20 that these newly added $b' \in B' \backslash B$ cannot themselves cause consequences in this invocation of CLEARING COINCIDENCES.

Accordingly the procedure CLEARING COINCIDENCES must terminate after a finite number of steps, having cleared all coincidences from the coincidence stack Cp. □

Proposition 4.2.22 *Let Φ denote the A-module closure of the S-submodule of Σ^u at a stage (ι) which is generated by a set consisting of the following:*

- *the elements $l \in L$ contained in the torsion sequence at the stage (ι);*
- *the elements of a set $\widetilde{T}^u$ which is the subset of $\widetilde{T}$ induced by the entries of those rows corresponding to $b \in B^u$ of a connected multiplication table $T_{(\iota)}$.*

If $G = \widetilde{T} \cup L \cup Cp$ is an MGE-basis of Ψ, then

$$\Sigma/\Psi \cong_A \Sigma^u/\Phi.$$

Proof. If G is an MGE-basis of Ψ then we know that the set G generates Ψ. As the set of pending coincidences Cp must be contained in the generating set of Ψ it must follow that $\langle Cp\rangle_A \subset \langle \widetilde{T} \cup L\rangle_A$. Thus $\Psi = \Phi + \langle Ca\rangle_A$ and we can form congruence classes $|v + \Phi|_{Ca}$ of Σ/Φ modulo $\langle \Phi + Ca\rangle_A$. We define a mapping $\beta : \Sigma/\Psi \longrightarrow \Sigma^u/\Phi$ which maps a congruence class $v + \Psi = (v + \langle Ca\rangle + \Phi) \in \Sigma/\Psi$ to a representative $\widetilde{v} + \Phi$ of the congruence class $|v + \Phi|_{Ca}$.

Since the generating set G is an MGE-basis we can conclude that G is prefix inter-reduced. This implies that the elements of $\widetilde{T}^u$ and L must be prefix-minimal with respect to Ca and accordingly $\widetilde{T}^u \cup L \subset \Sigma^u$. Moreover, for every $v \in \Sigma$ there exists $\overline{v} \in \Sigma^u$ which is prefix-minimal with respect to Ca and $v - \sum_{i=1}^{m} c_i \cdot a_i = \overline{v}$ where $c_i \in Ca$. As an MGE-basis is also a prefix Gröbner basis, we can choose representatives in a canonical way, so in particular we can choose the representative $\overline{v} + \Phi$ of $|v + \Phi|_{Ca}$ such that $\overline{v}$ is prefix-minimal with respect to Ca. This implies that $\overline{v} + \Phi \in \Sigma^u/\Phi$.

The map β is well-defined: let $v_1, v_2 \in \Sigma$ such that $v_1 + \Psi = v_2 + \Psi$, so $v_1 = v_2 + \sum_{i=1}^{t_1} c_i \cdot a_i + \sum_{j=1}^{t_2} l_j \cdot a_j + \sum_{k=1}^{t_3} h_k \cdot a_k$, with $a \in A, c_i \in Ca, l_j \in L, h_k \in \widetilde{T}$, and therefore, $|v_1 + \Phi|_{Ca} = |v_2 + \Phi|_{Ca}$. The mapping β is an A-module homomorphism. Indeed let $\lambda \in S$. As the head coefficients of elements of Ca are units it follows that $\lambda \cdot \overline{v} = \overline{\lambda \cdot v}$ for the canonical representatives $\overline{v}$ with respect to Ca. Therefore

$$\lambda \cdot \beta(v + \Psi) = \beta(\lambda \cdot v + \Psi).$$

For the same reason it follows that $\beta(v_1 + \Psi) + \beta(v_2 + \Psi) = \beta(v_1 + v_2 + \Psi)$. Now let $a \in A$, then $\beta(v + \Psi).a = \overline{v}.a + \Phi$ from which we conclude that $\overline{v}.a \in \Sigma^u$. This, however, implies that $\overline{v}.a = \overline{v.a}$ and therefore

$$\beta\big(v + \Psi\big).a = \overline{v}.a + \Phi = \overline{v \cdot a} + \Phi = \beta\big((v + \Psi).a\big).$$

Moreover, β is injective. If $\beta(v + \Psi) = \overline{v} + \Phi = 0 + \Phi$, then v certainly must have been element of Ψ. Since the generating set of Ψ is prefix inter-reduced, it follows that $v \notin \Sigma^u$ and accordingly v must have been an element of Ca.

Also, β is surjective. Let $\overline{v} + \Phi \in \Sigma^u/\Phi$ and we suppose that $\overline{v} + \Phi \neq \beta(v + \Psi)$. Therefore, $\overline{v} \in \Sigma^u$ cannot be a canonical representative of a class $|v|_{Ca}$ and there must exist $c_{i_1}, \ldots, c_{i_t} \in Ca$ with

$$\overline{v} - \sum_{j=1}^{t} c_{i_j} \cdot a_j = v''$$

such that v'' is prefix-minimal with respect to Ca. Since Ca is an inter-reduced set this implies that $HM(c_{i_j}) \neq HM(c_{i_k})$ for all $i_j \neq i_k$. However, this is a contradiction to the assumption that $\overline{v} \in \Sigma^u$. □

Theorem 4.2.23 *Suppose that* MAIN ROUTINE *is at a stage* (ι) *of the computation such that* $Cp = \emptyset$, *where the given multiplication table* T *is connected and where the given torsion sequence* L *is reduced and in pivot form. Then those rows* T^u *of* T *which correspond to the undeleted* S*-module generators* $b \in B^u$ *together with the elements of* L *encode a set of generators for the submodule* $\Phi_{(\iota)}$ *such that*

$$\mathcal{F}/\mathcal{N}_{(\iota)} \cong \Sigma^u_{(\iota)}/\Phi_{(\iota)}.$$

Proof. We remind ourselves that the P-module $\mathcal{M}$ can also be considered as an A-module. Then it has the form

$$\mathcal{M}_A = \mathcal{F}/\mathcal{N}$$

where $\mathcal{N}$ denotes the submodule of the free A-module $\mathcal{F}$ that is generated by the set *Rels* which, in the case that $\mathcal{M}_P$ has relations induced by the finitely presented algebra P, must be infinite.

In the case that $\mathcal{M}$ is P-module isomorphic to a P-module with finite generated as S-module it follows from Theorem 1.2.1 that there exists a finite set of generators for $\mathcal{N}$. In the MGE-procedure we aim to build up stepwise the module $\mathcal{N}$ by adding relations $r \in Rels$ which were chosen for the computation of coincidences. This gives us an ascending sequence

$$\mathcal{N}_{(0)} \subset \ldots \mathcal{N}_{(\iota)} \subset \mathcal{N}_{(\iota+1)} = \mathcal{N}_{(\iota)} + \langle r_{(\iota)} \rangle_A \cdots$$

By construction of the procedure in Section 2.4.1 we have S-modules Σ, Δ and Ω, the submodule of $\Sigma/(\Delta)_A$ which is generated by the processed coincidences, such that

$$\mathcal{F}/\mathcal{N}_{(\iota)} \cong \Sigma_{(\iota)}/(\Delta_{(\iota)})/(\Omega_{(\iota)})_A.$$

In Lemma 2.4.3 we showed that the right hand side is isomorphic to the quotient-module $\Sigma_{(\iota)}/\Upsilon_{(\iota)}$ and since $Cp = \emptyset$ we have that $\Upsilon_{(\iota)} = \Psi_{(\iota)}$. We can therefore conclude, also using the result of Proposition 4.2.22, that

$$\mathcal{M}_{(\iota)} = \mathcal{F}/\mathcal{N}_{(\iota)} \cong \Sigma^u_{(\iota)}/\Phi_{(\iota)}.$$

□

Corollary 4.2.24 *If the* MAIN ROUTINE *terminates at a state* (ν) *where the given multiplication table* T *is connected and where the given torsion sequence* L *is reduced and in pivot form then* MAIN ROUTINE *returns a correct result. Thus* MAIN ROUTINE *will have computed sets* T^u *and* L *which encode a set of generators of the submdodule* $\Phi_{(\nu)}$ *such that* $\mathcal{F}/\mathcal{N}_{(\nu)} \cong \Sigma^u_{(\nu)}/\Phi_{(\nu)}$.

Proof. We can deduce from Theorem 4.2.23 that MAIN ROUTINE is in fact computing, for those (ι) which satisfy the conditions of Theorem 4.2.23, a finitely generated S-module with additional A-module structure which is

A-module isomorphic to the given module $\mathcal{M}_{(\iota)}$. □

We will introduce in Chapter 5 certain conditions on the tools used in the procedure subject to which we can show the termination of the MGE-procedure. We will show that, in the case of termination, the module $\Sigma^u_{(\iota)}/\Phi_{(\iota)}$ will in fact induce a finitely generated S-module which is isomorphic as P-module to $\mathcal{M}$.

Chapter 5

Termination of the MGE-Procedure

In this chapter we show termination of the MGE-procedure. In order to do so we again relate the MGE-procedure to the setting of reduction and Gröbner bases as described in Chapter 3 and Chapter 4.

Section 5.1: We introduce an ordering on the elements of the free module $\mathcal{F}_A$ which is induced by the ordering on Σ and the image under the isomorphism $\gamma : \mathcal{F} \longrightarrow \Sigma/(\Delta)_A$. Moreover we describe how coincidences lead to reduction-rules on $\mathcal{F}$. We then proceed by showing that all reduction-rules which have been induced by coincidences applied in the course of an MGE-procedure do not lead to infinite sequences of reduction.

Section 5.2: We introduce so-called important congruence classes in $\mathcal{F}$ modulo $\mathcal{N}$; certain properties of these important classes are investigated. Moreover we describe the connection between these classes and the MGE-procedure.

Section 5.3: We describe the prerequisites that are needed for the MGE-procedure in order to terminate in terms of the tools accompanying an MGE-procedure. We interpret the effect of those prerequisites on the S-modules which are constructed in the course of the computation and prove that, in the case that $\mathcal{M}$ is isomorphic to a finitely generated S-module, these prerequisites will eventually be satisfied by the procedure.

5.1 Induced Ordering on $\mathcal{F}$

We will again denote by ζ, as defined in Section 4.2, the right-inverse of the canonical quotient-map $\pi : \Sigma \longrightarrow\!\!\!\!\!\rightarrow \Sigma/(\Delta)_A$, and by $\chi : \mathcal{F} \longrightarrow \Sigma$ the composition of $\gamma : \mathcal{F} \longrightarrow \Sigma/(\Delta)_A$ with ζ. As has been described earlier, since we are given a prefix Gröbner basis for $(\Delta)_A$ we are able to define ζ in a unique way. We define ζ such that a class $v + (\Delta)_A \in \Sigma/(\Delta)_A$ is mapped to its canonical representative $\overline{v} \in \Sigma$.

Definition 5.1.1 *Let $f_1, f_2 \in \mathcal{F}$ such that $\chi(f_1) = v_1$ and $\chi(f_2) = v_2$. We define the* **ordering induced by image** *on the elements of $\mathcal{F}$, which will be denoted by $\succ_{ii}$, by:*

$$f_1 \succ_{ii} f_2 \Longleftrightarrow v_1 \succ_{wei} v_2.$$

Moreover, we define the **weight of** *f, denoted $Wei(f)$, as*

$$Wei(f) := Wei(\chi(f)).$$

Lemma 5.1.2 *Let $f_1, f_2 \in \mathcal{F}$ such that f_2 is a prefix of a summand of f_1, then*

$$Wei(f_1) \geq Wei(f_2).$$

Proof. Let $\widetilde{f}$ denote the summand of f_1 such that $f_2.w = \widetilde{f}$. Since χ is an S-module homomorphism, the weight of elements of $\mathcal{F}$ is additive, accordingly $Wei(f_1) \geq Wei(\widetilde{f})$. Therefore $Wei(f_1) \geq Wei(\widetilde{f}) = Wei(\chi(\widetilde{f})) = Wei(\chi(f_2.w)) \geq Wei(\chi(f_2)) = Wei(f_2)$. □

Remark 5.1.3 *By definition, the image-induced ordering on $\mathcal{F}$ depends on the maps γ and ζ. As the homomorphisms $\gamma_{(\iota)_j}$, as well as $\zeta_{(\iota)_j}$, for $(0)_0 \leq (\iota)_j \leq (\nu)_0$, might change significantly during the course of the procedure, the image-induced ordering on the elements of $\mathcal{F}$ will change accordingly. However, we will only compare elements $f_1, f_2 \in \mathcal{F}$ at one stage $(\iota)_j$, therefore using only one ordering depending on one morphism $\chi_{(\iota)_j}$.*

Coincidences of the MGE-procedure induce prefix reduction-rules on the elements of Σ, but they can also be seen as leading to reduction-rules on the elements of $\mathcal{F}$: let $f_1, f_2 \in \mathcal{F}$ with $\chi(f_1) \succeq_{wei} \chi(f_2)$, and suppose that there exists a coincidence $c \in \Sigma/(\Delta)_A$ such that $HM\big(\zeta(c)\big)$ is a prefix of a summand $\lambda \cdot b.w$ of $\chi(f_1)$ with $HC\big((c)\big) \leq \lambda$ and also $\chi(f_1) - \kappa \cdot c.w \sim_{(\Delta)_A} \chi(f_2)$ for some suffix $w \in X^*$ and coefficient $\kappa \in S$. Then by the image-induced ordering we have that $f_1 \succeq_{ii} f_2$. We will now define prefix-reduction on elements of $\mathcal{F}$ and we will show that this simulates the reduction-process of the MGE-procedure.

Definition 5.1.4 *Let $f_1, f_2 \in \mathcal{F}$ and let Q be a finite set of elements of $\mathcal{F}$. Then Q* **prefix-reduces** *f_1* **to** *f_2* **in one step**, *denoted by $f_1 \xrightarrow[p]{Q} f_2$, if there exist $q \in Q$ with $\chi(q) = c \in \langle B \rangle$ and $v_1, v_2 \in \Sigma$ with $v_i = \chi(f_i)$ for $i = \{1, 2\}$ such that*

1. *$HM(c) = b$ and $b \in B$ is prefix of a summand $\lambda \cdot b.w$ of $v_1 = \chi(f_1)$,*
2. *there exist $\kappa, \kappa' \in S$ such that $\lambda = \kappa \cdot HC(c) + \kappa'$ where $\kappa' <_S HC(c)$.*
3. *$v_2 = v_1 - \kappa \cdot c.w$.*

We say that a set of elements Q **prefix-reduces** *f_1* **to** *f_2, denoted $f_1 \xrightarrow[p]{Q}{}^* f_2$, if there exists a sequence of one-step prefix-reductions*

$$f_1 \xrightarrow[p]{Q} \widetilde{f}_1 \xrightarrow[p]{Q} \cdots \widetilde{f}_t \xrightarrow[p]{Q} f_2$$

with $\widetilde{f}_i \in \mathcal{F}$. The definition of the terms **prefix-minimal** *and* **prefix inter-reduced** *corresponds to the one given in Definition 3.2.1.*

Example 5.1.5 *Let $A = \langle x_1, x_2 \rangle_{\mathbb{Z}}$, $P = \langle x_1, x_2 \mid x_1^2 - 1 \rangle_{\mathbb{Z}}, \mathcal{F} = \langle y \rangle_A$ and $\mathcal{M} = \langle y \mid y.x_1x_2x_1 - y.x_2, y.x_2x_1x_2 - y.x_1 \rangle_P$. We set $b_1 := \gamma_{(0)}(y)$. A possible MGE-procedure might have the following definition steps*

$$b_2 := \gamma_{(0)_1}(y.x_1), b_3 := \gamma_{(0)_2}(y.x_1x_2), b_4 := \gamma_{(0)_3}(y.x_1x_2x_1), b_5 := \gamma_{(0)_4}(y.x_2).$$

These definition-steps lead to the coincidence $c = b_5 - b_4$. If we are using the ordering induced by image, then $y.x_2^2 \in \mathcal{F}$ can be prefix-reduced by the

module-relation $r = y.x_1x_2x_1 - y.x_2$ *and accordingly*

$$y.x_2^2 \xrightarrow{r} y.x_1x_2x_1x_2,$$

as $HM(\gamma(r)) = b_5$ *is a prefix of* $\chi(y.x_2^2) = b_5.x_2$.

Remark 5.1.6 *Prefix-reduction rules on elements* $v \in \Sigma$ *which are induced by definition steps in order to bring an element of* $\mathcal{F}$ *into reach cannot lead to reductions on elements of* $\mathcal{F}$. *These are rules which are induced by the generators* H *of the submodule* Δ. *Since* $\mathcal{F} \cong \Sigma_{(\iota)_j}/(\Delta_{(\iota)_j})_A$ *for all* $(0)_0 \leq (\iota)_j \leq (\nu)_0$, *an element* $f \in \mathcal{F}$ *corresponds to an element of* $\Sigma/(\Delta)_A$, *therefore reduction rules by elements of* H *do not affect elements* $f \in \mathcal{F}$.

The image-induced ordering on the elements of $\mathcal{F}$ depends on the order in which the generating elements $b_1, \ldots, b_m$ are assigned to prefixes of relations. The assignment of an element $y.w$ depends on its position as a prefix of a relation and on where this relation appears for the first time in the set of relations *Rels*. Because of this, reduction induced by image might possibly lead to reductions on elements of $\mathcal{F}$ in an unexpected way. For instance in Example 5.1.5, if we were given an ordering by length of words then we would certainly have that $y.x_1x_2x_1x_2$ is greater than $y.x_2^2$. We will now show that prefix-reduction, using image-induced ordering on the elements of $\mathcal{F}$, does not lead to infinite sequences of reduction in the context of an MGE-procedure.

In order to ensure that the reduction process induced by an ordering is Noetherian, W. Adams and P. Loustaunau in [1] introduce the concept of a **term ordering** on the elements of a module. An ordering " $\succ_t$ " is called a term ordering if the following two conditions are satisfied:

1. Let $v \in \Sigma$, then $v.w \succ_t v$ for all $w \in X^* \setminus \varepsilon$;

2. Let $v_1, v_2 \in \Sigma$, if $v_2 \succ_t v_2$ then $v_2.w \succ_t v_1.w$ for all $w \in X^*$.

However, as we will see in the following example, the second condition on an ordering to be a term ordering does not necessarily need to hold for the image-induced ordering on $\mathcal{F}$ during an MGE-procedure:

Example 5.1.7 *Let* $\mathcal{M} = \langle y \mid y.x_1^2 - y.x_2x_1, 2 \cdot y.x_1^3 \rangle_P$ *and let* $P = \langle x_1, x_2 \rangle_{\mathbb{Z}}$. *We begin the procedure by setting* $b_1 = \gamma_{(0)_0}(y)$ *and* $B_{(0)_0} = \{b_1\}$. *We suppose that we will trace the relations in the order they are written in the presentation of* $\mathcal{M}$. *Tracing of the relation* $y.x_1^2 - y.x_2x_1$ *leads to*

$$b_2 = \gamma_{(0)_1}(y.x_1), b_3 = \gamma_{(0)_2}(y.x_1^2), \gamma_{(0)_3}(y.x_2) \text{ and } b_4 = \gamma_{(0)_4}(y.x_2x_1),$$

and the next relation $2 \cdot y.x_1^3$ *leads to*

$$b_6 = \gamma_{(1)_1}(y.x_1^3).$$

Since $b_3 \prec_{wei} b_4$ *as elements of* Σ, *it follows that* $y.x_1^2 \prec_{ii} y.x_2$, *however,* $y.x_1^2x_1 \succ_{ii} y.x_2x_1$ *as* $\chi(y.x_1^2x_1) = b_6$ *and* $\chi(y.x_2x_1) = b_5$.

Since it cannot be shown in general that the ordering induced by image on the elements of $\mathcal{F}$ is Noetherian, we have to check that in the case of prefix-reduction following the MGE-procedure no infinite descending reduction-sequences or any cycles in a reduction-sequence of elements of $\mathcal{F}$ are possible.

Recall that the reduction-rules are of two kinds. Those rules which come from the submodule Δ, which reduce the weight of elements of Σ, do not lead to reduction-rules on elements of $\mathcal{F}$. Moreover, since the weight of elements is bounded below by 0, neither descending sequences of reduction of infinite length on elements of Σ, nor cycles of reduction are possible if the reduction rule is strictly reducing the weight of elements.

Both the cases of reduction sequences as described above must be induced by reduction rules on elements of $\Sigma \backslash \langle B \rangle_S$. Therefore, it remains to investigate reduction-rules which are induced by coincidences. Since the sets of generators $B = \{b_1, \ldots, b_m\}$ are bounded below, infinite descending sequences of reduction are not possible on elements of $\langle B \rangle$ and we conclude that they must be impossible for the induced prefix-reduction on elements of $\mathcal{F}$. We now have to show that cycles in a reduction sequence of elements of $\mathcal{F}$ are not possible either.

Lemma 5.1.8 *If* G *is an MGE-basis of* Ψ, *then prefix-reduction of elements of* $\mathcal{F}$ *ordered by image-induced ordering by elements of* R, *where*

$R = \{\gamma^{-1}(\pi(g_1)), \ldots, \gamma^{-1}(\pi(g_t))\}$ for $g_i \in G$, does not lead to cycles in the reduction sequences.

Proof. Suppose there are elements $f_1, f_2 \in \mathcal{F}$ with

$$f_1 \xrightarrow[p]{} {}^* f_2 \xrightarrow[p]{} {}^* f_1$$

and let $\chi(f_i) = v_i \in \Sigma$ for $i \in \{1, 2\}$. If $f_1 \xrightarrow[p]{} {}^* f_2$ then there are $r_{i_1}, \ldots, r_{i_m}$ in R such that

$$\chi(f_1) = v_1 \xrightarrow[p]{r_{i_1}} \widetilde{v}_1, \zeta(\pi(\widetilde{v}_1)) \xrightarrow{r_{i_2}} \widetilde{v}_2, \ldots, \zeta(\pi(\widetilde{v}_{m-1})) \xrightarrow{r_{i_m}} \widetilde{v}_m,$$

where $\zeta(\pi(\widetilde{v}_m)) = \chi(f_2)$. Whenever there is $\widetilde{v}_j$ such that $\widetilde{v}_j$ is not contained in the image of the map χ, we have that $\widetilde{v}_j \neq \zeta(\pi(\widetilde{v}_j))$. In this case there is at least one summand of $\zeta(\pi(\widetilde{v}_j))$ which has strictly smaller weight than the corresponding summand of $\widetilde{v}_j$, because

$$\zeta(\pi(\widetilde{v}_j)) = \widetilde{v}_j - \sum_{k=1}^{n} h_{j_k}.a_{j_k},$$

where $a_{j_k} \in A$ and $h_{j_k} = b.x - b' \in H$, the generating set of the module Δ induced by the definition process.

Since the set G is an MGE-basis it follows that for v_1, v_2 and $g \in G$ with $v_1 \xrightarrow[p]{g} v_2$ we must always have that $Wei(v_1) \geq Wei(v_2)$. In order to obtain a cycle $f_1 \xrightarrow{*} f_2 \xrightarrow{*} f_1$, we then must have that $Wei(f_1) = Wei(f_2)$ and in particular $\widetilde{v}_i = \zeta(\pi(\widetilde{v}_i))$ for all $\widetilde{v}_i$ in the prefix reduction sequences $f_1 \xrightarrow{*} f_2$ and $f_2 \xrightarrow{*} f_1$.

The reduction-sequence

$$v_1 \xrightarrow[p]{} \widetilde{v}_1 \xrightarrow[p]{} \widetilde{v}_2 \cdots \xrightarrow[p]{} \widetilde{v}_{t-1} \xrightarrow[p]{} v_2$$

must therefore be induced by a set of coincidences, $\{c_1, \ldots c_t\} \subset G$. We will denote this set by C_1 and analogously the set leading to the reduction sequence $\chi(f_2) = v_2 \xrightarrow[p]{} {}^* v_1$ by C_2. Amongst the head monomials of the coincidences there is one which has the greatest index. We set

$$b_{max} := max\{HM(c_i) \mid c_i \in C_1\},$$

and let c_k denote the coincidence with $b_{max} = HM(c_k)$. Since b_{max} is the maximal element amongst the head monomials of the coincidences involved in this situation, it cannot have been added as a reduct of some other coincidence. Therefore b_{max} must have been a (not necessarily proper) prefix of a summand of v_1.

Therefore, in order to obtain the element $v_1 = \chi(f_1)$ again by the second sequence of reductions, we need that b_{max} is contained in the reduct of a coincidence $c_j \in C_2$, leading to one of the prefix reductions-rules of the sequence $v_2 \xrightarrow[p]{} {}^*v_1$. This, however, is a contradiction to the assumption that the set G is prefix inter-reduced. □

Corollary 5.1.9 *Prefix reduction on elements of $\mathcal{F}$ induced by a set of coincidences $C_1 = \{c_1, \ldots, c_t\}$ which have already been processed cannot lead to cycles in the reduction-sequences in an MGE-procedure.*

Proof. Whenever a new relation is traced in order to find a further coincidence the tracing uses the undeleted image. Tracing gives rise to a coincidence c which is minimal with respect to the set of previously computed coincidences C_1. In particular, $RED(c)$ cannot contain the head monomial of an earlier processed coincidence. We can conclude that we cannot obtain cycles of reduction on the elements of $\mathcal{F}$ in the MGE-procedure. □

5.2 Important Classes

Definition 5.2.1 *Let $|-|$ denote the congruence classes in $\mathcal{F}$ modulo the submodule $\mathcal{N}$ with generating set $R \subset \mathcal{F}$. We call a class $|f|$* **important with respect to** *R if we can choose a representative $\overline{f} \in |f|$ which is a prefix of an element of R and which moreover is prefix-minimal with respect to R by the image-induced ordering.*

Example 5.2.2 *Let $\mathcal{M} = \langle y \mid y.x_1^2 - y \rangle_P$ and $P = \langle x_1, x_2 \mid x_2^2 - x_1 \rangle_{\mathbb{Z}}$ and suppose that we have processed the relations $y.x_1^2 - y$ and $b_1.(x_2^2 - x_1)$ giving*

rise to the multiplication table

	del_b	$prod(b, x_1)$	$prod(b, x_2)$	$\gamma^{-1}(b)$	r_b
b_1	f	b_2	b_4	y	$\perp$
b_2	f	b_1	$\perp$	$y.x_1$	$\perp$
b_3	t	$\perp$	$\perp$	$y.x_1^2$	b_1
b_4	f	$\perp$	b_2	$y.x_2$	$\perp$
b_5	t	$\perp$	$\perp$	$y.x_2^2$	b_2

Then $\mathcal{F} = \langle y \rangle_A$ *and we are given a set* $R = \{y.x_1^2 - y, y.x_2^2 - y.x_1\}$ *and* $\mathcal{N} = \langle y.x_1^2 - y, y.x_2^2 - y.x_1 \rangle_A$. *The congruence classes of* $y, y.x_1$ *and* $y.x_2$ *of* $\mathcal{F}$ *modulo* $\mathcal{N}$ *are important with respect to* R. *There are however infinitely many congruence classes which are not important, for instance those classes containing the elements* $y.x_1x_2$ *or* $y.x_2x_1$.

In the following we will assume that $\mathcal{N}$ is a finitely generated A-submodule of the free A-module $\mathcal{F} = \langle Y \rangle_A$ where $Y = \{y_1, \ldots, y_n\}$ and we are computing an S-module presentation for the module $\mathcal{M}$.

Lemma 5.2.3 *Let* $\mathcal{N}$ *be generated by a set* R *where for every* $r \in R$ *we have that* $r := \gamma^{-1}(\pi(g))$ *for the elements* g *of an MGE-basis* G *of* Ψ. *Then a congruence class* $|f|_{\mathcal{N}}$ *is important if and only if it has a representative* $\overline{f}$ *such that* $\chi(\overline{f}) = b \in B^u$.

Proof. " $\Longrightarrow$: " We suppose that $|f|_{\mathcal{N}}$ is important. Then it has a representative $\overline{f}$ which is the prefix of an element r where $r = \gamma^{-1}(\pi(g))$ for $g \in G$. Such an element g is either an element of weight 0 or it is congruent modulo $(\Delta)_A$ to an element of weight 0. It follows from Lemma 5.1.2 that we must have that $Wei(r) \geq Wei(\overline{f})$ and therefore $\chi(r) \in \langle B \rangle_S$ implies that $\chi(\overline{f}) \in \langle B \rangle_S$ as well. Moreover, the map χ is injective and its image is not affected by coincidences, so it follows that $\chi(\overline{f}) \in B$. As $\overline{f}$ is prefix-minimal with respect to R we must have that $\chi(\overline{f}) \in B^u$.
" $\Longleftarrow$ " : Suppose there exists a representative $\overline{f}$ of a class $|f|_{\mathcal{N}}$ with $\chi(\overline{f}) \in B^u$. Since $Wei(\chi(\overline{f})) = 0$, an image for $\overline{f}$ under the map γ must have been defined at an earlier point and this must have happened in order to bring a relation into reach. Thus $\overline{f}$ is a prefix of a relation. As $\chi(\overline{f}) \in B^u$

it follows that there is no $g \in G$, where g corresponds to an applicable coincidence which prefix-reduces $\chi(\overline{f})$. Moreover, as $\chi(\overline{f}) \in B^u$, $\chi(\overline{f})$ cannot be prefix-reducible by an element of L since the elements of L have head coefficients which are not units of S. Therefore $\overline{f}$ must be prefix-minimal with respect to R and the class $|f|_{\mathcal{N}}$ is important. □

Corollary 5.2.4 *Let $\mathcal{N}$ be generated by the set R where for every $r \in R$ we have that $r := \gamma^{-1}(\pi(g))$ for all $g \in G$ where G is an MGE-basis of Ψ. Let $|f|_{\mathcal{N}}$ be a congruence class in $\mathcal{F}$. Then a representative $\overline{f}$ of $|f|_{\mathcal{N}}$ which is prefix-minimal with respect to R is unique.*

Proof. Suppose we are given a class $|f|_{\mathcal{N}}$ with representatives f_1, f_2 which are prefix-minimal with respect to R and $f_1 \neq f_2$. Since $f_1 + \mathcal{N} = f_2 + \mathcal{N}$ we have that $\chi(f_1 - f_2) = \chi(f_1) - \chi(f_2) \in \Psi$. However, as $f_1 \neq f_2$ it follows that $\gamma(f_1) \neq \gamma(f_2)$, therefore $\chi(f_1) - \chi(f_2) \in \Psi \backslash (\Delta)_A$. We conclude that $\chi(f_1)$ and $\chi(f_2)$ must differ by an element $v \in \Psi \backslash (\Delta)_A$, and without loss of generality we can assume that $\chi(f_1) - v = \chi(f_2)$.

As G is an MGE-basis of Ψ there must be $g \in G$ such that $HT(v) = \lambda \cdot HT(g).w$. This however implies that $\chi(f_1)$ is prefix-reducible by g and, as there is $r \in R$ with $r = \gamma^{-1}(\pi(g))$, it follows that the elements f_1 cannot be prefix-minimal with respect to R. □

Example 5.2.5 *In the case that a generating set R of the module $\mathcal{N}$ is not induced by an MGE-basis, a representative of $|-|_{\mathcal{N}}$ is not necessarily unique. Indeed let $R = \{y.x_1x_2x_1 - y.x_1^2, y.x_1x_2 - y\}$ and suppose that these elements are used in order to construct coincidences. Then these can lead to the following definitions for an MGE-procedure*

$$b_1.x_1 - b_2, b_2.x_1 - b_3, b_2.x_2 - b_4 \text{ and } b_4.x_1 - b_5.$$

This corresponds to the multiplication table

	del_b	$prod(b, x_1)$	$prod(b, x_2)$	$\gamma^{-1}(b)$	r_b
b_1	f	b_2	$\perp$	y	$\perp$
b_2	f	b_3	b_4	$y.x_1$	$\perp$
b_3	t	$\perp$	$\perp$	$y.x_1^2$	$\perp$
b_4	f	b_5	$\perp$	$y.x_1x_2$	$\perp$
b_5	t	$\perp$	$\perp$	$y.x_1x_2x_1$	$\perp$

Then the relation $y.x_1x_2x_1 - y.x_1^2$ *gives rise to the coincidence* $c_1 = b_5 - b_3$, *from* $y.x_1x_2 - y$ *we obtain* $c_2 = b_4 - b_1$. *If we would now omit the consequence* $b_3 - b_2$ *which is caused by the prefix-closure of* $b_4 - b_1$ *and* $b_4.x_1 - b_5 \xrightarrow{c_1} b_4.x_1 - b_3$, *and would only perform S-module reductions such as* $b_5 \longrightarrow b_3$ *and* $b_4 \longrightarrow b_1$. *We would obtain the generating set* $G = \{b_1.x_1 - b_2, b_2.x_1 - b_3, b_2.x_2 - b_1, b_4.x_1 - b_3, b_5 - b_3, b_4 - b_1\}$. *The generating set obtained from* $\gamma^{-1}(\pi(g))$ *for* $g \in G$ *is equal to* R *and accordingly the element* $y.x_1^2$ *is prefix-minimal with respect to* R. *However, following an MGE-procedure further would reveal that* $y.x_1^2$ *is not prefix-minimal at all and moreover that* $y.x_1^2$ *is in fact congruent to* $y.x_1$ *modulo* $\mathcal{N}$. *The prefix-closure would lead to a consequence,*

$$b_4.x_1 - b_1.x_1 \longrightarrow b_3 - b_2,$$

and therefore $\gamma^{-1}(\pi(b_3)) = y.x_1^2 \sim_{\mathcal{N}} y.x_1\gamma^{-1}(\pi(b_2))$. *This gives a new generating set*

$$\widetilde{G} = \{b_1.x_1 - b_2, b_2.x_1 - b_2, b_2.x_2 - b_1, b_4.x_1 - b_2, b_5 - b_2, b_4 - b_1, b_3 - b_2\}$$

which is an MGE-basis. The set $\widetilde{G}$ *also leads to a generating set* $\widetilde{R}$ *for* $\mathcal{N}$,

$$\widetilde{R} = \{y.x_1x_2x_1 - y.x_1, y.x_1x_2 - y, y.x_1^2 - y.x_1\}.$$

We can conclude that there are only two congruence classes modulo $\mathcal{N}$ *which are important with respect to* $\widetilde{R}$, *namely those classes for which we can choose the respective representatives* y *and* $y.x_1$.

Lemma 5.2.6 *Let* $\mathcal{F}$ *be a finitely generated A-module with a finitely generated submodule* $\mathcal{N}$. *Then there are a finite number of important congruence classes of elements of* $\mathcal{F}$ *modulo* $\mathcal{N}$.

Proof. Let $Y = \{y_1, \ldots, y_n\}$ denote the generating set of $\mathcal{F}$ and let R denote the generating set of $\mathcal{N}$. Then for all $r \in R$ we have that $r = \sum_{i=1}^{n} \sum_{w \in X^*} \lambda_{i,w} \cdot y_i.w$ with $\lambda_{i,w} \in S, y_i \in Y$ and $w \in X^*$, where $\lambda_{i,w} \neq 0$ only for a finite number of summands and where each $w \in X^*$ is a word of finite length. Therefore there can only exist a finite number of prefixes of elements of R, so in particular there is a finite number of such prefixes which are also prefix-minimal with respect to R. We conclude that only a finite number of congruence classes can be important. □

Lemma 5.2.7 *If $\mathcal{M} = \mathcal{F}/\mathcal{N}$ is P-module isomorphic to a P-module $\Theta_{(\nu)}$ that is finitely generated as S-module then every congruence class $|f|_{\mathcal{N}}$ of $f \in \mathcal{F}$ is either important with respect to some generating set R of $\mathcal{N}$, or it has a representative $\overline{f}$ which lies in the S-linear span of the representatives of such important congruence classes.*

Proof. Since $\mathcal{M} = \mathcal{F}/\mathcal{N}$ is isomorphic to a module with finite generating set as S-module it follows from Theorem 1.2.1 that $\mathcal{N}$ is finitely generated as an A-module, say by a finite set R. Then, by Lemma 5.2.6, the number of important congruence classes with respect to R must be finite.

Let $|f|_{\mathcal{N}}$ denote a congruence class where we suppose that it has a representative $\overline{f}$ which is prefix-minimal with respect to R but which is not a prefix of any $r \in R$. Then for all $w \in X^* \backslash \{\varepsilon\}$, $\overline{f}$ will be S-linearly independent of $\overline{f}.w$, which also must be prefix-minimal with respect to R. Moreover, $\overline{f}.w$ cannot be a prefix of a $r \in R$ either. We therefore obtain an infinite number of congruence classes of $\mathcal{F}$ modulo $\mathcal{N}$ with elements that are S-linearly independent. This, however, is a contradiction to the assumption that $\mathcal{M}$ is isomorphic to a finitely generated S-module. □

Corollary 5.2.8 *Let $\mathcal{N}$ be generated by the set $R := \{\gamma^{-1}(\pi(g)) \mid g \in G\}$ where G is an MGE-basis G of Ψ and suppose that $\mathcal{M} = \mathcal{F}/\mathcal{N}$ is P-module isomorphic to a P-module that is finitely generated as S-module. Then for all congruence classes $|f|_{\mathcal{N}}$ for $f \in \mathcal{F}$ we have that $\chi(\overline{f}) \in \langle B^u \rangle_S$.*

Proof. It follows from Lemma 5.2.6 that there are a finite number of important congruence classes. Suppose there are m, and let $\overline{f}_1, \ldots, \overline{f}_m$ denote the prefix-minimal representatives of these. Now let $|f|_{\mathcal{N}}$ denote a congruence class in $\mathcal{F}$ which is not important with prefix-minimal representative $\overline{f}$. Then, by Lemma 5.2.7, we have that $\overline{f} = \sum_{i=1}^{m} \lambda_i \cdot \overline{f}_i$. As χ is an S-module homomorphism it follows immediately that $\chi(\overline{f}) = \sum_{i=1}^{m} \lambda_i \cdot \chi(\overline{f}_i)$, and therefore $\chi(\overline{f}) \in \langle B^u \rangle_S$ follows. □

5.3 The Final State of an MGE-procedure

Definition 5.3.1 *We say that the multiplication table T, belonging to an MGE-procedure at a certain stage (ι), is* **closed** *if for all $b \in B^u$ and for all $x \in X$ the product "$\star$" of $\Sigma/(\Psi)_A$ satisfies that $(b + \Psi) \star x \in \langle B^u \rangle_S + \Psi$.*

Lemma 5.3.2 *Suppose we are at stage (ι) of an MGE-procedure, with multiplication table T and where $Cp = \emptyset$. We denote by $G = \widetilde{T} \cup L$ the generating set of Ψ and we denote by R the generating set of $\mathcal{N}_{(\iota)}$ with $R := \{\gamma^{-1}(\pi(g)) \mid g \in G\}$.*

Then T is closed if and only if for all $f \in \mathcal{F}$ a congruence class $|f|_{(\iota)}$ in $\mathcal{F}$ modulo $\mathcal{N}_{(\iota)}$ is either important or it has a representative $\overline{f}$, prefix-minimal with respect to R, such that $\overline{f}$ lies in the S-linear span of the representatives of the important congruence classes.

Proof. We have seen in Lemma 4.2.5 that the entries of T correspond to a certain subset of the generating set G of Ψ. Since the coincidence stack Cp is empty, it follows from Lemma 4.2.15 that the set G in fact forms an MGE-basis of Ψ.

" $\Longrightarrow$ " : Suppose that T is closed. Then for all $b \in B^u$ and $x \in X$ we have that $(b + \Psi) \star x \in \langle B^u \rangle_S$, so the free product is congruent to an element $v \in \langle B^u \rangle_S$ modulo Ψ. Hence there is a $g \in G$ such that $g = b.x - v$. Therefore for all $z \in \Sigma^u$ with $Wei(z) > 0$ there is $\overline{z} \in \langle B^u \rangle_S$ such that z is congruent modulo Ψ to $\overline{z}$.

Now suppose we are given a congruence class $|f|_{(\iota)}$ of $f \in \mathcal{F}$ and we choose a representative $\overline{f}$ which is prefix-minimal with respect to R. Then,

as $\overline{f}$ is prefix-minimal, $\chi(\overline{f}) \in \Sigma^u$, and as T is closed, $\chi(\overline{f}) \in \langle B^u \rangle_S$; otherwise $\chi(\overline{f})$ would not be prefix-minimal with respect to G which would be a contradiction to the choice of $\overline{f}$. From the definition of the module Σ it follows that for all $b_i \in B^u$ we have that $b_i = \chi(f_i)$ for some element $f_i \in \mathcal{F}$. Thus f_i must in fact be a prefix-minimal representative $\overline{f}_i$ of its congruence class modulo $\mathcal{N}_{(\iota)}$, which then has to be an important class. Therefore $\chi(\overline{f}) = \sum_{i=1}^{m} \lambda_i \cdot b_i$ for $b_i \in B^u$ and so $\overline{f} = \sum_{i=1}^{m} \lambda_i \cdot \gamma^{-1}(\pi(b_i)) = \sum_{i=1}^{m} \lambda_i \cdot \overline{f}_i$.

" $\Longleftarrow$ " : Let $\overline{f}$ be the prefix-minimal representative of a class $|f|_{(\iota)}$ in $\mathcal{F}$. Then $\overline{f} = \sum_{i=1}^{m} \lambda_i \cdot \overline{f}_i$ where the $\overline{f}_i$ are the prefix-minimal representatives of some important congruence classes. Therefore $\chi(\overline{f}) = \sum_{i=1}^{m} \lambda_i \cdot b_i$ with $b_i \in B^u$. Since $Cp = \emptyset$ it follows from Lemma 2.4.3 that $\mathcal{F}/\mathcal{N} \cong \Sigma/\Psi$ and therefore $(b + \Psi) \star x \in \langle B^u \rangle_S + \Psi$ for all $b \in B^u$ and $x \in X$. We conclude that the multiplication table T is closed. □

Definition 5.3.3 *Let G denote the generating set of Ψ. We say that a torsion sequence $L \subset G$ is* **closed** *if for all $l \in L, x \in X$ the element $l \star x$ has been considered as a coincidence and at some stage of the procedure has been added to the coincidence stack Cp.*

We will now introduce certain conditions on a state (ι) of an MGE-procedure. We will show, in the case that these conditions are satisfied for the module

$$\Theta_{(\iota)} := \Sigma_{(\iota)}/\Psi_{(\iota)}$$

which is constructed by the MGE-procedure, that $\Theta_{(\iota)}$ is isomorphic as a P-module to $\mathcal{M}$.

Definition 5.3.4 *Let G denote the generating set of $\Psi_{(\iota)}$. We call a state (ι) of an MGE-procedure a* **final state**, *if the following conditions for the tools accompanying the state (ι), are satisfied:*

1. *The multiplication table T is closed.*

2. *The stack Cp containing the pending coincidences is empty.*

3. *The torsion sequence L is closed, therefore $(\Lambda)_A = \Lambda$ for the S-linear span Λ of L.*

4. *For all $b \in B^u$ and all algebra-relations $r \in R \subset A$ we have that $b.r$ can be prefix-reduced to 0 by G.*

5. *For each of the module-relations $\omega \in U \subset \mathcal{F}$ we have that $\chi(\omega)$ can be prefix-reduced to 0 by G.*

When the MGE-procedure has reached a final state, since all of the algebra- and module relations must hold on the respective generators $b \in B_{(\nu)}$, we can conclude that we have obtained an A-submodule

$$\mathcal{N}_{(\nu)} = \langle r_{(1)}, \ldots, r_{(\nu)} \rangle$$

such that $\mathcal{N}_{(\nu)} \cong \mathcal{N}_A$ for $\mathcal{M} = \mathcal{F}/\mathcal{N}_A$. If we additionally assume that we are given a reduced torsion sequence which is in pivot-form then the condition on Cp ensures that the generating set G of $\Psi_{(\nu)}$ forms an MGE-basis. Moreover, we can show the following:

Proposition 5.3.5 *If the MGE-procedure is in a final state (ν) where the given torsion sequence $L_{(\nu)}$ is reduced and in pivot form, then the following P-module isomorphisms hold:*

$$\frac{\langle B^u_{(\nu)} \rangle}{\Lambda_{(\nu)}} \cong \Theta_{(\nu)} \cong \mathcal{M}_P.$$

Proof. We aim to construct $\Theta_{(\nu)}$ as the quotient-module $\Sigma_{(\nu)}/\Psi_{(\nu)}$. In a final state of an MGE-procedure it is ensured that $Cp = \emptyset$, so the module $\Psi_{(\nu)}$ is actually of the form of the module $\Upsilon_{(\nu)}$ as stated in Lemma 2.4.3. From this Lemma it then follows that

$$\Theta_{(\nu)} = \Sigma_{(\nu)}/\Psi_{(\nu)} \cong \big(\Sigma_{(\nu)}/(\Delta_{(\nu)})_A\big)/(\Omega_{(\nu)})_A.$$

In the following we shall omit the index "(ν)" for the S-modules concerned. The S-module Δ is the submodule of Σ generated by elements $b.x - b'$, obtained from definition steps, and the module Ω is that submodule of $\Sigma/(\Delta)_A$ which is generated by the coincidences $Ca \cup L$.

The construction of the modules Σ, Δ and Ω implies that

$$(\Sigma/(\Delta)_A)/(\Omega)_A \cong \mathcal{F}/\mathcal{N}_{(\nu)},$$

where the latter is just $\mathcal{M}_{(\nu)}$.

Conditions 4 and 5 of the definition of a final state imply that every relation $r \in Rels$ of $\mathcal{M}$ is contained in the A-linear span of the relations which have been chosen for the generating of coincidences so far. Thus for all $r \in Rels$ we have

$$r \in \langle \widetilde{r}_1, \ldots, \widetilde{r}_t \rangle_A = \mathcal{N}_{(\nu)},$$

and we can conclude that $\mathcal{M}_{(\nu)} \cong \mathcal{M}$. This confirms the isomorphism on the right hand side of the assumption.

Let G denote the generating set of Ψ. By condition 2 of the definition of a final state we know that $Cp = \emptyset$. As the given torsion sequence is reduced and in pivot-form it follows from Lemma 4.2.15 that G is an MGE-basis of Ψ. Condition 1 of a final state states that the multiplication table T must be closed. Therefore T, in particular, is connected and it follows from Proposition 4.2.22 that $\Theta \cong_A \Sigma/\Psi \cong_A \Sigma^u/\Phi$ where Φ is the A-module as defined in Proposition 4.2.22 Because of condition 4 of a final state we know that all algebra-relations $r \in R$ are satisfied in these quotient-modules and we can conclude that the given isomorphism must be a P-module isomorphism.

Since T is closed we have $(b + \Psi) \star x \in \langle B^u \rangle_S$ for all $b \in B^u$ and $x \in X$. Thus for every $z \in \Sigma^u$ with $Wei(z) > 0$ there exists $\overline{z} \in \langle B^u \rangle_S$ which is minimal with respect to the generators of weight 1 of Φ. These generators are just all those generators which are not elements of the torsion sequence L and we can conclude that $\Sigma^u/\Phi \cong_P \langle B^u \rangle_S/\Lambda$. Condition 3 of a final state implies that the S-linear span of the torsion sequence is closed with respect to the product " $\star$ " in Σ/Ψ, so $\Lambda = (\Lambda)_A$ and

$$\Theta = \Sigma/\Psi \cong_P \langle B^u \rangle_S/\Lambda.$$

□

Corollary 5.3.6 *If the MGE-procedure is in a final state* (ν) *then there exists a finite number of important congruence classes* $|f_1|_{(\nu)}, \ldots, |f_t|_{(\nu)}$ *with* $\chi(\overline{f}_j) = b_j \in B^u$ *for all* $1 \leq j \leq t$. *Moreover, every congruence class in* $\mathcal{F}$ *modulo* $\mathcal{N}_{(\nu)}$ *then has a prefix-minimal representative* $\overline{f}$ *such that* $\chi(\overline{f}) \in \langle B^u \rangle_S$.

Proof. If the MGE-procedure is in a final state, all relations $r \in Rels$ of $\mathcal{M}_A$ are satisfied in the constructed module $\Theta_{(\nu)}$ and it follows that there exists a finite generating set for the module $\mathcal{N} = \langle Rels \rangle_A$, namely the one of the module $\mathcal{N}_{(\nu)}$ constructed by the MGE-procedure. As $\mathcal{N}$ is finitely generated we can deduce from Lemma 5.2.6 that there are finitely many important congruence classes $|f_j|$ of $\mathcal{F}$ modulo $\mathcal{N}$ for which, by Lemma 5.2.3, there exists a representative $\overline{f}_j$ such that $\chi(\overline{f}_j) = b \in B^u \subset \Sigma$.

Moreover, it follows from Proposition 5.3.5 that $\mathcal{M}$ is P-module isomorphic to $\Theta_{(\nu)}$. We can conclude from Corollary 5.2.8 that for all congruence classes of $\mathcal{F}$ modulo $\mathcal{N}$ there exists a representative $\overline{f}$ such that $\chi(\overline{f}) \in \langle B^u \rangle_S$, and since $\chi(\overline{f})$ is contained in the S-linear span of the undeleted S-module generators and is of weight 0 it follows that $\overline{f}$ must be prefix-minimal as well. □

The following definition of a fair strategy is necessary in order to prove the termination of the MGE-procedure. The condition that the strategy of an MGE-procedure is fair corresponds to the condition formulated by N. Mendelsohn [30] in the case of the Todd-Coxeter procedure for coset enumeration.

Definition 5.3.7 *We call a strategy of an MGE-procedure* **fair** *if it is guaranteed for every* $b \in B^u_{(\iota)_k}$ *at each stage* $(\iota)_k$ *of the MGE-procedure that we reach after a finite number of steps a stage* $(\iota'')_{k''}$ *such that either* $b \in B^d_{(\iota'')_{k''}}$ *or where for every* $x \in X$ *an* S*-module generator* $b' \in B'$ *has been defined such that* $b.x - b'$ *has been contained in the generating set of* $\Delta_{(\iota')_{k'}}$ *for some* $(\iota')_{k'} \leq (\iota'')_{k''}$.

Theorem 5.3.8 *Let $\mathcal{F}$ be a finitely generated and free A-module. If $\mathcal{M}_P$ is P-module isomorphic to a P-module $\Theta_{(\nu)}$ that is finitely generated as S-module, then the computation of the MGE-procedure reaches a final state where the given torsion sequence is reduced and in pivot-form, provided that we are following a fair strategy.*

Proof. We can consider $\mathcal{M}$ again as A-module, where $\mathcal{M}$ is the quotient-module of $\mathcal{F}$ by the submodule $\mathcal{N} = \langle Rels \rangle$. Thus the submodule $\mathcal{N} \subset \mathcal{F}$ is generated by an infinite set of module-relations of $\mathcal{M}_A$. In the case that $\mathcal{M}$ is isomorphic to a module with finite S-module generating set, we showed in Theorem 1.2.1 that a finite A-module generating set for $\mathcal{N}$ exists. Therefore, if a finitely generated S-module $\Theta_{(\nu)}$ exists, then there is a finite ascending sequence of A-modules

$$\mathcal{N}_{(1)} \subset \cdots \subset \mathcal{N}_{(\nu)} = \mathcal{N}.$$

where $\mathcal{N}_{(\iota)} = \langle r_{(1)}, \ldots, r_{(\iota)} \rangle$. To each of these modules $\mathcal{N}_{(\iota)}$ we assign S-modules $\Sigma_{(\iota)}, \Delta_{(\iota)}, \Pi_{(\iota)}$ and $\Psi_{(\iota)}$ as described in Chapter 2 and Chapter 4.

We have seen in Lemma 4.2.10 that the routine HANDLE INAPPLICABLE COINCIDENCES maintains the properties of a torsion sequence being reduced and in pivot-form. Since CLEAN TORSION SEQUENCE only modifies the reducts of elements of the torsion sequence, the same holds for this routine and it follows that we can obtain a reduced torsion sequence in pivot-form.

Let $r \in Rels \backslash \{r_{(1)}, \ldots, r_{(\iota-1)}\}$. Then in the case that r is not contained in the module $\mathcal{N}_{(\iota-1)}$ it will lead to a new coincidence c of elements of $\Sigma_{(\iota-1)}/(\Delta_{(\iota-1)})_A$. The coincidence c will be added to Cp, and we showed in Proposition 4.2.20 that the procedure CLEARING COINCIDENCES is a terminating procedure which will compute an MGE-basis G of a module Ψ such that, by Proposition 4.2.22, we have that

$$\mathcal{F}/\mathcal{N}_{(\iota)} \cong_A \Sigma/\Psi \cong_A \Sigma^u/\Phi.$$

We set $\widetilde{\mathcal{N}}_{(\iota)} = \langle \widetilde{R}_{(\iota)} \rangle_A$ where for $\widetilde{r} \in \widetilde{R}_{(\iota)}$ we have that $\widetilde{r}_j := \gamma^{-1}(\pi(g))$ for $g \in G$, so it follows that $\mathcal{N}_{(\iota)} \cong \widetilde{\mathcal{N}}_{(\iota)}$. If the strategy used by the MGE-procedure is fair in the sense that not only relations which are linearly

dependent will be investigated then we will find after a finite number of steps a relation $r_{(\nu)} \in Rels$ such that $\langle \widetilde{R}_{(\nu-1)}, r\rangle_A = \mathcal{N}$. Following the usual procedure we can obtain an MGE-basis for $\Psi_{(\nu)}$; thus Lemma 4.2.19 implies that $\langle Cp\rangle_A \subset \langle \widetilde{T} \cup L\rangle_A$. Therefore the coincidences contained in Cp will not lead to any further reductions of the elements of $\widetilde{T} \cup L$. Accordingly they will not give rise to any further consequences which might lead to any further definition steps either. Then after a finite number of steps all pending coincidences will have been processed and we obtain $Cp = \emptyset$.

For every $r \in Rels$ we must have that $r \in \widetilde{\mathcal{N}}_{(\nu)}$, and accordingly we have $\chi(r) \in \Psi_{(\nu)}$ for all $r \in Rels$. From this the conditions 4. and 5. of Definition 5.3.4 follow.

We will now suppose that the multiplication table T is not closed. By assumption, $\mathcal{M}$ is isomorphic to a P-module with finite S-module generating set, and since $\widetilde{\mathcal{N}}_{(\nu)} = \mathcal{N}$ we can conclude that T must become closed after a finite number of steps. Every further coincidence must be trivial, so cannot lead to deletion of an S-module generator $b \in B^u_{(\nu)}$, and each definition step of a new S-module generator must lead to a coincidence, removing the newly defined row again. Since $\widetilde{\mathcal{N}}_{(\nu)} = \mathcal{N}$, those coincidences can only affect the newly defined S-module generators. Therefore, we will obtain a multiplication table T that is closed after a finite number of steps if it is ensured that we follow a fair strategy.

Since T is closed we have that $b \star x \in \langle B^u\rangle$ for all $b \in B^u$ and $x \in X$. Therefore the A-module closure of $\Lambda_{(\nu)}$ with respect to the product " $\star$ " must be contained as a submodule in $\langle B^u\rangle_S$. The submodule of a finitely generated module is finitely generated itself, so $(\Lambda)_A$ must be finitely generated itself and so after adding a finite number of generators we will obtain a torsion sequence L such that for $\Lambda = \langle L\rangle_S$ we have that $(\Lambda)_A = \Lambda$. Then, all conditions of a final state are satisfied. □

Remark 5.3.9 *It is possible that an actual MGE-procedure terminates even if the table is not closed. Suppose we have been computing an S-module Θ for a finitely presented P-module $\mathcal{M}$ where $P = \langle X \mid R\rangle_S$. This situation is only possible if there are algebra generators $\{x_1, \ldots, x_t\} \subset X$ which*

are not contained in any relations $r \in Rels$. Therefore these generators act freely on the S-module generators $b \in B^u$ of Θ and so the module $\mathcal{M}$ is not P-module isomorphic to a P-module with finite S-module generating set. The output provides a description of a module over a finitely generated algebra P' with strictly smaller generating set. We can interpret the output as a finitely generated S-module Θ that has been obtained from a module $\mathcal{M}'_{P'}$ where $P' = \langle X' \mid R \rangle_S$ and $X' = X \backslash \{x_1, \ldots, x_t\}$. Situations like this can be circumvented if it is ensured that each $x \in X$ is contained in at least one relation $r \in Rels$.

Chapter 6

A Schreier Presentation

In this chapter we will describe a method to obtain an A-module presentation of a certain P-module $\widehat{\mathcal{N}}_{\mathcal{P}}$. The module $\widehat{\mathcal{N}}_{\mathcal{P}}$ is the submodule of the free P-module $\mathcal{D}$ such that $\mathcal{M}_P = \mathcal{D}/\widehat{\mathcal{N}}$. This construction in particular uses the results obtained from a terminated MGE-computation for the module $\mathcal{M}$. In our description we follow the ideas presented by C. Sims in [41].

Section 6.1 We will explain how, from a given MGE-procedure, we can obtain a set of Schreier-generators, denoted E, for $\widehat{\mathcal{N}}$. Moreover certain linear dependencies between elements contained in the A-linear span of these Schreier-generators will be described.

Section 6.2 We will introduce relations on the set of Schreier generators E, which must be satisfied in order to obtain a module with generating set E which is isomorphic to $\widehat{\mathcal{N}}$. Moreover we will provide an upper bound for the size of the set of generators and for the set of the needed relations.

6.1 Generators for a Submodule

The MGE procedure aims to compute a generating set for an S-module Θ which is isomorphic to a finitely presented P-module $\mathcal{M}$ where P denotes the finitely presented algebra $P = \langle X \mid R \rangle_S$. The algebra P is the quotient of the free algebra $A = \langle X \rangle_S$ by the two-sided ideal $I = \langle ARA \rangle$ which is generated by the finite set R. We can consider $\mathcal{M}$ as an A-module as well, as has been described in Section 2.1, and as an A-module it is the

quotient-module

$$\mathcal{M}_A = \mathcal{F}/\mathcal{N}$$

of the finitely generated and free A-module $\mathcal{F} = \langle Y \rangle_A$ by the submodule which is defined as $\mathcal{N}_A = \langle Rels \rangle_A$ where $Rels := U \cup YX^*R$ is the infinite set of relations formed from the set R and the set $U \subset \mathcal{F}$ of module-relations of $\mathcal{M}$.

We showed in Theorem 1.2.1 that there must exist a finite generating set of the A-module $\mathcal{N}$ in the case that $\mathcal{M}$ is isomorphic to a finitely generated S-module. In that theorem an argument was used which follows the idea of the argument used in the Theorem of Schreier-generators for subgroups of finite index of finitely generated groups (see for instance [40, 41, 17]).

As a P-module, $\mathcal{M}$ is of the following form

$$\mathcal{M} = \mathcal{D}/\widehat{\mathcal{N}},$$

where $\mathcal{D}$ is the free P-module generated by a set Y' which is in bijection to the generating set Y of $\mathcal{F}$ and where $\widehat{\mathcal{N}}$ is a P-submodule of $\mathcal{D}$.

Lemma 6.1.1 *If $\mathcal{M}$ is P-module isomorphic to a finitely generated S-module then there exists a finite generating set for $\widehat{\mathcal{N}}$.*

Proof. We can consider $\mathcal{D}$ as an A-module as well: an element $d \in \mathcal{D}$ is of the form $d = \sum_{i=1}^{n} y_i.a_i + \langle YX^*R \rangle_A$. Accordingly we can define the canonical quotient map

$$\phi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}$$

which is an A-module homomorphism, and the image of the submodule $\mathcal{N}_A$ under ϕ is the module $\widehat{\mathcal{N}}_A$. In the case that $\mathcal{N}$ is finitely generated we can conclude that $\widehat{\mathcal{N}}$ must be finitely generated as A-module, and so also as P-module, since ϕ is an A-module homomorphism. □

We will describe how we can construct a presentation of the module $\widehat{\mathcal{N}} \subset \mathcal{D}$, considered as module over the free algebra A, from a given MGE-procedure which has terminated. In doing this, we follow the ideas of C. Sims as presented in [41], Chapter 6. Therefore our approach corresponds to

the Reidemeister-Schreier procedure for subgroups of finite index of finitely presented groups.

We suppose that we have applied an MGE-procedure to a module $\mathcal{M}$ which, as an S-module, has a finite generating set and moreover that the procedure has terminated, having successfully constructed a finitely generated S-module Θ which is isomorphic to $\mathcal{M}$. In accordance with previous chapters we will denote the resulting generating set of Θ again by B^u.

We assume that the MGE-procedure has terminated with an accompanying closed multiplication table T. For all $b \in B^u$ and all $x \in X$ we have that $b.x \sim_\Psi v$ where $v \in \langle B^u \rangle_S$. As $Cp = \emptyset$, the module Ψ constructed by the MGE-procedure has the form of the module Υ described in Chapter 2. As has been described in the previous chapters, the generating set G of Υ (or Ψ) is given by the following elements of Σ :

- Entries of rows $b \in B^u$ of the multiplication table correspond to generators $g = b.x - v$ of weight 1;
- Rows $b \in B^d$ together with the replacement r_b in the multiplication table correspond to applicable coincidences which give generators $g = b - r_b$;
- The inapplicable coincidences stored in L.

We will construct from the elements of G a generating set for $\widehat{\mathcal{N}}$ as follows. By using Lemma 2.4.3 we have that

$$\mathcal{M} = \mathcal{F}/\mathcal{N} \cong \Sigma/\Upsilon = \Sigma/\Psi.$$

An element of $\mathcal{M}$ corresponds to a congruence class of elements of $\mathcal{F}$ modulo $\mathcal{N}$, so we can assign to every generator $b \in B^u$ a representative $f_b = \sum_{i=1} y_i.a_i \in \mathcal{F}$ and accordingly we can set $\widehat{f_b} := \phi(f_b) \in \mathcal{D}$. We will choose the representative f_b for $b \in B^u$ as $f_b := \gamma^{-1}(\pi(b))$. In the case of the MGE-procedure where we obtain elements $b \in B^u$ from the process of tracing prefixes of relations of $\mathcal{M}$, a representative corresponding to $b \in B^u$ will be of the form $f_b = y.w$ with $w \in X^*$.

An element $b \in B^u$ is certainly (prefix-)minimal with respect to the MGE-basis G of Υ which implies that f_b is minimal with respect to the image-induced ordering. Accordingly we define the representative f_v for an element $v \in \Sigma$ as the element corresponding to the unique minimal element $\overline{v} \in \langle B^u \rangle_S$ contained in the congruence class of v modulo Υ, and we therefore set

$$f_v := \gamma^{-1}(\pi(\overline{v})).$$

It follows that $f_{\overline{v}} = f_0 = 0$ is the representative of the class of those elements which are contained in Υ.

In the case that $v \xrightarrow[p]{G} \overline{v} \in \langle B^u \rangle$ it is implied that $\gamma^{-1}(\pi(v)) \sim_{\mathcal{N}} \gamma^{-1}(\pi(\overline{v}))$. In particular, for an element $b.x$, since the table is closed, there exists $\overline{v} \in \langle B^u \rangle_S$ with $b.x \sim_\Upsilon \overline{v}$ and therefore $\gamma^{-1}(\pi(b.x)) \sim_{\mathcal{N}} \gamma^{-1}(\pi(\overline{v}))$. It follows that

$$f_b.x - f_{\overline{v}} \in \mathcal{N}$$

and accordingly $\phi(f_b.x - f_{\overline{v}}) \in \widehat{\mathcal{N}}$. Moreover, if $b.x \not\sim_{(\Delta)_A} \overline{v}$, then $f_b.x \sim_{\mathcal{N}} f_{\overline{v}}$. However $f_b.x \neq f_{\overline{v}} = \gamma^{-1}(\pi(\overline{v}))$ which yields an element $f_b.x - f_{\overline{v}} \neq 0$.

Similarly if we are given an S-module generator $b \in B^u$ which is a torsion-element of $\Theta = \Sigma/\Upsilon$ then there exists a coefficient $\lambda \in S$ such that $\lambda \cdot b = 0 \in \Theta$. Accordingly $\lambda \cdot b \in \Upsilon$, which implies that

$$\lambda \cdot f_b \neq f_{\lambda \cdot b}.$$

As $f_{\lambda \cdot b} = f_0$ we see $\lambda \cdot f_b \in \mathcal{N}$ and $\lambda \cdot \phi(f_b) \in \widehat{\mathcal{N}}$. Furthermore, in the case that for an A-module generator $y_k \in Y$ of $\mathcal{M}$ we have that $y_k \sim_{\mathcal{N}} \sum_{i=1}^{k-j} \lambda_i \cdot y_i$ this leads to $f_{b_k} \sim_{\mathcal{N}} f_{\sum_{i=1}^{k-j} \lambda_i \cdot b_i}$ where we have set $b_i := \gamma(y_i)$ for all $1 \leq i \leq k$ in the course of an MGE-procedure.

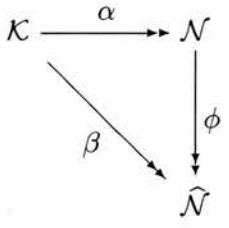
Lemma 6.1.2 *Let $E := \{\gamma^{-1}(\pi(G))\}$ where G is an MGE-basis of Υ. The set E consists of elements of $e \in \mathcal{F}$ such that $e = f_b.x - f_v, e = \sum_{j=1}^{m} \lambda_j \cdot f_{b_j}$ where λ_j are non-units of S, or $e = y_k - f_{b_k} = y_k - \sum_{i=1}^{k-1} \lambda_i \cdot y_i$.*

Proof. The set G consists of elements of $\widetilde{T}$, the set obtained from the multiplication table T, together with the elements of the torsion sequence L. Thus the elements of $\widetilde{T}$ are either of the form $b.x - v$, with $b \in B^u$ and

$v \in \langle B^u \rangle_S$, or $b - r_b$ where $b \in B^d$ and $r_b \in \langle B^u \rangle_S$; the elements $l \in L$ are of the form $\sum_{j=1}^{m} \lambda_j \cdot b_j \in \langle B^u \rangle_S$ where $HT(l) \sim_\Upsilon RED(l)$ and $b_j \in B^u$ for all summands b_j of $l \in L$.

We conclude that those elements of G which are induced by $\widetilde{T}$ give rise to $e \in E$ such that $e = f_b.x - f_{b.x}$ or $e = y_k - f_{b_k} = y_k - \sum_{i=1}^{k-1} \lambda_i \cdot y_i$, for A-module generators $y \in Y$, and that the elements of L lead to elements $e \in E$ with $e = \sum_{j=1}^{m} \lambda_j \cdot f_{b_j}$. As all $g \in G$ are minimal with respect to $G \backslash \{g\}$ the assumption follows. □

By the construction of the modules Δ and Υ we know that $\mathcal{N}$ is A-module isomorphic to $\Upsilon/(\Delta)_A$, and therefore the so-defined set E is a generating set for $\mathcal{N}$. We denote by $\mathcal{K} := \langle E \rangle_A$ the free A-module generated by E. Thus we obtain a homomorphism $\alpha : \mathcal{K} \longrightarrow \mathcal{F}$ which maps onto $\mathcal{N}_A \subset \mathcal{F}$. Furthermore, composition with $\phi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}$ yields an A-module epimorphism $\beta : \mathcal{K} \longrightarrow\!\!\!\!\!\rightarrow \widehat{\mathcal{N}}$,



Remark 6.1.3 *In order to emphasise that an entry of the multiplication table leads to a generator $g \in G$ where $g = b.x - prod(b, x)$, we can insert the respective generators into the multiplication table.*

We will now show in the following example how to obtain a set E from a given MGE-procedure.

Example 6.1.4 *Let $P = \langle x_1, x_2 \mid x_2x_1 - x_1x_2, x_2 - x_1x_2 \rangle_{\mathbb{Z}}$ and let $\mathcal{M} = \langle y_1, y_2 \mid y_1.x_2^3 - y_1.x_1x_2 - y_1, y_1.x_1^2 - y_1, 2 \cdot y_2.x_1x_2, y_2 - 2 \cdot y_1 \rangle_P$. A possible way of assigning S-module generators to the prefixes of the relations leads to the table on p. 137. At this stage, we have already computed the following relations: the module relation $y_1.x_2^3 - y_1.x_1x_2 - y_1$ has lead to the coincidence $b_7 - b_4 - b_1$, the module relation $y_1.x_1^2 - y_1$ to $b_8 - b_1$. The module-relation*

$2 \cdot y_2.x_1x_2$ *gives rise to the inapplicable coincidence* $2 \cdot b_{10}$, *so this element gets added to the torsion sequence:* $L = [2 \cdot b_{10}]$. *The relation* $2 \cdot y_2 - y_1$ *leads to* $b_2 - 2 \cdot b_1$ *and accordingly to* $b_9 - 2 \cdot b_3$, *the element contained in the torsion sequence reduces to* $4 \cdot b_4$.

Application of the algebra-relations at b_1 *led to* $b_1.x_2x_1 - b_1.x_1x_2 \longrightarrow b_{11} - b_4$ *and* $b_1.x_2 - b_1.x_1x_2 \longrightarrow b_5 - b_4$. *The latter coincidence then gave rise to the consequences* $b_4 - b_{12}$ *and* $b_6 - b_{13}$.

Application of the algebra relations at b_3 *only led to the trivial coincidence* $b_4 - b_4$; *application at* b_4 *however has lead to* $b_4.x_2x_1 - b_4.x_1x_2 \longrightarrow b_{14} - b_6$. *The relation* $b_4.x_2 - b_4.x_1x_2$ *only led to the trivial coincidence* $b_6 - b_6$.

	$prod(b, x_1)$	$prod(b, x_2)$	del_b	r_b	$\gamma^{-1}(\pi(b))$
b_1	b_3	b_5	f	$\perp$	y_1
b_2	$\perp$	$\perp$	t	$2 \cdot b_1$	y_2
b_3	b_8	b_4	f	$\perp$	$y_1.x_1$
b_4	b_{12}	b_{13}	f	$\perp$	$y_1.x_1x_2$
b_5	$\perp$	$\perp$	t	b_4	$y_1.x_2$
b_6	b_{14}	b_7	f	$\perp$	$y_1.x_2^2$
b_7	$\perp$	$\perp$	t	$b_4 + b_1$	$y_1.x_2^3$
b_8	$\perp$	$\perp$	t	b_1	$y_1.x_1^2$
b_9	$\perp$	$\perp$	t	$2 \cdot b_3$	$y_2.x_1$
b_{10}	$\perp$	$\perp$	t	$2 \cdot b_4$	$y_2.x_1x_2$
b_{11}	$\perp$	$\perp$	t	b_4	$y_1.x_2x_1$
b_{12}	$\perp$	$\perp$	t	b_4	$y_1.x_1x_2x_1$
b_{13}	$\perp$	$\perp$	t	b_6	$y_1.x_1x_2^2$
b_{14}	$\perp$	$\perp$	t	b_6	$y_1.x_2^2x_1$

Since the generator b_5 *has been deleted we will now apply the algebra-relations to* b_6. *We obtain* $b_6.x_2x_1 - b_6.x_1x_2 \longrightarrow b_3 - b_1$. *This coincidence does not lead to new consequences. The relation* $x_2 - x_1x_2$ *again only leads to a trivial coincidence.*

Computing the torsion sequence closure of $4 \cdot b_4$ *yields the elements* $4 \cdot b_6$ *and* $4 \cdot b_4 + 4 \cdot b_1$. *Insertion of the latter element into the torsion sequence leads to* $4 \cdot b_4 + 4 \cdot b_1 \xrightarrow{4 \cdot b_4} 4 \cdot b_1$ *and we obtain* $L = \{4 \cdot b_6, 4 \cdot b_4, 4 \cdot b_1\}$.

At the point of termination, the MGE-computation has produced a module Υ *with generating set* G :

- $b_1.x_1 - b_1, b_1.x_2 - b_4, b_4.x_1 - b_4, b_4.x_2 - b_6, b_6.x_1 - b_6, b_6.x_2 - b_4 - b_1,$
- $b_2 - 2 \cdot b_1, b_3 - b_1, b_5 - b_4, b_7 - b_4 - b_1, b_8 - b_1, b_9 - 2 \cdot b_1,\ b_{10} - 2 \cdot b_4, b_{11} - b_4, b_{12} - b_4, b_{13} - b_6, b_{14} - b_6,$
- $4 \cdot b_6, 4 \cdot b_4, 4 \cdot b_1.$

We will insert the generators $g_j \in G$ which correspond to table entries, namely where $g_j = b_i.x_k - prod(b_i, x_k)$, into the multiplication table at their respective places:

	$b.x_1$	$b.x_2$	$\gamma^{-1}(\pi(b))$
b_1	$b_1 + g_1$	$b_4 + g_2$	y_1
b_4	$b_4 + g_3$	$b_6 + g_4$	$y_1.x_1x_2$
b_6	$b_6 + g_5$	$b_4 + b_1 + g_6$	$y_1.x_2^2$

Moreover, $L = [g_7 := 4 \cdot b_6, g_8 := 4 \cdot b_4, g_9 := 4 \cdot b_1]$ and $g_{10} := b_2 - 2 \cdot b_1$. We obtain the set E consisting of $\{e_1, \ldots, e_{10}\}$ such that:

- $\alpha(e_1) \equiv y_1.x_1 - y_1;$
- $\alpha(e_2) \equiv y_1.x_2 - y_1.x_1x_2;$
- $\alpha(e_3) \equiv y_1.x_1x_2x_1 - y_1.x_1x_2;$
- $\alpha(e_4) \equiv y_1.x_1x_2^2 - y_1.x_2^2;$
- $\alpha(e_5) \equiv y_1.x_2^2x_1 - y_1.x_2^2;$
- $\alpha(e_6) \equiv y_1.x_2^3 - y_1.x_1x_2 - y;$
- $\alpha(e_7) \equiv 4 \cdot y_1.x_2^2;$
- $\alpha(e_8) \equiv 4 \cdot y_1.x_1x_2;$
- $\alpha(e_9) \equiv 4 \cdot y_1;$
- $\alpha(e_{10}) \equiv y_2 - 2 \cdot y_1;$

Every element of $\widehat{\mathcal{N}}$ is contained in the image of the A-linear span of the set E under the homomorphism β; in order to construct an A-module presentation of $\widehat{\mathcal{N}}$ in terms of the generating set E we however need to introduce relations on the elements of $\mathcal{K}$. The image of the homomorphism β induces a congruence relation on the elements of $\mathcal{K}$. Let $k_1, k_2 \in \mathcal{K}$, if (and only if) $\beta(k_1) = \beta(k_2)$ then we will denote this by

$$k_1 \approx k_2.$$

Moreover we will from now onwards denote by "$\equiv$" the congruence relation on the elements of $\mathcal{F}$ which is generated by the image under $\phi : \mathcal{F} \longrightarrow\!\!\!\!\!\rightarrow \mathcal{D}$ in $\widehat{\mathcal{N}}$; therefore if $\phi(f_1) = \phi(f_2)$ for $f_1, f_2 \in \mathcal{F}$ we will denote this by

$$f_1 \equiv f_2.$$

Since the homomorphism $\beta : \mathcal{K} \longrightarrow \widehat{\mathcal{N}}$ is surjective there must exist $k \in \mathcal{K}$ such that $\beta(k) = \phi(f_v.a) - \phi(f_{\overline{v}})$ for $v.a \sim_\Upsilon \overline{v}$, so in particular there exists an A-linear combination of $e_j \in E$ with $\beta(\sum_{j=1}^{m} e_j.a_j) = \phi(f_v.a) - \phi(f_{\overline{v}})$. In order to specify the notation we set $\Omega(v,a) \in \mathcal{K}$ to be an element that depends on the representative $f_v \in \mathcal{F}$ corresponding to $v \in \Sigma$, and $a \in A$, such that

$$\alpha\big(\Omega(v,a)\big) \equiv f_v.a - f_{\overline{v}}$$

and accordingly $\Omega(v,a) \approx \sum_{j=1}^{m} e_j.a_j$. It follows from the definition of $\Omega(v,a)$ that the choice of an element $\Omega(v,a)$ is not necessarily unique. In a similar way to $\Omega(v,a)$ we define elements $\Omega(y_i)$ for the A-module generators $y_i \in Y$ of $\mathcal{M}$ such that $\alpha\big(\Omega(y_i)\big) \equiv y_i - f_{b_i}$, where initially in the MGE-procedure the assignment $b_i = \gamma(y_i)$ had been made.

Example 6.1.5 *In the case of the Example 6.1.4 we obtain elements Ω induced by the generating set E as follows. The generators $e_1, \ldots e_6$ are all of the form $\Omega(b_i, x_j)$ as $\alpha\big(\Omega(b_i,x_j)\big) \equiv f_{b_i}.x_j - f_{b_i.x_j}$. The generators e_7, e_8 and e_9 are of the form $\Omega(b_i,\lambda)$ since $\alpha(e_k) = \alpha\big(\Omega(b_i,\lambda)\big) \equiv \lambda \cdot f_{b_i}$, the generator e_{10} is of the form $\Omega(y_i)$.*

In Chapter 1.2 we have described elements similar to the elements $\Omega(v,a)$ introduced here. Those elements of Chapter 1.2 were considered as elements of $\mathcal{N}$ and they were used to construct a finite generating set for the A-module $\mathcal{N} \subset \mathcal{F}$. Here the $\Omega(v,a)$ are elements of $\mathcal{K}$. We will now develop a constructive way to express elements $\Omega(v,a)$, modulo the congruence relation " $\approx$ ", as an A-linear combination of elements $\Omega(b,x)$ together with elements $\Omega(b,\lambda)$, for $b \in B^u, x \in X$ and where $\lambda \in S$ is contained in the finite set of the exponents of the torsion-generators of Θ.

Similar to the process of prefix-reducing an element $v \in \Sigma$ modulo generators of Υ we can describe the process of expressing $\Omega(v,a)$ in terms of $\Omega(b,x)$ and $\Omega(b,\lambda)$. As we are given a closed multiplication table after the termination of the MGE-procedure there exists $\overline{v} \in \langle B^u \rangle$ such that $v.a \sim_\Upsilon \overline{v}$ for all pairs $v \in \Sigma$ and $a \in A$ and, as the generating set G of Υ is an MGE-basis, we have that

$$v.a \xrightarrow[p]{G} {}^{*}\, \overline{v}$$

which induces reduction on the respective representatives $f_v \in \mathcal{F}$ by the image-induced ordering. We give an example where we aim to express an element $f \in \mathcal{N}$ as A-linear combination of the images of generators $e \in E$ under α such that $f \equiv \sum_{j=1}^{t} \alpha(e_j).a_j$.

Example 6.1.6 *Suppose we are given the setting of Example 6.1.4 where we are given* $6 \cdot y_1.x_2^3 - y_2.x_1 - 2 \cdot y_1.x_2 \in \mathcal{N}$. *Mapping this to* Σ *by* χ *yields* $6 \cdot \chi(y_1).x_2^3 - \chi(y_2).x_1 - 2 \cdot \chi(y_1).x_2 = 6 \cdot b_1.x_2^3 - b_2.x_1 - 2 \cdot b_1.x_2 \in \Sigma$ *and by prefix-reduction of the respective terms by generators* $g \in G$ *of* Υ *we obtain*

$$6 \cdot b_1.x_2^3 \xrightarrow{g_9.x_2^3} 2 \cdot b_1.x_2^3 \xrightarrow{2 \cdot g_2.x_2^2} 2 \cdot b_4.x_2^2 \xrightarrow{2 \cdot g_4.x_2} 2 \cdot b_6.x_2 \xrightarrow{2 \cdot g_6} 2 \cdot b_4 + 2 \cdot b_1.$$

As moreover $b_2.x_1 \xrightarrow{(b_2 - 2 \cdot b_1).x_1} 2 \cdot b_1.x_1 \xrightarrow{2 \cdot g_1} 2 \cdot b_1$ *and* $2 \cdot b_1.x_2 \xrightarrow{2 \cdot g_2} 2 \cdot b_4$ *we can deduce that*

$$6 \cdot b_1.x_2^3 - b_2.x_1 - 2 \cdot b_1.x_2 = g_9.x_2^3 - g_{10}.x_1 + 2 \cdot \big(g_6 + g_4.x_2 + g_2.(x_2^2 - 1) - g_1\big).$$

Translating this term-wise into the setting of the representatives $f_v \in \mathcal{N}$, *where we use that* $f_{b_2} = f_{2 \cdot b_1} = 2 \cdot f_{b_1}$ *and where, for example,*

- $6 \cdot f_{b_1}.x_2^3 \equiv 2 \cdot f_{b_1}.x_2^3 + \alpha\big(\Omega(b_1, 4)\big).x_2^3 = 2 \cdot f_{b_1}.x_2^3 + \alpha(e_9).x_2^3$;
- $2 \cdot f_{b_1}.x_2^3 \equiv 2 \cdot \big(f_{b_4} + \alpha\big(\Omega(b_1, x_2)\big)\big).x_2^2 = 2 \cdot f_{b_4}.x_2^2 + 2 \cdot \alpha(e_2).x_2^2$;

we obtain $6 \cdot f_{b_1}.x_2^3 - f_{b_2}.x_1 - 2 \cdot f_{b_1}.x_2 \equiv$

$$\alpha(e_9).x_2^3 - \alpha(e_{10}).x_1 + 2 \cdot \big(\alpha(e_6) + \alpha(e_4).x_2 + \alpha(e_2).(x_2^2 - 1) - \alpha(e_1)\big)$$

and accordingly we have that $6 \cdot y_1.x_2^3 - y_2.x_1 - 2 \cdot y_1.x_2 \equiv$

$$\alpha(e_9).x_2^3 - \alpha(e_{10}).x_1 + 2 \cdot \big(\alpha(e_6) + \alpha(e_4).x_2 + \alpha(e_2).(x_2^2 - 1) - \alpha(e_1)\big).$$

If we obtain the generating set B^u of Θ from the computation of an MGE-procedure it is possible that the set of generators of Θ is not clearly divided into a set of generators of the torsion-free submodule and the torsion-submodule. Instead we are given the free S-module $\langle B^u \rangle_S$ of which Θ is a quotient by the S-module Λ, generated by the elements contained in the torsion sequence L. The output of the torsion sequence of an MGE-computation

possibly contains elements $l \in L$ such that $l = \sum_{i=1}^{m} \lambda_i \cdot b_i \in \langle B^u \rangle$ instead of a torsion element of the form $\lambda \cdot b$ for a single generator $b \in B^u$. A Smith Normal Form computation could be used in order to avoid this situation and obtain Θ as the direct sum of a torsion-free and a torsion-submodule. In that case however we will lose the generating set B^u obtained from the MGE-computation. We will show that we can express an elements $\alpha(\Omega(l,1)$, which corresponds to an element $l \in L$, as the sum of $\alpha(\Omega(b_i, \lambda_i))$ for the summands $\lambda_i \cdot b_i$ of l. First we note the following:

Lemma 6.1.7 *Let $v \in \Sigma$ such that $v \sim_\Upsilon \overline{v}$ where $\overline{v} = \sum_{i=1}^{m} \lambda_i \cdot b_i$ and $b_j \neq b_k$ for all $j \neq k$. Then the choice of a canonical representative $f_{\overline{v}} = f_v \sim_{\mathcal{N}} \gamma^{-1}(\pi(v))$ is additive in the sense that $f_{\sum_{i=1}^{m} \lambda_i \cdot b_i} = \sum_{i=1}^{m} f_{\lambda_i \cdot b_i}$.*

Proof. The element f_v is chosen as $\gamma^{-1}(\pi(\overline{v}))$ where $\overline{v}$ is minimal with respect to elements of an MGE-basis G of Υ, then if $\overline{v}$ is minimal then certainly each of its summands must be minimal also. On the other hand suppose that an element $\overline{v}$ is not minimal but each of its summands $\lambda_i \cdot b_i$ is. Then $f_{\overline{v}} \neq \sum_{i=1}^{m} f_{\lambda_i \cdot b_i}$, by assumption we have that $b_j \neq b_k$ whenever $j \neq k$, thence there cannot be any summands which add up to a (multiple of a) torsion element. This however implies that at least one of the $\lambda_i \cdot b_i$ must be head term of an element of G which is a contradiction to the assumption that each of the summands $\lambda_i \cdot b_i$ of $\overline{v}$ is minimal with respect to G. □

In order to provide the setting for showing that an element $\Omega(v, a)$ with $\alpha\big(\Omega(v,a)\big) \equiv f_v.a - f_{v.a}$ is contained in the A-linear span of the subset of the Schreier-generators consisting of elements of the form $\Omega(b, x)$ and $\Omega(b, \lambda)$, we will first prove a set of lemmata.

Lemma 6.1.8 *Let $b \in B^u$, then $\Omega(\kappa \cdot b, \lambda) \approx \Omega(b, \kappa \cdot \lambda) - \lambda \cdot \Omega(b, \kappa)$ for $\kappa, \lambda \in S$.*

Proof. The element $\Omega(\kappa \cdot b, \lambda)$ is defined such that $\alpha\big(\Omega(\kappa \cdot b, \lambda)\big) \equiv \lambda \cdot f_{\kappa \cdot b} - f_{\lambda \cdot \kappa \cdot b}$; for abbreviation we set $\mu := \lambda \cdot \kappa$. Then $\lambda \cdot f_{\kappa \cdot b} - f_{\mu \cdot b} = \mu \cdot f_b - \mu \cdot f_b + \lambda \cdot f_{\kappa \cdot b} - f_{\mu \cdot b} \equiv \mu \cdot f_b - \lambda \cdot \alpha\big(\Omega(b, \kappa)\big) - f_{\mu \cdot b} \equiv \alpha\big(\Omega(b, \mu)\big) - \lambda \cdot \alpha\big(\Omega(b, \kappa)\big)$

from which it follows that

$$\Omega(\kappa \cdot b, \lambda) \approx \Omega(b, \mu) - \lambda \cdot \Omega(b, \kappa).$$

□

Lemma 6.1.9 *Let $v \in \Sigma$ such that $v \sim_\Upsilon \overline{v} = \sum_{i=1}^{m} \lambda_i \cdot b_i \in \langle B^u \rangle$ and let $\kappa \in S$, then $\Omega(v, \kappa) \approx \sum_{i=1}^{m} \Omega(b_i, \kappa \cdot \lambda_i) - \kappa \cdot \Omega(b_i, \lambda_i)$.*

Proof. The element $\Omega(v, \kappa)$ is defined such that $\alpha\big(\Omega(v, \kappa)\big) \equiv \kappa \cdot f_v - f_{\kappa \cdot v} = \kappa \cdot f_{\overline{v}} - f_{\kappa \cdot \overline{v}}$; we will again abbreviate $\mu_i := \kappa \cdot \lambda_i$. We insert $\overline{v} = \sum_{i=1}^{m} \lambda_i \cdot b_i$ into the equation above. From Lemma 6.1.7, together with the definition of an element Ω, it then follows that

$$\kappa \cdot f_{\sum_{i=1}^{m} \lambda_i \cdot b_i} - f_{\sum_{i=1}^{m} \mu_i \cdot b_i} = \sum_{i=1}^{m} \kappa \cdot f_{\lambda_i \cdot b_i} - \sum_{i=1}^{m} f_{\mu_i \cdot b_i} \equiv \sum_{i=1}^{m} \alpha\big(\Omega(\lambda_i \cdot b_i, \kappa)\big).$$

The Lemma 6.1.8 implies that

$$\alpha\big(\Omega(v, \kappa)\big) \equiv \sum_{i=1}^{m} \alpha\big(\Omega(b_i, \mu_i)\big) - \sum_{i=1}^{m} \kappa \cdot \alpha\big(\Omega(b_i, \lambda_i)\big)$$

and therefore

$$\Omega(v, \kappa) \approx \sum_{i=1}^{m} \Omega(b_i, \mu_i) - \sum_{i=1}^{m} \kappa \cdot \Omega(b_i, \lambda_i).$$

□

The last lemma in particular specifies the handling of torsion elements which are caused by inapplicable coincidence in the MGE-procedure. A torsion-element $l \in L \subset \Upsilon$, where $l = \sum_{i=1}^{m} \lambda_i \cdot b_i$ and $HT(l) = \lambda_m \cdot b_m$ then gives rise to an element $\Omega(l, 1) \in \mathcal{K}$ such that $\alpha\big(\Omega(l, 1)\big) \equiv \big(\sum_{i=1}^{m-1} \lambda_i \cdot f_{b_i}\big) + f_{RED(l)} + HC(l) \cdot f_{HM(l)} - f_{HT(l)}$. Since $HT(l) \sim_\Upsilon RED(l)$ we certainly have that $f_{HT(l)} = f_{RED(l)}$.

Proposition 6.1.10 *For all $v \in \Sigma$ and $a \in A$ an element $\Omega(v, a)$ is equivalent by " $\approx$ " to an element which is contained in the A-linear span of elements of the form $\Omega(b, x)$ and $\Omega(b, \lambda)$.*

Proof. We will show that for every $\Omega(v,a)$ with $v \in \Sigma$ and $a \in A$ we have that $\alpha(\Omega(v,a))$ is equivalent by "$\equiv$" to an element which is contained in the A-linear span of elements $\alpha(\Omega(b,x))$ and $\alpha(\Omega(b,\lambda))$. From this then will follow the assumption for the respective elements of $\mathcal{K}$ and the relation "$\approx$". We will regularly use in the following calculations that for every pair $v \in \Sigma$ and $a \in A$ there exists $\overline{v} \in \langle B^u \rangle_S$ such that $v.a \sim_\Upsilon \overline{v}$ as we are in the situation that a given MGE-procedure has already terminated and produced a closed multiplication table. In order to prove the claim we will first show different cases in the following Lemmata:

Lemma 6.1.11 $\Omega(\lambda \cdot b, x) \approx \lambda \cdot \Omega(b,x) - \Omega(b,\lambda).x + \Omega(\overline{v},\lambda)$ *where* $b.x \sim_\Upsilon \overline{v}$.

Proof. The element $\Omega(\lambda \cdot b, x)$ has been defined such that $\alpha\big(\Omega(\lambda \cdot b, x)\big) \equiv f_{\lambda \cdot b}.x - f_{\lambda \cdot b.x} = f_{\lambda \cdot b}.x - f_{\lambda \cdot \overline{v}}$. Then

$$f_{\lambda \cdot b}.x - f_{\lambda \cdot \overline{v}} = \lambda \cdot f_b.x - \lambda \cdot f_b.x + f_{\lambda \cdot b}.x - \lambda \cdot f_{\overline{v}} + \lambda \cdot f_{\overline{v}} - f_{\lambda \cdot \overline{v}} \equiv$$
$$\lambda \cdot \alpha\big(\Omega(b,x)\big) - \alpha\big(\Omega(b,\lambda)\big) + \alpha\big(\Omega(\overline{v},\lambda)\big)$$

from which the relationship follows. □

Lemma 6.1.12 $\Omega(b, \lambda \cdot x) \approx \lambda \cdot \Omega(b,x) + \Omega(\overline{v},\lambda)$ *where* $\overline{v} \in \langle B^u \rangle$ *such that* $b.x \sim_\Upsilon \overline{v}$.

Proof. By the definition of $\Omega(b, \lambda \cdot x)$ we have that $\alpha\big(\Omega(b, \lambda \cdot x)\big) \equiv \lambda \cdot f_b.x - f_{\lambda \cdot b.x}$; therefore

$$\alpha\big(\Omega(b, \lambda \cdot x)\big) \equiv \lambda \cdot f_b.x - \lambda \cdot f_{\overline{v}} + \lambda \cdot f_{\overline{v}} - f_{\lambda \cdot \overline{v}} \equiv \lambda \cdot \alpha\big(\Omega(b,x)\big) + \alpha\big(\Omega(\overline{v},\lambda)\big)$$

and again the relationship follows immediately. □

Lemma 6.1.13 *An element* $\Omega(b,w)$, *where* $w \in X^* \backslash \{\varepsilon\}$, *is equivalent by* " $\approx$ " *to an element which is contained in the* A*-linear span of elements* $\Omega(v,x)$ *of elements* $v \in \langle B^u \rangle_S$ *and* $x \in X$.

Proof. The element $\Omega(b,w)$ is defined such that $\alpha\big(\Omega(b,w)\big) \equiv f_b.w - f_{b.w}$ for $w = x_1 \dots x_m \in X^*$. We will use the abbreviations $w^{(i)} = x_i \dots x_m$ and $v_{(i)}$ for an element $v_{(i)} \in \langle B^u \rangle$ such that $v_{(i)} \sim_\Upsilon b.x_1 \dots x_i$ for $1 \leq i \leq m$, furthermore we set $v_{(0)} := b$ and $w^{(m+1)} = \varepsilon$.

Then $f_b.w - f_{v_{(m)}} = f_b.x_1w^{(2)} - f_{v_{(m)}} \equiv \big(f_{v_{(1)}} + \alpha(\Omega(b,x_1))\big).w^{(2)} - f_{v_{(m)}}$ which again is equivalent to $\big(f_{v_{(2)}} + \alpha(\Omega(v_{(1)},x_2))\big).w^{(3)} + \alpha(\Omega(b,x_1)).w^{(2)} - f_{v_{(m)}}$. Pursuing this in an inductive way we eventually obtain that

$$f_b.w - f_{v_{(m)}} \equiv f_{v_{(m)}} + \sum_{i=1}^{m} \alpha\big(\Omega(v_{(i-1)},x_i)\big).w^{(i+1)} - f_{v_{(m)}}$$

and it therefore follows that

$$\alpha\big(\Omega(b,w)\big) \equiv \sum_{i=1}^{m} \alpha\big(\Omega(v_{(i-1)},x_i)\big).w^{(i+1)}.$$

Thus for the respective elements of $\mathcal{K}$ we can conclude that $\Omega(b,w) \approx \sum_{i=1}^{m} \Omega(v_{(i-1)},x_i).w^{(i+1)}$. □

Lemma 6.1.14 *Let $b \in B^u$ and $\sum_{j=1}^{t} x_j$. Then*

$$\Omega(b, \sum_{j=1}^{t} x_j) - \sum_{j=1}^{t} \Omega(b,x_j)$$

is equivalent by "$\approx$" to an element which is contained in the S-module generated by the finite number of elements of the form $\Omega(b,\kappa)$ for $b \in B^u$ and $\kappa \in S$.

Proof. The element $\Omega(b, \sum_{j=1}^{t} x_j)$ is defined such that $\alpha\big(\Omega(b, \sum_{j=1}^{t} x_j)\big) \equiv \sum_{j=1}^{t} f_b.x_j - f_{b.\sum_{j=1}^{t} x_j}$. For every pair $b \in B^u$ and $x_j \in X$ we know that $b.x_j \sim_\Upsilon \sum_{i=1}^{m} \kappa_{i,j} \cdot b_i$ where $B^u = \{b_1, \dots, b_m\}$ and possibly $\kappa_{i,j} = 0$. Therefore $\sum_{j=1}^{t} b.x_j \sim_\Upsilon \sum_{j=1}^{t} \sum_{i=1}^{m} \kappa_{i,j} \cdot b_i$, and we set $\widetilde{\lambda}_i$ such that $\widetilde{\lambda}_i \cdot b_i \sim_\Upsilon \big(\sum_{j=1}^{t} \kappa_{i,j}\big) \cdot b_i$. Thus

$$\sum_{j=1}^{t} b.x_j \sim_\Upsilon \sum_{i=1}^{m} \widetilde{\lambda}_i \cdot b_i.$$

Using this we obtain that

$$\alpha(\Omega(b,\sum_{j=1}^{t}x_j)) \equiv \sum_{j=1}^{t} f_b.x_j - f_{b.\sum_{j=1}^{t}x_j} \equiv \sum_{j=1}^{t} f_b.x_j - f_{\sum_{i=1}^{m}\widetilde{\lambda}_i\cdot b_i} \equiv$$
$$\sum_{j=1}^{t} f_b.x_j - \sum_{i=1}^{m} f_{\widetilde{\lambda}_i\cdot b_i} \equiv \sum_{j=1}^{t} f_b.x_j + \sum_{i=1}^{m}\alpha(\Omega(b_i,\widetilde{\lambda}_i)) - \sum_{i=1}^{m}\widetilde{\lambda}_i\cdot f_{b_i}.$$

Since $f_{\sum_{j=1}^{t}\kappa_{i,j}\cdot b_i} = f_{\widetilde{\lambda}_i\cdot b_i}$ we have that $\sum_{i=1}^{m}\alpha(\Omega(b_i,\widetilde{\lambda}_i)) - \sum_{i=1}^{m}\widetilde{\lambda}_i\cdot f_{b_i} = \sum_{i=1}^{m}\alpha(\Omega(b_i,\sum_{j=1}^{t}\kappa_{i,j})) - \sum_{i=1}^{m}\sum_{j=1}^{t}\kappa_{i,j}\cdot f_{b_i}$. Moreover,

$$\sum_{j=1}^{t}\alpha(\Omega(b,x_j)) \equiv \sum_{j=1}^{t}\left(f_b.x_j - f_{b.x_j}\right) = \sum_{j=1}^{t} f_b.x_j - \sum_{j=1}^{t} f_{\sum_{i=1}^{m}\kappa_{i,j}\cdot b_i} \equiv$$
$$\sum_{j=1}^{t} f_b.x_j - \sum_{j=1}^{t}\sum_{i=1}^{m} f_{\kappa_{i,j}\cdot b_i} \equiv \sum_{j=1}^{t} f_b.x_j - \sum_{j=1}^{t}\sum_{i=1}^{m}\left(\kappa_{i,j}\cdot f_{b_i} - \alpha(\Omega(b_i,\kappa_{i,j}))\right) =$$
$$\sum_{j=1}^{t} f_b.x_j - \sum_{i=1}^{m}\sum_{j=1}^{t}\kappa_{i,j}\cdot f_{b_i} + \sum_{i=1}^{m}\sum_{j=1}^{t}\alpha(\Omega(b_i,\kappa_{i,j})).$$

Therefore it follows that

$$\alpha(\Omega(b,\sum_{j=1}^{t}x_j)) \equiv \sum_{j=1}^{t}\alpha(\Omega(b,x_j)) + \sum_{i=1}^{m}\left(\alpha(\Omega(b_i,\sum_{j=1}^{t}\kappa_{i,j})) - \sum_{j=1}^{t}\alpha(\Omega(b_i,\kappa_{i,j}))\right)$$
$$\equiv \sum_{j=1}^{t}\alpha(\Omega(b,x_j)) - \sum_{i=1}^{m}\left(f_{\widetilde{\lambda}_i\cdot b_i} - \sum_{j=1}^{t} f_{\kappa_{i,j}\cdot b_i}\right).$$

□

We proceed with the proof of Proposition 6.1.10. First we consider the case of $\Omega(b,a)$ where $b \in B^u$ and $a \in A$. By the definition of $\Omega(b,a)$ we have that $\alpha\big(\Omega(b,a)\big) \equiv f_b.a - f_{b.a}$ where $a = \sum_{w\in X^*}\lambda_w\cdot w$. Since only finitely many λ_w are unequal to 0, the element a can be written as $a = \sum_{j=1}^{t}\lambda_j\cdot w_j$.

Therefore

$$f_b.a - f_{b.a} = \sum_{j=1}^{t} \lambda_j \cdot f_b.w_j - f_{\sum_{j=1}^{t} \lambda_j \cdot b.w_j} =$$

$$\sum_{j=1}^{t} \lambda_j \cdot f_b.w_j - \sum_{j=1}^{t} \lambda_j \cdot f_{b.w_j} + \sum_{j=1}^{t} \lambda_j \cdot f_{b.w_j} - f_{\sum_{j=1}^{t} \lambda_j \cdot b.w_j} \equiv$$

$$\sum_{j=1}^{t} \lambda_j \cdot \alpha(\Omega(b, w_j)) + \sum_{j=1}^{t} \alpha(\Omega(v_j, \lambda_j)) + \sum_{j=1}^{t} f_{\lambda_j \cdot b.w_j} - f_{\sum_{j=1}^{t} \lambda_j \cdot b.w_j},$$

where we set $v_j \in \langle B^u \rangle$ such that $b.w_j \sim_\Upsilon v_j$. We also set $\widetilde{v}_j = \sum_{i=1}^{m} \kappa_{i,j} \cdot b_i$ such that $\widetilde{v}_j \sim_\Upsilon \lambda_j \cdot b.w_j$ and moreover $\widetilde{v} = \sum_{i=1}^{m} \widetilde{\lambda}_i \cdot b_i$ such that $\widetilde{v} \sim_\Upsilon \sum_{j=1}^{t} \sum_{i=1}^{m} \kappa_{i,j} \cdot b_i$. Thus again $\widetilde{\lambda}_i \cdot b_i \sim_\Upsilon \sum_{j=1}^{t} \kappa_{i,j} \cdot b_i$. It follows that

$$\sum_{j=1}^{t} \lambda_j \cdot \alpha(\Omega(b, w_j)) + \sum_{j=1}^{t} \alpha(\Omega(v_j, \lambda_j)) + \sum_{j=1}^{t} f_{\lambda_j \cdot b.w_j} - f_{\sum_{j=1}^{t} \lambda_j \cdot b.w_j} =$$

$$\sum_{j=1}^{t} \lambda_j \cdot \alpha(\Omega(b, w_j)) + \sum_{j=1}^{t} \alpha(\Omega(v_j, \lambda_j)) + \sum_{j=1}^{t} \sum_{i=1}^{m} f_{\kappa_{i,j} \cdot b_i} - \sum_{i=1}^{m} f_{\sum_{j=1}^{t} \kappa_{i,j} \cdot b_i} \equiv$$

$$\sum_{j=1}^{t} \big(\lambda_j \cdot \alpha(\Omega(b, w_j)) +$$

$$\alpha(\Omega(v_j, \lambda_j))\big) + \sum_{i=1}^{m} \Big(\alpha\big(\Omega(b_i, \sum_{j=1}^{t} \kappa_{i,j})\big) - \sum_{j=1}^{t} \alpha\big(\Omega(b_i, \kappa_{i,j})\big)\Big)$$

and the assumption for $\Omega(b, a)$ follows.

We suppose we are given $v \in \Sigma$ and $a \in A$. Then we have that $\alpha\big(\Omega(v, a)\big) \equiv f_v.a - f_{v.a}$. As before we know that there exists $\overline{v} = \sum_{i=1}^{m} \lambda_i \cdot b_i \in \langle B^u \rangle$ such that $v \sim_\Upsilon \overline{v}$. Therefore

$$f_v.a - f_{v.a} = f_{\sum_{i=1}^{m} \lambda_i \cdot b_i}.a - f_{\sum_{i=1}^{m} \lambda_i \cdot b_i.a} = \sum_{i=1}^{m} f_{\lambda_i \cdot b_i}.a - f_{\sum_{i=1}^{m} \lambda_i \cdot b_i.a} \equiv$$

$$\sum_{i=1}^{m} \lambda_i \cdot f_{b_i.a} - f_{\sum_{i=1}^{m} \lambda_i \cdot b_i.a} + \sum_{i=1}^{m} \lambda_i \cdot \alpha\big(\Omega(b_i, a)\big) - \sum_{i=1}^{m} \alpha\big(\Omega(b_i, \lambda_i)\big).a.$$

We denote by v_i the element of $\langle B^u \rangle$ such that $v_i \sim_\Upsilon b_i.a$. Then $v_i = \sum_{j=1}^{m} \kappa_{j_i} \cdot b_j$, so

$$\sum_{i=1}^{m} \lambda_i \cdot f_{b_i.a} - f_{\sum_{i=1}^{m} \lambda_i \cdot b_i.a} =$$

$$\sum_{i=1}^{m} \lambda_i \cdot f_{\sum_{j=1}^{m} \kappa_{j_i} \cdot b_j} - f_{\sum_{i=1}^{m} \lambda_i \cdot (\sum_{j=1}^{m} \kappa_{j_i} \cdot b_j)}.$$

We set $\tau_j \in S$ such that $\tau_j := \sum_{i=1}^{m} \lambda_i \cdot \kappa_{j_i}$. This gives

$$\sum_{i=1}^{m} \lambda_i \cdot f_{\sum_{j=1}^{m} \kappa_{j_i} \cdot b_j} - f_{\sum_{j=1}^{m} \tau_j \cdot b_j} = \sum_{i=1}^{m} \lambda_i \cdot \Big(\sum_{j=1}^{m} f_{\kappa_{j_i} \cdot b_j}\Big) - \sum_{j=1}^{m} f_{\tau_j \cdot b_j} =$$

$$\sum_{j=1}^{m} \big(\tau \cdot f_{b_j} - f_{\tau_j \cdot b_j}\big) - \sum_{i=1}^{m} \lambda_i \cdot \Big(\sum_{j=1}^{m} \kappa_{j_i} f_{b_j} + \sum_{j=1}^{m} f_{\kappa_{j_i} \cdot b_j}\Big) \equiv$$

$$\sum_{j=1}^{m} \alpha\big(\Omega(b_j, \tau_j)\big) - \sum_{i=1}^{m} \lambda_i \cdot \sum_{j=1}^{m} \alpha\big(\Omega(b_j, \kappa_{j_i})\big)$$

and it follows that

$$\Omega(v, a) \approx \sum_{i=1}^{m} \lambda_i \cdot \Omega(b_i, a) - \sum_{i=1}^{m} \Omega(b_i, \lambda_i).a +$$

$$\sum_{j=1}^{m} \big(\Omega(b_j, \tau_j) - \sum_{i=1}^{m} \lambda_i \cdot \Omega(b_j, \kappa_{i,j})\big)$$

which confirms the assumption. □

Corollary 6.1.15 *Let $a_1, a_2 \in A$ and $v \in \Sigma$. Then*

$$\Omega(v, a_1.a_2) \approx \Omega(v, a_1).a_2 + \Omega(v.a_1, a_2).$$

Proof. By the definition of $\Omega(v, a_1 a_2)$ we have that $\alpha(\Omega(v, a_1 a_2)) \equiv f_v.a_1 a_2 - f_{v.a_1 a_2}$, and then $f_v.a_1 a_2 - f_{v.a_1 a_2} = f_v.a_1 a_2 - f_{v.a_1}.a_2 + f_{v.a_1}.a_2 - f_{v.a_1 a_2} \equiv \alpha\big(\Omega(v, a_1)\big).a_2 + \alpha\big(\Omega(v.a_1, a_2)\big)$. Therefore it follows that

$$\Omega(v, a_1 a_2) \approx \Omega(v, a_1).a_2 + \Omega(v.a_1, a_2).$$

□

6.2 Relations on the Generators of the Submodule

In the previous section we described the generators of $\mathcal{K}$ and how the elements $\beta(\Omega(v,a))$ are contained in the A-linear span of elements $\Omega(b,x)$ and $\Omega(b,\lambda)$. We will now explain the relations on the elements of $\mathcal{K}$ which are needed in order to obtain a module with generating set E which is isomorphic to $\widehat{\mathcal{N}}_{\mathcal{A}}$.

The first set of relations on the elements of $\mathcal{K}$ is induced by the set of algebra relations of the quotient-algebra P. As before we denote by R the set of elements of the free algebra A which give the algebra-relations of P. Since $\widehat{\mathcal{N}}$ is a P-module as well, the algebra-relations R must certainly hold for all elements of a module which is isomorphic to $\widehat{\mathcal{N}}$.

Let $b \in B^u$ and suppose we are given $a_1, a_2 \in A$ and $r \in R$ such that $a_2 = a_1 + r$. By the definition of the elements Ω we have that $\alpha(\Omega(b,a_1)) \equiv f_b.a_1 - f_{b.a_1}$ and $\alpha(\Omega(b,a_2)) \equiv f_b.a_2 - f_{b.a_2}$ respectively, and furthermore $f_b.a_2 - f_{b.a_2} = f_b.a_1 + f_b.r - f_{b.(a_1+r)}$. Since $r \in R$ we must have that $\phi(f_b.r) = 0$ for the respective image under ϕ in $\mathcal{D}$ and also that $f_{b.a_1} = f_{b.(a_1+r)}$ as certainly $b.a_1 \sim_\Upsilon b.(a_1 + r)$. It follows that

$$\alpha(\Omega(b,a_2)) \equiv f_b.a_2 - f_{b.a_2} \equiv f_b.a_1 - f_{b.a_1} \equiv \alpha(\Omega(b,a_1))$$

and therefore $\Omega(b,a_2) \approx \Omega(b,a_1)$. We will define a set of relations Z_1 on the elements of $\mathcal{K}$ such that

$$Z_1 = \{\Omega(b,a_1) - \Omega(b,a_2) \mid b \in B^u, a_2 = a_1 + r \text{ for } r \in R\}$$

Example 6.2.1 *We will compute the relations of type Z_1 for the module stated in Example 6.1.4. At the point of termination of the MGE-procedure we are given the multiplication table*

	$b.x_1$	$b.x_2$	$\gamma^{-1}(\pi(b))$
b_1	$b_1 + g_1$	$b_4 + g_2$	y_1
b_4	$b_4 + g_3$	$b_6 + g_4$	$y_1.x_1x_2$
b_6	$b_6 + g_5$	$b_4 + b_1 + g_6$	$y_1.x_2^2$

and $L = [4 \cdot b_6, 4 \cdot b_4, 4 \cdot b_1]$ where $g_7 = 4 \cdot b_6, g_8 = 4 \cdot b_4$ and $g_9 = 4 \cdot b_1$ and moreover $g_{10} = b_2 - 2 \cdot b_1$. We are given the representatives $f_{b_1} = y_1, f_{b_4} = y_1.x_1x_2$ and $f_{b_6} = y_1.x_2^2$ for which we will construct the relations of type Z_1.

In this example we have the two algebra-relations $x_2x_1 - x_1x_2$ *and* $x_2 - x_1x_2$. *These then give rise to the following six relations on the elements of* $\mathcal{K}$:

1. $\Omega(b_1, x_2x_1 - x_1x_2) \sim_{Z_1} \Omega(b_1, 0) = 0$: *we have that* $\alpha\big(\Omega(b_1, x_2x_1 - x_1x_2)\big) \equiv f_{b_1}.(x_2x_1 - x_1x_2) \equiv (f_{b_4} + \alpha(e_2)).x_1 - (f_{b_1} + \alpha(e_1)).x_2 \equiv f_{b_4} + \alpha(e_3) + \alpha(e_2).x_1 - f_{b_4} - \alpha(e_2) - \alpha(e_1).x_2$, *and it follows that*

$$e_3 + e_2.(x_1 - 1) - e_1.x_2 \sim_{Z_1} 0;$$

2. $\Omega(b_4, x_2x_1 - x_1x_2) \sim_{Z_1} 0$, *since* $\alpha\big(\Omega(b_4, x_2x_1 - x_1x_2)\big) \equiv f_{b_4}.(x_2x_1 - x_1x_2) \equiv (f_{b_6} + \alpha(e_4)).x_1 - (f_{b_4} + \alpha(e_3)).x_2 \equiv f_{b_6} + \alpha(e_5) + \alpha(e_4).x_1 - f_{b_5} - \alpha(e_4) - \alpha(e_3).x_2$ *it follows that*

$$e_5 + e_4.(x_1 - 1) - e_3.x_2 \sim_{Z_1} 0;$$

3. $\Omega(b_6, x_2x_1 - x_1x_2) \sim_{Z_1} 0 \Longrightarrow e_1 + e_3 + e_6.(x_1 - 1) - e_5.x_2 \sim_{Z_1} 0$;

4. $\Omega(b_1, x_2 - x_1x_2) \sim_{Z_1} 0 \Longrightarrow e_1.x_2 \sim_{Z_1} 0$;

5. $\Omega(b_4, x_2 - x_1x_2) \sim_{Z_1} 0 \Longrightarrow e_3.x_2 \sim_{Z_1} 0$;

6. $\Omega(b_6, x_2 - x_1x_2) \sim_{Z_1} 0 \Longrightarrow e_5.x_2 \sim_{Z_1} 0$.

The next set of relations on the elements of $\mathcal{K}$ is induced from the following. The representative f_v of an element $v \in \Sigma$ is chosen as $f_v := \gamma^{-1}(\pi(\overline{v}))$ where $\overline{v}$ is the element in the congruence class of v which is minimal with respect to the MGE-basis G of Υ. The ordering given on the elements of $\mathcal{F}$ is the image-induced ordering obtained from an MGE-procedure. As has been described in previous chapters, it is actually possible that an element $f_v = y.wx \in \mathcal{F}$ is minimal with respect to the image-induced ordering where at the same time there is a prefix $y.w$ of $y.wx$ and an element $g \in G$ such that $HM(g) = \chi(y.w)$ (where $\chi : \mathcal{F} \longrightarrow \Sigma$). In this case there is a prefix of f_v which itself is not a minimal element.

An example of this is given by a coincidence c which leads to a consequence $\widetilde{c}$ such that $\widetilde{c} \sim_{\Delta} c.x$. If now for summands b of $RED(c)$ we have

that $b.x$ is not congruent modulo $(\Delta)_A$ to any element $v \in \langle B^u \rangle_S$ then this implies that $HM(c).x \not\sim_\Delta HM(\widetilde{c})$.

In such a situation the tracing of a representative $f_v = y.wx$ might lead to linear combinations of generators in E. For $f = \sum_{i=1}^{n} y_i.a_i \in \mathcal{F}$ we define an element $\Omega(f)$ such that $\alpha(\Omega(f)) \equiv \sum_{i=1}^{n} \alpha(\Omega(y_i)).a_i + \sum_{i=1}^{n} \alpha(\Omega(b_i, a_i))$.

Now let $e \in E$, then $\alpha(e) \in \mathcal{N}$, suppose that $\alpha(e) = \sum_{i=1}^{n} y_i.\widetilde{a}_i$. Then

$$\alpha(e) \equiv \sum_{i=1}^{n} \alpha(\Omega(y_i)).\widetilde{a}_i + \sum_{i=1}^{n} f_{b_i}.\widetilde{a}_i.$$

Since $\sum_{i=1}^{n} y_i.\widetilde{a}_i \in \mathcal{N}$ it follows that $f_{\sum_{i=1}^{n} y_i.\widetilde{a}_i} = f_{\sum_{i=1}^{n} b_i.\widetilde{a}_i} = f_0$, which also implies $\sum_{i=1}^{n} f_{b_i.\widetilde{a}_i} = f_0$. Accordingly

$$\alpha(e) = \sum_{i=1}^{n} y_i.\widetilde{a}_i = \sum_{i=1}^{n} y_i.\widetilde{a}_i - \sum_{i=1}^{n} f_{b_i}.\widetilde{a}_i + \sum_{i=1}^{n} f_{b_i}.\widetilde{a}_i - \sum_{i=1}^{n} f_{b_i.\widetilde{a}_i} \equiv$$
$$\sum_{i=1}^{n} \alpha(\Omega(y_i)).\widetilde{a}_i + \sum_{i=1}^{n} \alpha(\Omega(b_i, \widetilde{a}_i)) \equiv \alpha(\Omega(\alpha(e)))$$

and it follows that $e \approx \Omega(\alpha(e))$. We define a set of relations $Z_2 \subset \mathcal{K}$ on the elements of E such that

$$Z_2 = \{e - \Omega(\alpha(e)) \mid e \in E\}.$$

We proceed with an example where we compute the relations of type Z_2 for the setting given in Example 6.1.4.

Example 6.2.2 *We are given the multiplication table*

	$b.x_1$	$b.x_2$	$\gamma^{-1}(\pi(b))$
b_1	$b_1 + g_1$	$b_4 + g_2$	y_1
b_4	$b_4 + g_3$	$b_6 + g_4$	$y_1.x_1x_2$
b_6	$b_6 + g_5$	$b_4 + b_1 + g_6$	$y_1.x_2^2$

and the torsion sequence $L = [g_7 = 4 \cdot b_6, g_8 = 4 \cdot b_4, g_9 = 4 \cdot b_1]$ *and* $g_{10} = b_2 - 2 \cdot b_1$. *Computing relations of type* Z_2 *for generators* $e \in E$ *leads to the following relations:*

1. $\alpha(e_1) \equiv f_{b_1}.x_1 - f_{b_1} = y_1.x_1 - y_1$; *therefore* $\alpha(\Omega(\alpha(e_1))) \equiv f_{b_1} + \alpha(e_1) - f_{b_1}$. *We obtain the trivial relation* $e_1 \sim_{Z_2} e_1$.

2. *Similarly,* $\alpha(e_2) \equiv f_{b_1}.x_2 - f_{b_4}$ *leads to the trivial relation* $e_2 \sim_{Z_2} e_2$.

3. $\alpha(e_3) \equiv f_{b_4}.x_1 - f_{b_4} = y_1.x_1x_2x_1 - y_1.x_1x_2$, *so*

$$y_1.x_1x_2x_1 - y_1.x_1x_2 \equiv \big(f_{b_1} + \alpha(e_1)\big).x_2x_1 - \big(f_{b_1} + \alpha(e_1)\big).x_2 \equiv$$
$$\big(f_{b_4} + \alpha(e_2)\big).x_1 + \alpha(e_1).x_2x_1 - f_{b_4} - \alpha(e_2) - \alpha(e_1).x_2 \equiv$$
$$f_{b_4} + \alpha(e_3) + \alpha(e_2).x_1 + \alpha(e_1).x_2x_1 - f_{b_4} - \alpha(e_2) - \alpha(e_1).x_2 \equiv \alpha(\Omega(\alpha(e_3))).$$

We can conclude that $e_3 \sim_{Z_2} e_3 + e_2.(x_1 - 1) + e_1.(x_2x_1 - x_2)$ *and therefore that* $e_2.(x_1 - 1) + e_1.(x_2x_1 - x_2) \sim_{Z_2} 0$.

4. $\alpha(e_4) \equiv f_{b_4}.x_2 - f_{b_6} = y_1.x_1x_2^2 - y_1.x_2^2$ *and accordingly*

$$\alpha(e_4) \equiv \big(f_{b_1} + \alpha(e_1)\big).x_2^2 - (f_{b_4} + \alpha(e_2)).x_2 \equiv$$
$$\alpha(e_4) + \alpha(e_2).x_2 + \alpha(e_1).x_2^2 - \alpha(e_4) - \alpha(e_2).x_2 \equiv \alpha(\Omega(\alpha(e_4)))$$

from which it follows that $e_4 \sim_{Z_2} e_1.x_2^2$.

5. *From* $\alpha(e_5)$ *we obtain* $e_4.(x_1 - 1) + e_2.(x_2x_1 - x_2) \sim_{Z_2} 0$.

6. *From* $\alpha(e_6)$ *we obtain* $e_4.x_2 + e_2.(x_2^2 - 1) - e_1.x_2 \sim_{Z_2} 0$.

7. *For the first element contained in the torsion sequence we have that* $\alpha(e_7) \equiv 4 \cdot f_{b_6} = 4 \cdot y_1.x_2^2$, *thence*

$$\alpha(e_7) \equiv 4 \cdot (f_{b_4} + \alpha(e_2)).x_2 \equiv 4 \cdot \big(\alpha(e_2).x_2 + f_{b_6} + \alpha(e_4)\big) \equiv \alpha(\Omega(\alpha(e_7)))$$

from which it follows that $e_7 \sim_{Z_2} 4 \cdot e_2.x_2 + 4 \cdot f_{b_6} + 4 \cdot e_4$. *By the definition of* e_7 *we have that* $\alpha(e_7) \equiv 4 \cdot f_{b_6}$ *and we can deduce that* $4 \cdot \big(e_2.x_2 + e_4\big) \sim_{Z_2} 0$.

8. *From* $\alpha(e_8)$ *we obtain that* $4 \cdot (e_2 + e_1.x_2) \sim_{Z_2} 0$.

9. $\alpha(e_9) \equiv 4 \cdot f_{b_1} = 4 \cdot y_1$: *since* y_i *is a module generator it follows that we only obtain a trivial relation* $\alpha(e_9) \equiv y_1 \equiv \alpha(\Omega(\alpha(e_9)))$.

10. $\alpha(e_{10}) \equiv y_2 - 2 \cdot y_1$ *only leads to the trivial equivalence*

$$\alpha(e_{10}) \equiv f_{y_2} - f_{2 \cdot y_1} \equiv \alpha(\Omega(\alpha(e_{10}))).$$

We set $Z := Z_1 \cup Z_2$. We will now show that we obtain an A-module presentation for $\widehat{\mathcal{N}}$ if the relations Z_1 and Z_2 are satisfied for the generators $e \in E$, namely that

$$\widehat{\mathcal{N}} = \langle E \mid Z \rangle_A.$$

By construction of the set Z we know that $z' \approx z''$ for all $z' \sim_Z z''$ where $z' - z'' \in Z$. We need to show the other implication, namely if for given $k_1, k_2 \in \mathcal{K}$ we have that $k_1 \approx k_2$ that it then follows that $k_1 \sim_Z k_2$. We will show that

1. $\Omega(v, a_1) \sim_{Z_1} \Omega(v, a_2)$ holds for all $v \in \Sigma$ if $a_2 = a_1 + q$ where $q \in I$;
2. $\alpha(k) \sim_{Z_2} \alpha(\Omega(\alpha(k)))$ holds for all $k \in \mathcal{K}$.

Lemma 6.2.3 *Let $v \in \Sigma$. Then $\Omega(v, a_1) \sim_{Z_1} \Omega(v, a_2)$ for all $a_2 = a_1 + q \in A$ with $q \in I = \langle ARA \rangle$.*

Proof: If $q \in I$ then $q = \sum_{j=1}^{t} a'_j r_j a''_j$ and accordingly $\alpha(\Omega(v, a_2)) \equiv f_v.a_2 - f_{v.a_2} = f_v.a_1 + f_v.(\sum_{j=1}^{t} a'_j r_j a''_j) = f_v.a_1 + \sum_{j=1}^{t} \big(f_v.a'_j r_j a''_j - f_{v.a'_j}.r_j a''_j + f_{v.a'_j}.r_j a''_j - f_{v.a'_j r_j}.a''_j + f_{v.a'_j r_j}.a''_j - f_{v.a_1}$. Since $\alpha(\Omega(v, a'_j)) \equiv 0$ and also $f_{va'_j r_j} = f_0 = 0$ for all $1 \leq j \leq t$, we have that

$$\alpha\big(\Omega(v, a_2)\big) \equiv \alpha\big(\Omega(v, a_1)\big) + \sum_{j=1}^{t} \alpha\big(\Omega(\widetilde{v}_j, r_j)\big).a''_j$$

where we have set $\widetilde{v}_j = \sum_{i=1}^{m} \lambda_{i_j} \cdot b_i$ such that $v_j.a'_j \sim_\Upsilon \widetilde{v}_j$.

It follows from Proposition 6.1.10 that

$$\alpha(\Omega(\widetilde{v}_j, r_j)) \equiv \sum_{i=1}^{m} \big(\lambda_{i_j} \cdot \alpha(\Omega(b_i, r_j)) - \alpha(\Omega(b_i, \lambda_{i_j}).r_j)\big).$$

We note here that $v.r \sim_\Upsilon 0$ so it follows that the coefficients κ and τ, and also the corresponding terms stated in Proposition 6.1.10, all must be zero.

Again we have that $\alpha(\Omega(b_i, \lambda_{i_j}).r_j) \equiv 0$, so $\alpha\big(\Omega(v, a_2)\big) \equiv \alpha\big(\Omega(v, a_1)\big) + \sum_{j=1}^{t} \sum_{i=1}^{m} \lambda_{i_j} \cdot \Omega(b_i, r_j).a''_j$. The definition of the relation Z_1 implies that $\Omega(b_i, r_j) \sim_{Z_1} 0$ for all $b_i \in B^u$ and $r_j \in R$ and we can conclude that $\Omega(v, a_2) \sim_{Z_1} \Omega(v, a_1)$. □

Lemma 6.2.4 *Let $k \in \mathcal{K}$. Then $k \sim_{Z_2} \Omega(\alpha(k))$.*

Proof. If $k \in \mathcal{K}$ then $k = \sum_{j=1}^{t} e_j.a_j$ with $e_j \in E$. We will show that $\alpha(\Omega(\alpha(k))) \equiv \alpha(k)$ from which then will follow that $k \sim_{Z_2} \Omega(\alpha(k))$.

We have that $\alpha(k) = \alpha(\sum_{j=1}^{t} e_j.a_j)$. We suppose that $\alpha(e_j) = \sum_{i=1}^{n} y_i.\widetilde{a}_{i,j}$, so that $\alpha(k) = \sum_{j=1}^{t} \big(\sum_{i=1}^{n} y_i.\widetilde{a}_{i,j}\big).a_j = \sum_{i=1}^{n} y_i.a'_i$ where we set $a'_i := \sum_{j=1}^{t} \widetilde{a}_{i,j}.a_j$. We have that

$$\alpha(k) = \sum_{j=1}^{t} \alpha(e_j).a_j \equiv \sum_{j=1}^{t} \alpha(\Omega(\alpha(e_j))).a_j \equiv$$

$$\sum_{j=1}^{t} \big(\sum_{i=1}^{n} \alpha(\Omega(y_i)).\widetilde{a}_{i,j} + \sum_{i=1}^{n} \alpha(\Omega(b_i, \widetilde{a}_{i,j}))\big).a_j =$$

$$\sum_{i=1}^{n} \alpha(\Omega(y_i)).\sum_{j=1}^{t} \widetilde{a}_{i,j}a_j + \sum_{i=1}^{n}\sum_{j=1}^{t} \alpha(\Omega(b_i, \widetilde{a}_{i,j})).a_j \equiv$$

$$\sum_{i=1}^{n} \alpha(\Omega(y_i)).a'_i + \sum_{i=1}^{n} \alpha(\Omega(b_i, a'_i)) - \sum_{i=1}^{n}\sum_{j=1}^{t} \alpha(\Omega(b_i.\widetilde{a}_{i,j}, a_j)).$$

Since $\sum_{i=1}^{n}\sum_{j=1}^{t} \alpha(\Omega(b_i.\widetilde{a}_{i,j}, a_j)) \equiv \sum_{j=1}^{t} \alpha(\sum_{i=1}^{n} \Omega(b_i.\widetilde{a}_{i,j}, a_j))$ and $\alpha(e_j) = \sum_{i=1}^{n} y_i.\widetilde{a}_{i,j} \in \mathcal{N}$ it follows for the corresponding elements of Σ that

$$\sum_{i=1}^{n} \chi(y_i).\widetilde{a}_{i,j} = \sum_{i=1}^{n} b_i.\widetilde{a}_{i,j} \in \Upsilon$$

and therefore $f_{\sum_{i=1}^{n} b_i.\widetilde{a}_{i,j}} = f_0$. We can deduce that

$$\alpha(k) \equiv \sum_{i=1}^{n} \alpha(\Omega(y_i)).a'_i + \sum_{i=1}^{n} \alpha(\Omega(b_i, a'_i)) \equiv \alpha(\Omega(\alpha(k)))$$

and therefore in particular

$$k \approx \Omega(\alpha(k)).$$

□

Corollary 6.2.5 *We are given an A-module presentation*

$$\widehat{\mathcal{N}} = \langle E \mid Z \rangle_A.$$

with generating set E and the set of relations Z.

Proof. It has been shown before that E generates $\widehat{\mathcal{N}}$. It follows from Lemma 6.2.3 and Lemma 6.2.4 that for given $k_1, k_2 \in \mathcal{K}$ with $k_1 \approx k_2$ it follows that $k_1 \sim_Z k_2$ which confirms the assumption. □

We will now give an upper bound for the size of the sets E and Z.

Theorem 6.2.6 *Let $\widehat{\mathcal{N}}$ be such that $\mathcal{M}_A = \mathcal{F}/\mathcal{N} \cong \mathcal{D}/\widehat{\mathcal{N}}$. We suppose that $\mathcal{F}$ has a generating set Y of cardinality n and that the set of generators X of the algebra A has k elements. Moreover we assume that there are q elements in the set of algebra-relations R, that the set B^u of S-module generators of $\mathcal{M}$ has cardinality m, that there are t elements contained in the torsion sequence L and that we have obtained $i < n$ relations of the module-generators $\{y_1, dots, y_n\} = Y$. Then $\widehat{\mathcal{N}} = \langle E \mid Z \rangle_A$ where*

- *for the generating set E we have that $|E| \leq m \cdot (k+1) + n - 1$;*
- *for the set of relations Z we have that $|Z| \leq m \cdot (q+k) + t$.*

Proof. If a generator $y_\mu \in Y$ is equal to the head term of a relation of $\mathcal{M}_S$, then y_μ depends linearly on the generators $y_1, \ldots y_j$, where $j < \mu$, or it is in fact trivial all together. In the case that we have obtained $i = n$ relations of this kind we obtain trivial modules $\mathcal{D}$ and $\mathcal{F}$, so we can assume that $i < n$ which leads to $i < n$ generators of the type $\Omega(y)$ for $y \in Y$.

The multiplication table of the MGE-procedure has m rows corresponding to $b \in B^u$. Therefore it must have $m - n + i$ rows such that $b = \gamma(y.w)$ and $w \in X^* \backslash \{\varepsilon\}$. From the multiplication table we obtain generators $\Omega(b, x)$ such that $\alpha(\Omega(b, x)) \equiv f_b.x - f_v$ of which there are $m \cdot k$. If $v = b' \sim_\Delta b.x$ then $f_b.x = f_v$ and $\Omega(b, x) = 0$. In the case that the representative f_b for $b \in B^u$ has been chosen in a minimal way we can therefore conclude that for $m - n + i$ many $b' \in B^u$ we have that $f_b.x = f_{b'}$.

However, since we set $f_v := \gamma^{-1}(\pi(v))$ where v is minimal with respect to the generating set G of Υ and where we use image-induced ordering on the elements of $\mathcal{F}$, we cannot necessarily assume that a representative is minimal (compare for instance Example 6.1.4). Therefore it is possible that

none of the generators $\Omega(b, x)$ is zero, in this case there are at most $m \cdot k$ generators of the form $\Omega(b, x)$.

Together with $t \leq m$ generators $\Omega(b, \lambda)$ induced by L and $i < n$ generators of the form $\Omega(y_i)$ we then obtain that at most $m \cdot k + i + t \leq m \cdot (k+1) + n - 1$ elements are contained in E.

For the set of relations Z_1 we apply each of the q relations contained in R to every representative corresponding to $b \in B^u$, from which we obtain that $|Z_1| = m \cdot q$, but trivial relations might included.

The set Z_2 contains elements of the form $e - \Omega(\alpha(e))$. Since a module generator $y_i \in Y$ does not have any prefixes, and so in particular no prefixes which are non-minimal, it follows that for generators $e = \Omega(y))$ we must always have that $e = \Omega(\alpha(e))$ and in this case the obtained relation is trivial. Depending on the cardinality of the set E we remain with at most $m \cdot k + t \leq m \cdot (k+1)$ relations of type Z_2. □

Example 6.2.7 *The module $\widehat{\mathcal{N}}$ such that $\mathcal{M} = \mathcal{D}/\widehat{\mathcal{N}}$ for $\mathcal{M}$ in Example 6.1.4 has the A-module generating set $E = \{e_1, \ldots e_{10}\}$; the set of relations Z_1 from Example 6.2.1 has size 6 and, as was shown in Example 6.2.2, there are 6 non-trivial relations of type Z_2. Therefore we obtain a presentation*

$$\widehat{\mathcal{N}} = \langle E \mid Z_1 \cup Z_2 \rangle_A$$

where $Z_1 = \{e_3 + e_2.(x_1 - 1) - e_1.x_2, e_5 + e_4.(x_1 - 1) - e_3.x_2, e_1 + e_3 + e_6.(x_1 - 1) - e_5.x_2, e_1.x_2, e_3.x_2, e_5.x_2\}$ *and where* $Z_2 = \{e_2.(x1 - 1) + e_1.(x_2x_1 - x_2), e_4 - e_1.x_2^2, e_4.(x_1 - 1) + e_2.(x_2x_1 - x_2), e_4.x_2 + e_2.(x_2^2 - 1) - e_1.x_2, 4 \cdot (e_2.x_2 + e_4), 4 \cdot (e_2 + e_1.x_2)\}$.

Remark 6.2.8 *Let H be the subgroup of finite index of a finitely presented group G. C. Sims describes in [41], Chapter 6.1 p.275, the size of a presentation of H in terms of Schreier generators of H. If G has a presentation with n generators and r relations and where H is a subgroup of index k in G then H has a presentation with $1 + k \cdot (n-1)$ generators and $k \cdot r$ relations. Note that for the stated upper bound of both the set of generators as of the relations the presumption has been used that the representatives of the cosets*

have been chosen in a minimal and therefore irreducible way. In that case, relations corresponding to relations of type Z_2 for instance can be omitted.

Chapter 7

Implementation and Examples

In this chapter we shall discuss the thoughts which went into the planning and the implementation of the MGE-procedure and we will also present examples of computations with the MGE-procedure as it is installed in GAP.
Section 7.1: We introduce the strategy of the MGE-procedure implemented in GAP. The procedure handles modules over Euclidean domains. Since elements of a Euclidean domain S are not necessary invertible, torsion in a module over S can arise and methods have to be developed in order to handle such torsion elements. Moreover, also in parts caused by the fact that elements are not necessarily units, vectors of great length with only few nonzero entries that can become exceedingly large can occur as part of the computation.
Section 7.2: We present a few examples of the results of MGE-procedure. Moreover from these terminated MGE-procedure we construct submodule presentations with a procedure as described in Chapter 6.
Section 7.3: We complete the chapter with a conclusion.

7.1 Implementation of the MGE-procedure in GAP

In this section we describe the MGE-procedure as it is implemented in GAP. This implementation mainly uses the procedures as they were presented in

Chapter 4; we highlight where it deviates. Moreover we also specify and explain in closer detail certain features of the procedure which were not mentioned in Chapter 4. We shall now describe the strategy of the MGE-procedure in GAP.

7.1.1 Strategy

When we consider $\mathcal{M}$ as a P-module, then by assumption $\mathcal{M}$ and P are finitely presented and therefore $\mathcal{M}$ has a finite set of module-relations which we denote by U, and moreover a finite set of relations R of the algebra P. We assume that $\mathcal{M}$ is isomorphic to a finitely generated S-module. The MGE-procedure works in the following order:

1. A table with rows $b_1, \ldots, b_n$ is initialised. Each row corresponds to a possible S-module generator $b \in B_{(0)}$ and $B_{(0)}$ is a set in bijection to the set of P-module generators Y' of $\mathcal{M}$.

2. An empty coincidence stack Cp is initialised.

3. If not all elements of the ring S are invertible, then an empty torsion sequence L is initialised.

4. By tracing their image in Σ, the coincidences caused by the module-relations $U \subset \mathcal{F}$ of $\mathcal{M}$ will be computed and processed.

5. We now interleave the following two types of steps until "$\perp$" no longer appears as entry of the table.

   (a) Certain coincidences caused by the finite set of algebra-relations R will be traced, computed and processed: we will compute the coincidences obtained from $b.r$ for all $b \in B^u$ and $r \in R$. These correspond to a certain finite subset of the set $Rels$, namely the set of those elements $y.wr$ with $\gamma(y.w) \in B^u$.

   (b) For every $l \in L$ we will compute $l \star x$ for all $x \in X$ and these elements will be added to the coincidence stack.

6. We finally check for closure of the torsion sequence by completing any remaining steps of type 5.(b).

7.1.2 Storing Elements

Storing Elements of $\langle B \rangle_S$

At all times we work with elements of the free module $\mathcal{F}$ in order to obtain S-linear dependencies between these. Whenever an element $f \in \mathcal{F}$ is needed in the course of the procedure, for instance if it is a relation or the prefix of a relation, we aim to express it in terms of the free module $\langle B \rangle_S$. The elements of this are called **vectors**. Whenever necessary, an element $b \in \mathcal{B} \backslash B$ is assigned to a prefix $y.w$ of a summand of f. If the MGE-procedure terminates then a finite number of such assignments have become necessary. This leads to a finitely generated free module $\langle B \rangle$ and every $b_i \in B = \{b_1, \ldots b_n\}$, with $b_i := \gamma(y.w)$, is a vector of length n with $b_i = [0, \ldots, 1, 0 \ldots 0]$ where the entry 1 can be found at the i-th position.

The vector-form is used to store the elements of Cp, L and the entries of the table T. If it is expected that a module $\mathcal{M}$ will lead to phases in the procedure where big generating sets B become necessary and therefore large vectors have to be handled, an option to handle specially vectors that are sparse is available.

Elements of T

Whenever a box $\text{prod}(b, x)$ or r_b of T has been filled it contains a vector $v \in \langle B \rangle$ (not necessarily $\langle B^u \rangle_S$). If a box has not been filled it contains as entry "$\perp$" which is a symbol for empty or unknown. This symbol is represented by the GAP object fail.

Storing elements of $\mathcal{F}$

In the MGE-procedure we consider the P-module $\mathcal{M}$ as a module over the free algebra A where it is a quotient-module of the free module $\mathcal{F}$ with generating set Y. We store preimages of $b \in B^u$ in the multiplication table. Each $b \in B^u$ either corresponds to a module generator $y \in Y$ or has been defined as the image of a prefix $p]r$ under the map ρ. Since every such prefix $p]r$ is of the form $p]r = y.w$ for $y \in Y$ and $w \in X^*$ we can present $\gamma^{-1}(b)$ as

a list

$$[y, [x_1, \ldots, x_t]]$$

stating the module generator y and the word $w = x_1 \ldots x_t$.

7.1.3 Root Procedure

While tracing the image of a relation, the MGE-procedure accesses certain entries of the multiplication table. For reasons of performance those entries, which are vectors $v \in \langle B \rangle$ are not adjusted immediately after a generator $b \in B^u$ has been deleted. Therefore when a prefix $v = \mathrm{prod}(b, x)$ has been found such that $v \neq u(v)$, we have to replace v by its undeleted image. This so-called **Root procedure** is a recursive process as we define the undeleted image as

$$u_{(\iota)}(v) := \sum_{i=1}^{m} \lambda_i \cdot \begin{cases} b_i \text{ if } b_i \in B^u_{(\iota)_j} \\ u_{(\iota)}(r_{b_i}), \text{ otherwise.} \end{cases}$$

Whenever we find in this process $r_{b_i} \neq u(r_{b_i})$, the entry r_{b_i} in the table will be replaced by $u(r_{b_i})$ immediately.

7.1.4 The Handling of Torsion Elements

As has been described before, possibly arising torsion elements lead to inapplicable coincidences. Whenever a coincidence c with $b = HM(c)$ is found, we aim eventually to replace the S-module generator $b \in B^u$ by $HC(c)^{-1} \cdot RED(c)$. This however is only feasible if $HC(c)$ is an invertible element of S. We therefore distinguish between applicable coincidence ($HC(c)$ is invertible) and inapplicable coincidence ($HC(c)$ is not invertible).

When coincidences are first detected they are stored in a stack Cp, irrespective of the fact that they are applicable or inapplicable. Only when the coincidences stored in Cp are inspected, using CLEARING COINCIDENCES, will the handling differ and inapplicable coincidences will be inserted into the torsion sequence L. This sequence is an ordered list and for the handling of the elements of L we need mainly two routines:

1. The inserting of new inapplicable coincidences into L;

2. Ensuring that the A-module closure of an element $l \in L$, with respect to all algebra-generators $x \in X$, has been taken into consideration as a possible further coincidence.

For a detailed description of the procedure of inserting inapplicable coincidences into L compare Section 4.1.2, p. 87.

The ordering on the elements of L is not necessarily compatible with the second routine of A-linear closure of elements of L. As was pointed out by J. Müller in private conversation, if we follow the given ordering by head terms for computing the A-module closure, the closure of the elements at the first position of L will be computed and information which should be obtained from linearly closing inapplicable coincidences with smaller head monomials possibly omitted. Computing the A-module closure of $l \in L$ possibly involves new definition steps, the resulting elements $\widetilde{c}_1, \ldots, \widetilde{c}_m$ will be stored in Cp and be processed. In the case that a $\widetilde{c}_j$ is an inapplicable coincidence, $\widetilde{c}_j$ will again be inserted into L. If $HC(\widetilde{c}_j) > HC(l_i)$ for all $l_i \in L$ then $\widetilde{c}_j$ will be inserted at the first position of L. This might subsequently lead to a loop if the procedure for A-module closure computes with those elements stored at the beginning of the sequence. Instead we will introduce a second ordering on the elements of L. This ordering shall depend on the point of insertion of elements, and the A-module closure of L shall be computed using this ordering.

Since the ordering by head monomials of elements of L plays an important role in the handling of the inapplicable vectors we will ensure that the information of the deleting of an S-module generator will be applied to the elements contained in L immediately, in contrast to the elements of Cp. It is an essential part of the proof of correctness that we are only given elements in L which are contained in $\langle B^u \rangle$. Moreover we must ensure that only coincidences which are inapplicable are contained in L. Therefore, when an applicable coincidence c with $HM(c) = b$ occurs we will then scan the elements of L to see if they contain a summand generated by b. If so the respective element will be replaced by its undeleted image.

To be precise, if we apply an applicable coincidence c we will check the elements of L to see if the vector $b = HM(c)$ generates a non-trivial

summand of an entry $l \in L$. If so, and if this summand is not $HM(l)$ itself we then will replace $l := u_{(\iota)}(l)$. If, however, $HM(c) = HM(l)$, then we will remove l from the list L altogether. We will add l to Cp where it will be processed as a coincidence at a later stage again. Only then will the procedure be able to decide if $u(l)$ is an applicable coincidence or not.

The Euclidean algorithm

An algorithm for computing the extended Euclidean algorithm can be found in GAP. This algorithm is used in the routine HANDLING INAPPLICABLE COINCIDENCES. For an entry $l \in L$ and inapplicable coincidence c with $HM(l) = HM(c)$ it computes the greatest common divisor $\mu := s_1 \cdot HC(l) + s_2 \cdot HC(c)$, the coefficients s_1 and s_2 and moreover coefficients t_1 and t_2 such that $t_1 \cdot HC(l) + t_2 \cdot HC(c) = 0$.

7.1.5 Lookahead

Different strategies have been developed for coset enumeration. The MGE-procedure is based on the HLT-strategy, developed by Haselgrove, Leech and Trotter, see [20, 44, 9]. The HLT-strategy for coset enumeration can be interpreted in the sense that the main objective is to obtain coincidences as quickly as possible, even if it is to the cost of having to make many definitions in order to assign names to new cosets. Other strategies in coset-enumeration try to avoid new definitions when possible and deduce possible coincidences of cosets by using the two-sided search. For instance in the Felsch-strategy [14, 9] every new definition is followed by a scan of the whole multiplication table in order to check if further coincidences can be deduced.

In the case of the MGE-procedure we handle right modules, that is the action of the algebra on the elements of $\mathcal{M}$ is from the right hand side, so the search for coincidences in an MGE-procedure can only be a one-sided approach. Moreover, as the generators $x \in X$ of the algebra P are elements of a monoid X^*, a generator x can only be considered to be invertible when there are elements $r_{i_1} = x.x' = 1$ and $r_{i_2} = x'.x$ contained in the set of

algebra relations R; a deduction of the form

$$b_i \star x = b_j \Longrightarrow b_j \star x^{-1} = b_i$$

can only be made if relations as above are given. It follows that coincidences in the MGE-procedure must mainly be obtained by a full search, similarly to the HLT-strategy. This implies that generally many more definition steps take place compared to, for instance, a Felsch strategy and consequently a HLT-strategy can lead to a fast increase in the use of memory-space. In the case of coset-enumeration, the so-called *lookahead method* has been developed (described for instance in [9]). Lookahead methods mainly aim to combine periods of HLT-strategy with periods of intensive search of the multiplication table for possible deductions.

A version of the lookahead method is used in the MGE-procedure in order to detect those coincidences which already lie in the S-linear span of the so-far defined generators but which otherwise might have been found only at a later stage after many further definitions might have taken place. Phases where many definitions take place and where the table grows quickly, possibly followed by phases of many collapses when coincidences are found, are avoided this way.

The MGE-procedure, as it is implemented in GAP, begins by examining all the module-relations which then are added to Cp and eventually are processed. Then, for each $b \in B^u$, beginning with b_1 and following the ordering given by the indices, every algebra-relation $r \in R$ will be applied to b. After a certain number of definitions (the definite number has been decided on à priori) the lookahead mode is called.

This leads to scanning the remaining rows of the table for possible coincidences without any further definitions in order to obtain coincidences. Accordingly, such a search is not necessarily full and only in some cases will new coincidences be obtained. If however coincidences have been found then this means that memory space has been saved. In particular in the case where a coincidence is caused by an algebra-relation applied to $\widetilde{b} \in B^u$ with comparatively big index it is likely that unnecessary definitions have been avoided.

Subsequent to this call of lookahead the normal search for coincidences will proceed, applied at that generator $b \in B^u$ (in the case that b has not been deleted in the meantime) and that relation where lookahead had initially been invoked.

Note that there is an important difference between lookahead in coset enumeration and that in the MGE-procedure. If in a coset enumeration a coincidence is found this leads to setting cosets g_{i_1} and g_{i_2} equal. Suppose that g_{i_2} is the one which is going to get deleted ($g_{i_2} > g_{i_1}$). Only in the case that cosets $\widetilde{g}_{i_j}$ have been assigned to both the products $g_{i_j}.x$ for $j \in \{1,2\}$ and a group generator x, does such a coincidence above lead to a consequence. If only $\widetilde{g}_{i_2} := g_{i_2}.x$ has been assigned then we can simply deduce that $\widetilde{g}_{i_2} \sim g_{i_1}.x$. Then the process of computing a coincidence does not lead to a new definition step.

This is substantially different to the way coincidences are handled in the MGE-procedure. Here, whenever we find an applicable coincidence $c = \sum_{i=1}^{m} \lambda_i \cdot b_i$, we have $b_m = HM(c)$, if $b_m \star x \in \langle B \rangle$ and then computing the according consequence $c \star x$ might lead to many new definition steps. Therefore in order to handle the consequences of applicable coincidences we must allow that further definition steps can be made in the lookahead mode of the MGE-procedure.

In the current implementation of the MGE-procedure in GAP the lookahead procedure is called for the first time after 10 definitions have been made, thereafter every time the length of the table doubles. If the length of the table exceeds 500 then it will be invoked again after 500 definition steps have taken place.

7.2 Examples and Runtimes

We present the results and runtimes of some examples the presentations of which can be found in the appendix. The main problem has been found to be exceedingly large entries of the torsion sequence but also large entries of the multiplication table.

The second column of Table 7.1 on p.165 states the length of the multipli-

Table 7.1: Examples of Performance of the MGE-procedure

module	total length of T	"rank" of $\mathcal{M}_S$	Length of L	del.	del. lookahead	runtime
$\mathcal{M}_1$	13 (39)	2	1	11	0	0:00:00.020
$\mathcal{M}_1'$	321 (2121)	0	0	265	56	0:00:00.990
$\mathcal{M}_2$	14 (40)	3	3	8	3	0:00:00.020
$\mathcal{M}_2'$	177 (1684)	2	0	160	15	0:00:00.340
$\mathcal{M}_2''$	?	?	?			?
$\mathcal{M}_3$	11 (35)	2	0	9	0	0:00:00.010
$\mathcal{M}_3'$	?	?	?			?
$\mathcal{M}_4$	18 (40)	2	0	12	4	0:00:00.020
$\mathcal{M}_4'$	177 (1051)	0	0	51	126	0:00:00.370
$\mathcal{M}_5$	17 (55)	4	0	13	0	0:00:00.020
$\mathcal{M}_6$	14 (45)	3	0	11	0	0:00:00.020
$\mathcal{M}_6'$	?	?	?			?
$\mathcal{M}_7$	26 (109)	2	0	15	9	0:00:00.040
$\mathcal{M}_7'$	388 (1153)	0	0	58	330	0:00:00.600
$\mathcal{M}_8$	16 (47)	3	0	13	0	0:00:00.010
$\mathcal{M}_9$	122 (error)	4	4	42	76	0:00:00.940
$\mathcal{M}_{10}$	2060	660	0	710	690	0:00:30.630
$\widetilde{\mathcal{M}}_{10}$	3022	720	60	748	1554	0:01:57.910
$\mathcal{M}_{11}$	7083	720	0	2778	3585	0:04:42.140
$\mathcal{M}_{12}$	1703	163	103	39	1501	0:06:44.470
$\mathcal{M}_{13}$	617	70	0	250	297	0:00:04.860
$\mathcal{M}_{14}$	10369	826	0	951	8592	5:59:25.060
$\mathcal{M}_{15}$	2687	289	109	584	1814	0:20:09.280
$\mathcal{M}_{16}$	2381	272	272	72	2037	0:01:17.860
$\mathcal{M}_{17}$	166	1	1	20	145	0:50:54.630
$\mathcal{M}_{18}$	7527	2448	0	2956	2123	0:09:18.290
$\mathcal{M}_{19}$	2984	544	544	34	2406	0:18:25.810
$\mathcal{M}_{20}$	2125	264	0	1288	573	0:10:48.220

cation table. This corresponds to the total number of definitions which were necessary in order to compute the S-module generating set of the respective module. The numbers enclosed in brackets are the numbers of definitions necessary in an earlier version of the procedure.

The third column, titled with *"rank" of* $\mathcal{M}_S$ gives the number of generators which were found to be necessary at the point of termination. This number differs from the usual definition of the rank of a module: in this case we mean the number of the generators of the free submodule together with the generators of the torsion submodule.

The fourth column gives the length of the torsion sequence and therefore the number of torsion generators of the respective module. The columns five and six state the number of generators which have been deleted in the course of the procedure: the column "del. lookahead" gives the number of generators which have been deleted in the Lookahead mode, the column "del." the ones which have been deleted in the normal mode. The last column states the time needed in order for the procedure to terminate which is measured in "hours: minutes: seconds. milliseconds".

The rows where as results question marks are given have been obtained from computations of modules of derived sequences of polycyclic groups. In the given cases the MGE-procedure had not terminated after 10 hours. As the numbers produced by the respective computations had been large the procedures had then been interrupted.

Large Entries

From the above we can see that some of the procedures take much longer for the computation where the respective sets of generators do not appear overly large. The reason for this are often the numbers the procedure has to handle. These large numbers can be found in the torsion sequences but also in the matrices that describe the action of the generators $x \in X$ on the S-module generators. We have chosen only some of the modules above to show entries of the respective sequences and matrices. In Table 7.2 we give examples of largest entries found in the respective torsion sequences of some of the modules of Table 7.1.

In Table 7.3 we state the largest entries found in the matrices of some of the modules of Table 7.1. Since $\mathcal{M}_{17}$ is a P-module, where P is generated by four elements, we state in Table 7.3 the entry of each of the matrices describing the action of the respective generator. As can be seen in Table 7.1 the computation of the generating set of $\mathcal{M}_{17}$ took comparatively long.

Table 7.2: Torsion sequence entries

module	Length of L	maximal Element
$\widetilde{\mathcal{M}_{10}}$	60	177146
$\mathcal{M}_{12}$	103	3
$\mathcal{M}_{15}$	109	3
$\mathcal{M}_{16}$	272	19682
$\mathcal{M}_{17}$	1	2
$\mathcal{M}_{18}$	0	-
$\mathcal{M}_{19}$	544	2

Table 7.3: Matrix entries

module	"rank" of $\mathcal{M}_S$	largest element [1]
$\mathcal{M}_9$	4	10^{22}
$\mathcal{M}_{17}$	1	10^{158324}
$\mathcal{M}_{17}$	1	10^{60744}
$\mathcal{M}_{17}$	1	10^{167945}
$\mathcal{M}_{17}$	1	10^{171342}
$\mathcal{M}_{19}$	544	-280348

Computing Submodule-Presentations

In Table 7.4 we show the result of the computation of presentations of submodules $\widehat{\mathcal{N}_i}$ which belong to some of the modules $\mathcal{M}_i$ from Table 7.1. The

[1] The largest element by absolute value

second column gives the number of generators of the module $\widehat{\mathcal{N}}_i$ and the third column states the time necessary for computing these generators. In columns four and five we state the size of the sets Z_1 and Z_2 respectively. In the last column we state the runtime of the computation of the relations $Z_1 \cup Z_2$.

Table 7.4: Submodule Presentations

quotient module	no. of submodule generators	runtime	size of Z_1	size of Z_2	runtime
$\mathcal{M}_{15}$	728	0:00:01.510	2601	460	0:00:25.280
$\mathcal{M}_{16}$	499	0:00:01.860	918	466	00:14.890
$\mathcal{M}_{20}$	1322	0:00:07.370	8976	10	0:23:40.660

7.3 Conclusion

The main bottle-neck in the MGE-procedure seems to be the exceedingly large numbers which are possibly produced in the course of the computation as entries of the multiplication table and of the torsion sequence. With respect to the torsion sequence, tests have been made using the LLL-algorithm (for a description of this algorithm see [22]). Unfortunately it has been found that this algorithm does not necessarily improve the performance as part of the HANDLE INAPPLICABLE COINCIDENCES procedure consists of ordering the entries in a certain order which then negates the effect of the LLL-algorithm.

It is very likely that the MGE-procedure can be extended to the case of modules over general Euclidean domains and even principal ideal domains. Theorem 1.2.1 has been proved for such modules. Moreover, in the case of ideals of a principal ideal S the greatest common divisor of elements $\kappa, \lambda \in S$ is that element $\mu \in S$ such that $\langle \kappa, \lambda \rangle = \langle \mu \rangle$ for the respective ideals generated by these elements.

So in the case that certain computability conditions are satisfied by the PID, for instance that the GCD not only exists but can be computed as well, inapplicable coincidences could possibly be handled in a similar way.

The MGE-procedure however has been implemented in GAP only for modules over Euclidean domains, therefore this has not been thought through completely.

Appendix A

Presentations

Presentation $\mathcal{M}_1$ up to $\mathcal{M}_{20}$

The example $\mathcal{M}_1$ corresponds to the FpExamples(2, 4) from the IPCQ-package of GAP;

$\mathcal{M}_2$ corresponds to FpExamples(2, 10);

$\mathcal{M}_3$ corresponds to FpExamples(2, 11);

$\mathcal{M}_4$ corresponds to FpExamples(2, 12);

$\mathcal{M}_5$ corresponds to FpExamples(2, 13);

$\mathcal{M}_6$ corresponds to FpExamples(2, 14);

$\mathcal{M}_7$ corresponds to FpExamples(2, 15);

$\mathcal{M}_8$ corresponds to FpExamples(2, 16);

$\mathcal{M}_9$ corresponds to FpExamples(3, 4);

If modules have been denoted $\mathcal{M}_i'$ and $\mathcal{M}_i''$ then they have been obtained from the first step, or respectively the second, of the derived series.

Presentation $\mathcal{M}_{10}$

This example has been translated into the setting of modules and has been obtained from the presentation of $PSL_2(11) \mid E$ as in [39]. It has the

module-presentation:

$$\mathcal{M}_{10} = \langle y \rangle_P, \quad P = \langle x_1, x_2, x_3 \mid R \rangle_{\mathbb{Z}}$$

where

$$R = \{x_1.x_3 - 1, x_3.x_1 - 1, x_1^{11} - 1, (x_1.x_2)^3 - 1,$$
$$(x_1^4.x_2.x_3^5.x_2)^2 - 1, x_2^2 - 1\}.$$

Moreover we set

$$\widetilde{\mathcal{M}}_{10} = \langle y_1, y_2 \mid 3 \cdot y_2.x_1 - y_1 \rangle_P.$$

Presentation $\mathcal{M}_{11}$

This is a presentation of $L_2(8)$ (see the Atlas [11]) translated into the setting of algebras with an additional module-relation:

$$\mathcal{M}_{11} := \langle y \mid y.x_1 - y \rangle_P, \quad P := \langle x_1, x_2, x_3, x_4, x_5, x_6 \mid R \rangle_{\mathbb{Z}};$$

where $R := \{x_1.x_4 - 1, x_4.x_1 - 1, x_2.x_5 - 1, x_5.x_2 - 1,$

$x_3.x_6 - 1, x_6.x_3 - 1, x_1^{11} - 1, x_2^5 - 1, x_3^4 - 1, (x_1^4.x_3^2)^3 - 1, (x_2.x_3^2)^2 - 1, (x_1.x_2.x_3)^3 - 1,$

$$x_5.x_1.x_2.x_4^4 - 1, x_6.x_2.x_3.x_5^2 - 1\}.$$

Presentation $\mathcal{M}_{12}$

This is a presentation of A_5 translated into the setting of modules. The module $\mathcal{M}$ is of rank 3 and has further module-relations:

$$\mathcal{M}_{12} := \langle y_1, y_2, y_3 \mid y_1.x_1 + 2 \cdot y_2, 3 \cdot y_3 \rangle_P, \quad P := \langle x_1, x_2, x_3, x_4, x_5, x_6 \mid R \rangle_{\mathbb{Z}};$$

with algebra-relations $R := \{((x_i x_j)^2 - 1 \; \forall \; 1 \leq i \neq j \leq 3,$

$$x_1^3 - 1, \; x_2^3 - 1, x_3^3 - 1\}.$$

Presentation $\mathcal{M}_{13}$

A presentation obtained from S. Linton:

$$\mathcal{M}_{13} = \langle y \rangle_P, \qquad P = \langle x_1, x_2, x_3, x_4, x_5 \mid R \rangle_{\mathbb{Z}}$$

which is a standard example for tests for commutative Gröbner bases.

$$R := \{x_i x_j - x_j x_i \forall 1 \leq i, j \leq 5, x_1 + x_2 + x_3 + x_4 + x_5, x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1, x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2, x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3x_4, x_1x_2x_3x_4x_5 - 1\}$$

Presentation $\mathcal{M}_{14}$

A presentation obtained from S. Linton:

$$\mathcal{M}_{14} = \langle y \rangle_P, \qquad P = \langle x_1, x_2, x_3, x_4, x_5, x_6, x_7 \mid R \rangle_{\mathbb{Z}}$$

which is a standard example for tests for commutative Gröbner bases.

$$R = \{x_i x_j - x_j x_i \forall 1 \leq i, j \leq 7, x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7, \sum_{i=1}^{6} x_i x_{i+1} + x_7 x_1, \sum_{i=1}^{5} x_i x_{i+1} x_{i+2} + x_6 x_7 x_1 + x_7 x_1 x_2, \sum_{i=1}^{4} x_i x_{i+1} x_{i+2} x_{i+3} + x_5 x_6 x_7 x_1 + x_6 x_7 x_1 x_2 + x_7 x_1 x_2 x_3, \sum_{i=1}^{3} x_i x_{i+1} x_{i+2} x_{i+3} x_{i+4} + x_4 x_5 x_6 x_7 x_1 + x_5 x_6 x_7 x_1 x_2 + x_6 x_7 x_1 x_2 x_3 + x_7 x_1 x_2 x_3 x_4, x_1 x_2 x_3 x_4 x_5 x_6 + x_2 x_3 x_4 x_5 x_6 x_7 + x_3 x_4 x_5 x_6 x_7 x_1 + x_4 x_5 x_6 x_7 x_1 x_2 + x_5 x_6 x_7 x_1 x_2 x_3 + x_6 x_7 x_1 x_2 x_3 x_4 + x_7 x_1 x_2 x_3 x_4 x_5, x_1 x_2 x_3 x_4 x_5 x_6 x_7 - 1\}$$

Presentation $\mathcal{M}_{15}$

This is a presentation of A_5 translated into the setting of algebras, the module $\mathcal{M}$ is of rank 5 and has further module-relations:

$$\mathcal{M}_{15} := \langle y_1, y_2, y_3, y_4, y_5 \mid y_1.x_1 + 2 \cdot y_2, 3 \cdot y_3 \rangle_P, \quad P := \langle x_1, x_2, x_3, x_4, x_5, x_6 \mid R \rangle_{\mathbb{Z}};$$

$$R := \{((x_i x_j)^2 - 1 \forall 1 \leq i \neq j \leq 3, x_1^3 - 1, x_2^3 - 1, x_3^3 - 1\}.$$

Presentation $\mathcal{M}_{16}$

This is a presentation of $L_2(17)$ translated into the setting of algebras. The module $\mathcal{M}$ is a module of rank 1 over this algebra and has additional module-relations:

$$\mathcal{M}_{16} := \langle y \mid y.x_2x_1x_2 - 3 \cdot y \rangle_P$$

$$P := \langle x_1, x_2 \mid x_1^9 - 1, x_2^2 - 1, (x_1x_2)^4 - 1, (x_1^2x_2)^3 - 1 \rangle_{\mathbb{Z}};$$

Presentation $\mathcal{M}_{17}$

The given algebra-presentation is a presentation of $L_(3)$ translated into the setting of algebras.

$$\mathcal{M}_{17} = \langle y \mid U \rangle_P, \quad P = \langle x_1, x_2, x_3, x_4 \mid R \rangle_{\mathbb{Z}}$$

The module $\mathcal{M}$ is a module of rank 1 over this algebra and has additional module-relations:

$$U := \{y.(x_1x_2x_1)^2 - y.x_2x_1, y.x_1 + y.x_1^2 + y.x_1^3 + y.x_1^4 - y.x_2 - y.x_2^2, 2 \cdot y, y.(x_1x_2)^2 - y.x_2^2x_1\}$$

$$R := x_i.x_{i+2} - 1 \text{ for } i \in \{1,2\}, x_i.x_{i-2} - 1 \text{ for } i \in \{3,4\}, x_1^6 - 1, x_2^3 - 1,$$

$$(x_1x_2)^4 - 1, (x_1^2x_2)^4 - 1, (x_1^3x_2)^3 - 1, x_1^2(x_2x_1^2x_2)^2x_3^2x_4x_3^2x_4^2x_3^2x_4 - 1$$

Presentation $\mathcal{M}_{18}$

The given algebra-presentation is a presentation of $L_2(17)$ translated into the setting of algebras.

$$\mathcal{M}_{18} = \langle y_1, y_2 \mid U \rangle_P \quad P = \langle x_1, x_2 \mid R \rangle_{\mathbb{Z}}$$

The module $\mathcal{M}_{22}$ is a module of rank 2 over this algebra. The algebra has relations

$$R = \{x_2^2 - 1, (x_1x_2)^4 - 1, (x_1^2x_2)^3 - 1, x_1^9 - 1\},$$

the module has the additional module-relations

$$U = \{y_1.x_2 - y_1 + 3 \cdot y_1.x_2^2, y_1.x_1 + y_1.x_1x_2 + y_1.x_1x_2x_1 + y.x_2x_1 + y_1.x_1\}.$$

Presentation $\mathcal{M}_{19}$

The given algebra-presentation is a presentation of $L_2(17)$ translated into the setting of algebras. The given module is of rank 1 over this algebra,

$$\mathcal{M}_{19} = \langle y \mid U \rangle_P \quad P = \langle x_1, x_2 \mid R \rangle_{\mathbb{Z}}$$

The algebra has relations

$$R = \{x_2^2 - 1, (x_1x_2)^4 - 1, (x_1^2x_2)^3 - 1, x_1^9 - 1\},$$

the module has the additional module-relations

$$U := \{y.(x_2x_1^2)^3 - 3 \cdot y; y.x_1 - y + 3 \cdot y.x_1^2\}.$$

Presentation $\mathcal{M}_{20}$

$$\mathcal{M}_{20} := \langle y_1 \rangle_P, \quad P := \langle x_1, x_2, x_3, x_4, x_5, x_6 \mid R \rangle_{(\mathbb{Z}(17)};$$

$$R := \{x_1 \cdot x_4, x_4 \cdot x_1, x_2 \cdot x_5, x_5 \cdot x_2, x_3 \cdot x_6, x_6 \cdot x_3, 16 \cdot x_1 + x_1 \cdot x_1, 16 \cdot x_4 + x_4 \cdot x_4,$$

$$16 \cdot x_2 + x_2 \cdot x_2, 16 \cdot x_5 + x_5 \cdot x_5, 16 \cdot x_3 + x_3 \cdot x_3,$$

$$16 \cdot x_6 + x_6 \cdot x_6, x_1 \cdot x_6 + 16 \cdot x_6 \cdot x_1, x_3 \cdot x_4 + 16 \cdot x_4 \cdot x_3, x_1 \cdot x_3 + 16 \cdot x_3 \cdot x_1, 16 \cdot x_4 \cdot x_6 + x_6 \cdot x_4,$$

$$9 \cdot x_1 + 8 \cdot x_2 + 11 \cdot x_4 + 6 \cdot x_5 + 7 \cdot x_1 \cdot x_4 + 10 \cdot x_2 \cdot x_5 + 7 \cdot x_4 \cdot x_1 + 10 \cdot x_5 \cdot x_2 +$$

$$2 \cdot x_1 \cdot x_2 \cdot x_1 + 15 \cdot x_1 \cdot x_2 \cdot x_4 + 15 \cdot x_1 \cdot x_5 \cdot x_1 + 2 \cdot x_1 \cdot x_5 \cdot x_4 +$$

$$15 \cdot x_2 \cdot x_1 \cdot x_2 + 2 \cdot x_2 \cdot x_1 \cdot x_5 + 2 \cdot x_2 \cdot x_4 \cdot x_2 + 15 \cdot x_2 \cdot x_4 \cdot x_5 + 15 \cdot x_4 \cdot x_2 \cdot x_1 +$$

$$2 \cdot x_4 \cdot x_2 \cdot x_4 + 2 \cdot x_4 \cdot x_5 \cdot x_1 + 15 \cdot x_4 \cdot x_5 \cdot x_4 + 2 \cdot x_5 \cdot x_1 \cdot x_2 + 15 \cdot x_5 \cdot x_1 \cdot x_5 +$$

$$15 \cdot x_5 \cdot x_4 \cdot x_2 + 2 \cdot x_5 \cdot x_4 \cdot x_5, 5 \cdot x_1 + 12 \cdot x_2 + 9 \cdot x_4 + 8 \cdot x_5 + 15 \cdot x_1 \cdot x_4 +$$

$$13 \cdot x_2 \cdot x_4 + 15 \cdot x_2 \cdot x_5 + 2 \cdot x_4 \cdot x_1 + 4 \cdot x_5 \cdot x_1 + 2 \cdot x_5 \cdot x_2 + 3 \cdot x_1 \cdot x_2 \cdot x_1 +$$

$$3 \cdot x_1 \cdot x_2 \cdot x_4 + 14 \cdot x_1 \cdot x_5 \cdot x_1 + 14 \cdot x_1 \cdot x_5 \cdot x_4 +$$

$$14 \cdot x_2 \cdot x_1 \cdot x_2 + 3 \cdot x_2 \cdot x_1 \cdot x_5 + 3 \cdot x_2 \cdot x_4 \cdot x_2 + 14 \cdot x_2 \cdot x_4 \cdot x_5 +$$

$$14 \cdot x_4 \cdot x_2 \cdot x_1 + 14 \cdot x_4 \cdot x_2 \cdot x_4 + 3 \cdot x_4 \cdot x_5 \cdot x_1 + 3 \cdot x_4 \cdot x_5 \cdot x_4 +$$

$$14\cdot x_5\cdot x_1\cdot x_2+3\cdot x_5\cdot x_1\cdot x_5+3\cdot x_5\cdot x_4\cdot x_2+14\cdot x_5\cdot x_4\cdot x_5, 3\cdot x_1+14\cdot x_2+14\cdot x_4+3\cdot x_5+12\cdot x_1\cdot x_4+$$
$$4\cdot x_2\cdot x_4+9\cdot x_2\cdot x_5+8\cdot x_4\cdot x_1+13\cdot x_5\cdot x_1+5\cdot x_5\cdot x_2+12\cdot x_1\cdot x_2\cdot x_1+16\cdot x_1\cdot x_2\cdot x_4+$$
$$5\cdot x_1\cdot x_5\cdot x_1+x_1\cdot x_5\cdot x_4+5\cdot x_2\cdot x_1\cdot x_2+12\cdot x_2\cdot x_1\cdot x_5+12\cdot x_2\cdot x_4\cdot x_2+5\cdot x_2\cdot x_4\cdot x_5+5\cdot x_4\cdot x_2\cdot x_1+$$
$$x_4\cdot x_2\cdot x_4+12\cdot x_4\cdot x_5\cdot x_1+16\cdot x_4\cdot x_5\cdot x_4+x_5\cdot x_1\cdot x_2+16\cdot x_5\cdot x_1\cdot x_5+16\cdot x_5\cdot x_4\cdot x_2+x_5\cdot x_4\cdot x_5,$$
$$5\cdot x_1+12\cdot x_2+9\cdot x_4+8\cdot x_5+2\cdot x_1\cdot x_4+4\cdot x_1\cdot x_5+2\cdot x_2\cdot x_5+15\cdot x_4\cdot x_1+13\cdot x_4\cdot x_2+$$
$$15\cdot x_5\cdot x_2+3\cdot x_1\cdot x_2\cdot x_1+14\cdot x_1\cdot x_2\cdot x_4+$$
$$14\cdot x_1\cdot x_5\cdot x_1+3\cdot x_1\cdot x_5\cdot x_4+14\cdot x_2\cdot x_1\cdot x_2+$$
$$14\cdot x_2\cdot x_1\cdot x_5+3\cdot x_2\cdot x_4\cdot x_2+3\cdot x_2\cdot x_4\cdot x_5+3\cdot x_4\cdot x_2\cdot x_1+$$
$$14\cdot x_4\cdot x_2\cdot x_4+14\cdot x_4\cdot x_5\cdot x_1+$$
$$3\cdot x_4\cdot x_5\cdot x_4+3\cdot x_5\cdot x_1\cdot x_2+3\cdot x_5\cdot x_1\cdot x_5+$$
$$14\cdot x_5\cdot x_4\cdot x_2+14\cdot x_5\cdot x_4\cdot x_5, 4\cdot x_1+13\cdot x_2+4\cdot x_4+13\cdot x_5+11\cdot x_1\cdot x_4+$$
$$4\cdot x_1\cdot x_5+13\cdot x_2\cdot x_4+6\cdot x_2\cdot x_5+11\cdot x_4\cdot x_1+13\cdot x_4\cdot x_2+4\cdot x_5\cdot x_1+$$
$$6\cdot x_5\cdot x_2+16\cdot x_1\cdot x_2\cdot x_1+10\cdot x_1\cdot x_2\cdot x_4+7\cdot x_1\cdot x_5\cdot x_1+x_1\cdot x_5\cdot x_4+x_2\cdot x_1\cdot x_2+$$
$$7\cdot x_2\cdot x_1\cdot x_5+10\cdot x_2\cdot x_4\cdot x_2+16\cdot x_2\cdot x_4\cdot x_5+10\cdot x_4\cdot x_2\cdot x_1+16\cdot x_4\cdot x_2\cdot x_4+$$
$$x_4\cdot x_5\cdot x_1+7\cdot x_4\cdot x_5\cdot x_4+7\cdot x_5\cdot x_1\cdot x_2+x_5\cdot x_1\cdot x_5+16\cdot x_5\cdot x_4\cdot x_2+10\cdot x_5\cdot x_4\cdot x_5,$$
$$12\cdot x_1+5\cdot x_2+8\cdot x_4+9\cdot x_5+14\cdot x_1\cdot x_4+4\cdot x_1\cdot x_5+8\cdot x_2\cdot x_4+8\cdot x_2\cdot x_5+$$
$$9\cdot x_4\cdot x_1+13\cdot x_4\cdot x_2+9\cdot x_5\cdot x_1+3\cdot x_5\cdot x_2+14\cdot x_1\cdot x_2\cdot x_1+3\cdot x_1\cdot x_2\cdot x_4+$$
$$12\cdot x_1\cdot x_5\cdot x_1+6\cdot x_1\cdot x_5\cdot x_4+3\cdot x_2\cdot x_1\cdot x_2+12\cdot x_2\cdot x_1\cdot x_5+$$
$$5\cdot x_2\cdot x_4\cdot x_2+14\cdot x_2\cdot x_4\cdot x_5+5\cdot x_4\cdot x_2\cdot x_1+11\cdot x_4\cdot x_2\cdot x_4+$$
$$3\cdot x_4\cdot x_5\cdot x_1+14\cdot x_4\cdot x_5\cdot x_4+14\cdot x_5\cdot x_1\cdot x_2+6\cdot x_5\cdot x_1\cdot x_5+$$
$$11\cdot x_5\cdot x_4\cdot x_2+3\cdot x_5\cdot x_4\cdot x_5,$$
$$3\cdot x_1+14\cdot x_2+14\cdot x_4+3\cdot x_5+8\cdot x_1\cdot x_4+13\cdot x_1\cdot x_5+$$
$$5\cdot x_2\cdot x_5+12\cdot x_4\cdot x_1+4\cdot x_4\cdot x_2+9\cdot x_5\cdot x_2+12\cdot x_1\cdot x_2\cdot x_1+$$
$$5\cdot x_1\cdot x_2\cdot x_4+5\cdot x_1\cdot x_5\cdot x_1+12\cdot x_1\cdot x_5\cdot x_4+5\cdot x_2\cdot x_1\cdot x_2+$$

$$x_2 \cdot x_1 \cdot x_5 + 12 \cdot x_2 \cdot x_4 \cdot x_2 + 16 \cdot x_2 \cdot x_4 \cdot x_5 + 16 \cdot x_4 \cdot x_2 \cdot x_1 + x_4 \cdot x_2 \cdot x_4 +$$

$$x_4 \cdot x_5 \cdot x_1 + 16 \cdot x_4 \cdot x_5 \cdot x_4 + 12 \cdot x_5 \cdot x_1 \cdot x_2 + 16 \cdot x_5 \cdot x_1 \cdot x_5 + 5 \cdot x_5 \cdot x_4 \cdot x_2 + x_5 \cdot x_4 \cdot x_5,$$

$$12 \cdot x_1 + 5 \cdot x_2 + 8 \cdot x_4 + 9 \cdot x_5 + 9 \cdot x_1 \cdot x_4 + 9 \cdot x_1 \cdot x_5 + 13 \cdot x_2 \cdot x_4 +$$

$$3 \cdot x_2 \cdot x_5 + 14 \cdot x_4 \cdot x_1 + 8 \cdot x_4 \cdot x_2 + 4 \cdot x_5 \cdot x_1 +$$

$$8 \cdot x_5 \cdot x_2 +$$

$$14 \cdot x_1 \cdot x_2 \cdot x_1 + 5 \cdot x_1 \cdot x_2 \cdot x_4 +$$

$$12 \cdot x_1 \cdot x_5 \cdot x_1 + 3 \cdot x_1 \cdot x_5 \cdot x_4 + 3 \cdot x_2 \cdot x_1 \cdot x_2 +$$

$$14 \cdot x_2 \cdot x_1 \cdot x_5 + 5 \cdot x_2 \cdot x_4 \cdot x_2 + 11 \cdot x_2 \cdot x_4 \cdot x_5 +$$

$$3 \cdot x_4 \cdot x_2 \cdot x_1 + 11 \cdot x_4 \cdot x_2 \cdot x_4 +$$

$$6 \cdot x_4 \cdot x_5 \cdot x_1 + 14 \cdot x_4 \cdot x_5 \cdot x_4 + 12 \cdot x_5 \cdot x_1 \cdot x_2 + 6 \cdot x_5 \cdot x_1 \cdot x_5 + 14 \cdot x_5 \cdot x_4 \cdot x_2 + 3 \cdot x_5 \cdot x_4 \cdot x_5,$$

$$11 \cdot x_1 + 6 \cdot x_2 + 3 \cdot x_4 + 14 \cdot x_5 + 2 \cdot x_1 \cdot x_4 + 9 \cdot x_1 \cdot x_5 + 8 \cdot x_2 \cdot x_4 + 15 \cdot x_2 \cdot x_5 + 2 \cdot x_4 \cdot x_1 + 8 \cdot x_4 \cdot x_2 +$$

$$9 \cdot x_5 \cdot x_1 + 15 \cdot x_5 \cdot x_2 + 10 \cdot x_1 \cdot x_2 \cdot x_1 + 10 \cdot x_1 \cdot x_2 \cdot x_4 + 6 \cdot x_1 \cdot x_5 \cdot x_1 + x_1 \cdot x_5 \cdot x_4 +$$

$$7 \cdot x_2 \cdot x_1 \cdot x_2 + 7 \cdot x_2 \cdot x_1 \cdot x_5 + 11 \cdot x_2 \cdot x_4 \cdot x_2 + 16 \cdot x_2 \cdot x_4 \cdot x_5 + 10 \cdot x_4 \cdot x_2 \cdot x_1 + 15 \cdot x_4 \cdot x_2 \cdot x_4 +$$

$$x_4 \cdot x_5 \cdot x_1 + x_4 \cdot x_5 \cdot x_4 + 7 \cdot x_5 \cdot x_1 \cdot x_2 +$$

$$2 \cdot x_5 \cdot x_1 \cdot x_5 + 16 \cdot x_5 \cdot x_4 \cdot x_2 + 16 \cdot x_5 \cdot x_4 \cdot x_5,$$

$$9 \cdot x_2 + 8 \cdot x_3 + 11 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_2 \cdot x_5 + 10 \cdot x_3 \cdot x_6 + 7 \cdot x_5 \cdot x_2 + 10 \cdot x_6 \cdot x_3 + 2 \cdot x_2 \cdot x_3 \cdot x_2 + 15 \cdot x_2 \cdot x_3 \cdot x_5 +$$

$$15 \cdot x_2 \cdot x_6 \cdot x_2 + 2 \cdot x_2 \cdot x_6 \cdot x_5 + 15 \cdot x_3 \cdot x_2 \cdot x_3 + 2 \cdot x_3 \cdot x_2 \cdot x_6 + 2 \cdot x_3 \cdot x_5 \cdot x_3 +$$

$$15 \cdot x_3 \cdot x_5 \cdot x_6 +$$

$$15 \cdot x_5 \cdot x_3 \cdot x_2 + 2 \cdot x_5 \cdot x_3 \cdot x_5 + 2 \cdot x_5 \cdot x_6 \cdot x_2 + 15 \cdot x_5 \cdot x_6 \cdot x_5 + 2 \cdot x_6 \cdot x_2 \cdot x_3 + 15 \cdot x_6 \cdot x_2 \cdot x_6 +$$

$$15 \cdot x_6 \cdot x_5 \cdot x_3 + 2 \cdot x_6 \cdot x_5 \cdot x_6, 5 \cdot x_2 + 12 \cdot x_3 + 9 \cdot x_5 + 8 \cdot x_6 + 15 \cdot x_2 \cdot x_5 + 13 \cdot x_3 \cdot x_5 + 15 \cdot x_3 \cdot x_6 + 2 \cdot x_5 \cdot x_2 +$$

$$4 \cdot x_6 \cdot x_2 + 2 \cdot x_6 \cdot x_3 + 3 \cdot x_2 \cdot x_3 \cdot x_2 + 3 \cdot x_2 \cdot x_3 \cdot x_5 + 14 \cdot x_2 \cdot x_6 \cdot x_2 + 14 \cdot x_2 \cdot x_6 \cdot x_5 +$$

$$14 \cdot x_3 \cdot x_2 \cdot x_3 + 3 \cdot x_3 \cdot x_2 \cdot x_6 + 3 \cdot x_3 \cdot x_5 \cdot x_3 +$$

$$14 \cdot x_3 \cdot x_5 \cdot x_6 + 14 \cdot x_5 \cdot x_3 \cdot x_2 + 14 \cdot x_5 \cdot x_3 \cdot x_5 + 3 \cdot x_5 \cdot x_6 \cdot x_2 +$$

$$3 \cdot x_5 \cdot x_6 \cdot x_5 + 14 \cdot x_6 \cdot x_2 \cdot x_3 + 3 \cdot x_6 \cdot x_2 \cdot x_6 + 3 \cdot x_6 \cdot x_5 \cdot x_3 + 14 \cdot x_6 \cdot x_5 \cdot x_6,$$

$$3\cdot x_2+14\cdot x_3+14\cdot x_5+3\cdot x_6+12\cdot x_2\cdot x_5+4\cdot x_3\cdot x_5+9\cdot x_3\cdot x_6+8\cdot x_5\cdot x_2+13\cdot x_6\cdot x_2+5\cdot x_6\cdot x_3+$$
$$12\cdot x_2\cdot x_3\cdot x_2+16\cdot x_2\cdot x_3\cdot x_5+5\cdot x_2\cdot x_6\cdot x_2+x_2\cdot x_6\cdot x_5+5\cdot x_3\cdot x_2\cdot x_3+12\cdot x_3\cdot x_2\cdot x_6+$$
$$12\cdot x_3\cdot x_5\cdot x_3+5\cdot x_3\cdot x_5\cdot x_6+5\cdot x_5\cdot x_3\cdot x_2+x_5\cdot x_3\cdot x_5+12\cdot x_5\cdot x_6\cdot x_2+16\cdot x_5\cdot x_6\cdot x_5+$$
$$x_6\cdot x_2\cdot x_3+16\cdot x_6\cdot x_2\cdot x_6+16\cdot x_6\cdot x_5\cdot x_3+x_6\cdot x_5\cdot x_6,$$
$$5\cdot x_2+12\cdot x_3+9\cdot x_5+8\cdot x_6+2\cdot x_2\cdot x_5+4\cdot x_2\cdot x_6+2\cdot x_3\cdot x_6+15\cdot x_5\cdot x_2+13\cdot x_5\cdot x_3+15\cdot x_6\cdot x_3+$$
$$3\cdot x_2\cdot x_3\cdot x_2+14\cdot x_2\cdot x_3\cdot x_5+14\cdot x_2\cdot x_6\cdot x_2+3\cdot x_2\cdot x_6\cdot x_5+14\cdot x_3\cdot x_2\cdot x_3+$$
$$14\cdot x_3\cdot x_2\cdot x_6+3\cdot x_3\cdot x_5\cdot x_3+3\cdot x_3\cdot x_5\cdot x_6+3\cdot x_5\cdot x_3\cdot x_2+14\cdot x_5\cdot x_3\cdot x_5+$$
$$14\cdot x_5\cdot x_6\cdot x_2+3\cdot x_5\cdot x_6\cdot x_5+3\cdot x_6\cdot x_2\cdot x_3+3\cdot x_6\cdot x_2\cdot x_6+14\cdot x_6\cdot x_5\cdot x_3+14\cdot x_6\cdot x_5\cdot x_6,$$
$$4\cdot x_2+13\cdot x_3+4\cdot x_5+13\cdot x_6+11\cdot x_2\cdot x_5+4\cdot x_2\cdot x_6+13\cdot x_3\cdot x_5+6\cdot x_3\cdot x_6+11\cdot x_5\cdot x_2+13\cdot x_5\cdot x_3+$$
$$4\cdot x_6\cdot x_2+6\cdot x_6\cdot x_3+16\cdot x_2\cdot x_3\cdot x_2+10\cdot x_2\cdot x_3\cdot x_5+7\cdot x_2\cdot x_6\cdot x_2+x_2\cdot x_6\cdot x_5+$$
$$x_3\cdot x_2\cdot x_3+$$
$$7\cdot x_3\cdot x_2\cdot x_6+10\cdot x_3\cdot x_5\cdot x_3+16\cdot x_3\cdot x_5\cdot x_6+10\cdot x_5\cdot x_3\cdot x_2+16\cdot x_5\cdot x_3\cdot x_5+x_5\cdot x_6\cdot x_2+7\cdot x_5\cdot x_6\cdot x_5+$$
$$7\cdot x_6\cdot x_2\cdot x_3+x_6\cdot x_2\cdot x_6+16\cdot x_6\cdot x_5\cdot x_3+10\cdot x_6\cdot x_5\cdot x_6, 12\cdot x_2+5\cdot x_3+8\cdot x_5+9\cdot x_6+14\cdot x_2\cdot x_5+4\cdot x_2\cdot x_6+$$
$$8\cdot x_3\cdot x_5+8\cdot x_3\cdot x_6+9\cdot x_5\cdot x_2+13\cdot x_5\cdot x_3+9\cdot x_6\cdot x_2+3\cdot x_6\cdot x_3+14\cdot x_2\cdot x_3\cdot x_2+3\cdot x_2\cdot x_3\cdot x_5+$$
$$12\cdot x_2\cdot x_6\cdot x_2+6\cdot x_2\cdot x_6\cdot x_5+3\cdot x_3\cdot x_2\cdot x_3+12\cdot x_3\cdot x_2\cdot x_6+5\cdot x_3\cdot x_5\cdot x_3+14\cdot x_3\cdot x_5\cdot x_6+5\cdot x_5\cdot x_3\cdot x_2+$$
$$11\cdot x_5\cdot x_3\cdot x_5+3\cdot x_5\cdot x_6\cdot x_2+14\cdot x_5\cdot x_6\cdot x_5+14\cdot x_6\cdot x_2\cdot x_3+6\cdot x_6\cdot x_2\cdot x_6+11\cdot x_6\cdot x_5\cdot x_3+3\cdot x_6\cdot x_5\cdot x_6,$$
$$3\cdot x_2+14\cdot x_3+14\cdot x_5+3\cdot x_6+8\cdot x_2\cdot x_5+13\cdot x_2\cdot x_6+5\cdot x_3\cdot x_6+12\cdot x_5\cdot x_2+$$
$$4\cdot x_5\cdot x_3+9\cdot x_6\cdot x_3+12\cdot x_2\cdot x_3\cdot x_2+5\cdot x_2\cdot x_3\cdot x_5+5\cdot x_2\cdot x_6\cdot x_2+$$
$$12\cdot x_2\cdot x_6\cdot x_5+5\cdot x_3\cdot x_2\cdot x_3+x_3\cdot x_2\cdot x_6+12\cdot x_3\cdot x_5\cdot x_3+16\cdot x_3\cdot x_5\cdot x_6+16\cdot x_5\cdot x_3\cdot x_2+$$
$$x_5\cdot x_3\cdot x_5+x_5\cdot x_6\cdot x_2+16\cdot x_5\cdot x_6\cdot x_5+12\cdot x_6\cdot x_2\cdot x_3+$$
$$16\cdot x_6\cdot x_2\cdot x_6+5\cdot x_6\cdot x_5\cdot x_3+x_6\cdot x_5\cdot x_6, 12\cdot x_2+5\cdot x_3+8\cdot x_5+9\cdot x_6+9\cdot x_2\cdot x_5+9\cdot x_2\cdot x_6+$$
$$13\cdot x_3\cdot x_5+3\cdot x_3\cdot x_6+14\cdot x_5\cdot x_2+8\cdot x_5\cdot x_3+4\cdot x_6\cdot x_2+8\cdot x_6\cdot x_3+14\cdot x_2\cdot x_3\cdot x_2+$$
$$5\cdot x_2\cdot x_3\cdot x_5+12\cdot x_2\cdot x_6\cdot x_2+3\cdot x_2\cdot x_6\cdot x_5+3\cdot x_3\cdot x_2\cdot x_3+14\cdot x_3\cdot x_2\cdot x_6+5\cdot x_3\cdot x_5\cdot x_3+$$
$$11\cdot x_3\cdot x_5\cdot x_6+3\cdot x_5\cdot x_3\cdot x_2+11\cdot x_5\cdot x_3\cdot x_5+6\cdot x_5\cdot x_6\cdot x_2+14\cdot x_5\cdot x_6\cdot x_5+$$

$$12 \cdot x_6 \cdot x_2 \cdot x_3 + 6 \cdot x_6 \cdot x_2 \cdot x_6 + 14 \cdot x_6 \cdot x_5 \cdot x_3 + 3 \cdot x_6 \cdot x_5 \cdot x_6, 11 \cdot x_2 + 6 \cdot x_3 +$$

$$3 \cdot x_5 + 14 \cdot x_6 + 2 \cdot x_2 \cdot x_5 + 9 \cdot x_2 \cdot x_6 + 8 \cdot x_3 \cdot x_5 + 15 \cdot x_3 \cdot x_6 +$$

$$2 \cdot x_5 \cdot x_2 + 8 \cdot x_5 \cdot x_3 + 9 \cdot x_6 \cdot x_2 + 15 \cdot x_6 \cdot x_3 +$$

$$10 \cdot x_2 \cdot x_3 \cdot x_2 + 10 \cdot x_2 \cdot x_3 \cdot x_5 + 6 \cdot x_2 \cdot x_6 \cdot x_2 + x_2 \cdot x_6 \cdot x_5 + 7 \cdot x_3 \cdot x_2 \cdot x_3 + 7 \cdot x_3 \cdot x_2 \cdot x_6 + 11 \cdot x_3 \cdot x_5 \cdot x_3 +$$

$$16 \cdot x_3 \cdot x_5 \cdot x_6 + 10 \cdot x_5 \cdot x_3 \cdot x_2 + 15 \cdot x_5 \cdot x_3 \cdot x_5 + x_5 \cdot x_6 \cdot x_2 +$$

$$x_5 \cdot x_6 \cdot x_5 + 7 \cdot x_6 \cdot x_2 \cdot x_3 + 2 \cdot x_6 \cdot x_2 \cdot x_6 + 16 \cdot x_6 \cdot x_5 \cdot x_3 + 16 \cdot x_6 \cdot x_5 \cdot x_6$$

Index of Notation

Bibliography

[1] Adams, W. W., & Loustaunau, P. (1994). *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics, Amer. Math. Soc.

[2] Arrell, D. G., & Robertson, E. F. (1984). A modified Todd-Coxeter algorithm. In Atkinson, M. D. (ed.), *Computational Group Theory.* London: Academic Press. pp. 27 – 32.

[3] Artin, M. (1991). *Algebra.* Prentice Hall Inc.

[4] Atkinson, M. D. (ed.) (1984). *Computational Group Theory.* London: Academic Press.

[5] Becker, T., & Weispfenning, V., in Cooperation with Kredel, H. (1993) *Gröbner Bases: A Computational Approach to Commutative Algebra.* Springer-Verlag, New York.

[6] Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Dissertation, Universität Innsbruck.

[7] Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In Bose, N. K. (ed.), *Multidimensional Systems Theory.* Reidel, Dordrecht, 184–232.

[8] Cannon, J. J. (1973). Construction of defining relations for finite groups. *Discrete Math.,* 5: 105 –29.

[9] Cannon, J. J., Dimino, L. A., Havas, G., & Watson, J. M. (1973). Implementation and analysis of the Todd-Coxeter algorithm. *Math. Comput.* 27: 463 –490.

[10] Carmody, S., Leeming, M., & Walters, R. F. C. (1995). The Todd-Coxeter Procedure and Left Kan Extensions. *J. Symbolic Comp.*, 19(5): 459–488.

[11] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., & Wilson, R. A. (1985). *Atlas of finite groups.* Clarendon Press, Oxford.

[12] Cox, D., Little, J., & O'Shea, D. (1992). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Verlag, Berlin and New York.

[13] Eick, B., Niemeyer, A. C., & Oreste, P. (2003). A polycyclic quotient algorithm. Preprint.

[14] Felsch, V. (1961). Programmierung der Restklassenabzählung einer Gruppe nach Untergruppen. *Numer. Math.*, 3: 250–256.

[15] The GAP group (2005). GAP – *Groups, Algorithms and Programming, Version 4.4.* `http://www.gap-system.org)`.

[16] Havas, G. (1991). Coset Enumeration Strategies. In *ISSAC '91, Proc.Symposium on Symbolic and Algebraic Computation* (Bonn 1991), pp. 191–9. Association for Computing Machinery.

[17] Johnson, D. L. (1980). *Topics in the theory of group presentations.* London Math. Soc. Lecture Note Series, Vol. 42, Cambridge University Press, Cambridge.

[18] Labonté, G. (1990) An algorithm for the construction of matrix representations for finitely presented non-commutative algebras. *J. Symbolic Comp.*, 9: 27 – 38.

[19] Lang, S. (1970). *Algebra.* Addison-Wesley, Reading, MA.

[20] Leech, J. (1963). Coset enumeration on digital computers. *Proc. Cambridge Philos. Soc.*, 257 –67.

[21] Leedham-Green. C.R. (1984). A soluble group algorithm. In Atkinson, M. D. (ed.), *Computational Group Theory.* London: Academic Press. pp. 85 – 101.

[22] Lenstra, A. K., Lenstra, H. W., Jr., & Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math. Ann.*, 261: 515–34.

[23] Linton, S. A. (1991a). Double coset enumeration. *J. Symbolic Comp.*, 12:415 –26.

[24] Linton, S. A. (1991b). Constructing matrix representations of finitely presented groups. *J. Symbolic Comp.*, 12: 427–38.

[25] Linton, S. A. (1993). On vector enumeration. *Linear Algebra and Applications,* 192: 235–248.

[26] Linton, S. A. (2000). A vector enumeration algorithm for modules over principal ideal rings. Unpublished.

[27] Lo, E. H. (1998). Finding intersections and normalizers in finitely generated nilpotent groups. *J. Symbolic Computations*, 25: 45–59.

[28] Lo, E. H. (1998). A polycyclic quotient algorithm. *J. Symbolic Comput.,* 25(1): 61–97.

[29] MacLane, S., Birkhoff, G. (1979). *Algebra.* Maxmillan Publishing Co., Inc., New York.

[30] Mendelsohn, N. S. (1964). An algorithmic solution for a word problem in group theory. *Canad. J. Math.* 16: 509–516. (1965). Correction. *Canad. J. Math.* 17: 505.

[31] Müller, J. (2003). A note on applications of the 'Vector Enumerator' algorithm. *Linear Algebra Appl.* 365: 291–300.

[32] Neubüser, J. (1982). An elementary introduction to coset table methods in computational group theory. In C. M. Campbell & E. F. Robertson (eds.), *Groups – St Andrews 1981,* pp. 1–45. London Math. Soc. Lecture Note Series 71. Cambridge: Cambridge University Press.

[33] Neubüser, J., & Sidki, S. (1988). Some computational approaches to groups given by a finite presentation. Published as Alguns procedimentos computacionais para grupos dados por uma apresentação finita. *Matemática Universitária,* Junho de 1988, Número 7, pp. 77–120.

[34] Reinert, B., & Madlener, K. (1993). On Gröbner bases in monoid and group rings. Report SR-93-08, SEKI, Universität Kaiserslautern.

[35] Reinert, B. (1995). On Gröbner bases in monoid and group rings. Dissertation, Universität Kaiserslautern.

[36] Reinert, B. (1998). Observations on Coset Enumeration. Reports on Computer Algebra No. 23, Centre for Computer Algebra. Universität Kaiserslautern.

[37] Reinert, B., Mora, T., & Madlener, K. (1998). A Note on Nielsen Reduction and Coset Enumeration. In *ISSAC'98,* pp. 171–178.

[38] Reinert, B., Mora, T., & Madlener, K. (1998). Coset enumeration – a comparison of methods. Technical report, Universität Kaiserslautern.

[39] Reinert, B., & Zeckzer, D. (1999). Coset enumeration using prefix Gröbner bases in MRC – An experimental approach. Reports on Computer Algebra Nr. 25. Centre for Computer Algebra, Universität Kaiserslautern.

[40] Schreier, O. (1927). Die Untergruppen der freien Gruppen. *Abh. Math. Sem. Hamburg,* 5:161–83.

[41] Sims, C. C. (1994). *Computation with finitely presented groups.* Volume 48 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge.

[42] Taylor, P. Commutative diagrams package for LaTeX, version 3.90.

[43] Todd, J. A., & Coxeter, H. S. M. (1936). A practical method for enumerating cosets of finite abstract groups. *Proc. Edinburgh Math. Soc.*, 5:26–34.

[44] Trotter, H. F. (1964). A machine program for coset enumeration. Canad. Math. Bull. 7: 357–368.