On Gröbner Bases

in

Monoid and Group Rings

Vom Fachbereich Informatik
der Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Naturwissenschaften (Dr. rer. nat.)
genehmigte Dissertation
von

Dipl.-Math. Birgit Reinert

Datum der wissenschaftlichen Aussprache: 14. Juni 1995

Dekan: Prof. Dr. Hans Hagen

Promotionskommission:

Vorsitzender: Prof. Dr. Theo Härder
Berichterstatter: Prof. Dr. Klaus E. Madlener
Prof. Dr. Volker Weispfenning

D 386

Zusammenfassung

Gröbnerbasen, entwickelt von Bruno Buchberger für kommutative Polynomringe, finden häufig Anwendung bei der Lösung algorithmischer Probleme. Beispielsweise läßt sich das Kongruenzproblem für Ideale mit Hilfe der Gröbnerbasen lösen. Bis heute wurden diese Ideen auf verschiedene zum Teil nichtkommutative und nichtnoethersche Algebren übertragen. Die meisten dieser Ansätze setzen eine zulässige Ordnung auf den Termen voraus.

In dieser Dissertation wird das Konzept der Gröbnerbasen für endlich erzeugte Monoid- und Gruppenringe verallgemeinert. Dabei werden Reduktionsmethoden sowohl zur Darstellung der Monoid- beziehungsweise Gruppenelemente, als auch zur Beschreibung der Rechtsidealkongruenz in den entsprechenden Monoid- beziehungsweise Gruppenringen benutzt. Da im allgemeinen Monoide und insbesondere Gruppen keine zulässigen Ordnungen mehr erlauben, treten bei der Definition einer geeigneten Reduktionsrelation wesentliche Probleme auf: Zum einen ist es schwierig, die Terminierung einer Reduktionsrelation zu garantieren, zum anderen sind Reduktionsschritte nicht mehr mit Multiplikationen verträglich und daher beschreiben Reduktionen nicht mehr unbedingt eine Rechtsidealkongruenz. In dieser Arbeit werden verschiedene Möglichkeiten Reduktionsrelationen zu definieren aufgezeigt und im Hinblick auf die beschriebenen Probleme untersucht. Dabei wird das Konzept der Saturierung, d.h. eine Polynommenge so zu erweitern, daß man die von ihr erzeugte Rechtsidealkongruenz durch Reduktion erfassen kann, benutzt, um Charakterisierungen von Gröbnerbasen bezüglich der verschiedenen Reduktionen durch s-Polynome zu geben. Mithilfe dieser Konzepte ist es gelungen für spezielle Klassen von Monoiden, wie z.B. endliche, kommutative oder freie, und verschiedene Klassen von Gruppen, wie z.B. endliche, freie, plain, kontext-freie oder nilpotente, unter Ausnutzung struktureller Eigenschaften spezielle Reduktionsrelationen zu definieren und terminierende Algorithmen zur Berechnung von Gröbnerbasen bezüglich dieser Reduktionsrelationen zu entwickeln.

Vorwort

Mein Dank gilt allen, die auf vielfältige Weise zum Gelingen meiner Promotion beigetragen haben.

Professor Madlener hat mir die Gelegenheit zur Erstellung dieser Arbeit gegeben. Ich danke ihm für alles, was ich fachlich und menschlich durch ihn lernen durfte. Professor Weispfenning danke ich für die Übernahme der Zweitbegutachtung meiner Arbeit. Professor Härder hat freundlicherweise die Leitung der Promotionskommission übernommen.

Mein Dank gilt auch den Mitgliedern der Arbeitsgruppen von Professor Madlener und Professor Avenhaus, sowie Frau Rita Kohl, die das Entstehen meiner Arbeit mit Anteilnahme mitverfolgt und unterstützt haben. Insbesondere Andrea Sattler-Klein, Inger Sonntag, Thomas Deiß, Roland Fettig und Claus-Peter Wirth waren immer für mich da und haben mir stets geduldig zugehört.

Meinen Freunden und Verwandten danke ich für die Ermunterungen und Gebete. Gewidmet ist diese Arbeit meinen Eltern und Joachim. Ihre Liebe hat mir geholfen, den Blick für das Wesentliche nicht zu verlieren.

Nada te turbe,
nada te espante,
todo se pasa.

Dios no se muda.
La paciencia
todo lo alcanza.

Quien a Dios tiene,
nada le falta:
sólo Dios basta.

Teresa de Jesús

Für meine Eltern
und Joachim

Contents

Chapter 1

Introduction

Was wir sind, ist nichts,
was wir suchen, ist alles.

LESSING

One of the amazing features of computers is the ability to discover new mathematical results due to extensive computations impossible to be done by hand. Besides incredible numerical calculations, symbolical mathematical manipulations are substantial to many fields in mathematics and physics. Hence the idea of using a computer to do such manipulations led to open up whole new areas of mathematics and computer science. In the wake of these developments has come a new access to abstract algebra in a computational fashion - computer algebra. One important contribution is Buchberger's algorithm for manipulating systems of polynomial equations. In 1965 Buchberger introduced the theory of Gröbner bases for polynomial ideals in commutative polynomial rings over fields (see [Bu65]). It established a rewriting approach to the theory of polynomial ideals. Polynomials can be used as rules by giving an admissible[1] ordering on the terms and using the largest monomial according to this ordering as a left hand side of a rule. "Reduction" as defined by Buchberger then can be compared to division of one polynomial by a set of finitely many polynomials. A Gröbner basis G is a set of polynomials such that every polynomial in the polynomial ring has a unique normal form with respect to reduction using the polynomials in G as rules (especially the polynomials in the ideal generated by G reduce to zero using G). Buchberger developed a terminating procedure to transform a finite generating set of a polynomial ideal into a finite Gröbner basis of the same ideal.

The method of Gröbner bases allows to solve many problems related to polynomial ideals in a computational fashion. It was shown by Hilbert (compare Hilbert's basis theorem) that every ideal in a polynomial ring has a finite generating set. However,

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

an arbitrary finite generating set need not provide much insight into the nature of the ideal. Let $f_1 = X_1^2 + X_2$ and $f_2 = X_1^2 + X_3$ be two polynomials in the polynomial ring $\mathbf{Q}[X_1, X_2, X_3]$. Then $\mathfrak{i} = \{f_1 * g_1 + f_2 * g_2 | g_1, g_2 \in \mathbf{Q}[X_1, X_2, X_3]\}$ is the ideal they generate and it is not hard to see that the polynomial $X_2 - X_3$ belongs to $\mathfrak{i}$ since $X_2 - X_3 = f_1 - f_2$. But what can be said about the polynomial $f = X_3^3 + X_1 + X_3$? Does it belong to $\mathfrak{i}$ or not?
The problem to decide whether a given polynomial lies in a given ideal is called the membership problem for ideals. In case the generating set is a Gröbner basis this problem becomes immediately solvable, as the membership problem then reduces to checking whether the polynomial reduces to zero.
In our example the set $\{X_1^2 + X_3, X_2 - X_3\}$ is a generating set of $\mathfrak{i}$ which is in fact a Gröbner basis. Now returning to the polynomial $f = X_3^3 + X_1 + X_3$ we find that it cannot belong to $\mathfrak{i}$ since neither X_1^2 nor X_2 is a divisor of a term in f and hence f cannot be reduced to zero by the polynomials in the Gröbner basis.
Further applications of Gröbner bases to algebraic questions can be found e.g. in the work of Buchberger [Bu87], Becker and Weispfenning [BeWe92] and in the book of Cox, Little and O'Shea [CoLiOS92].

Since the theory of Gröbner bases turned out to be of outstanding importance for polynomial rings, several generalizations of Buchberger's ideas to other structures followed. We only want to give a brief outline of some of them, mainly of those which influenced our work.

A first generalization was given by Buchberger himself and his student Stifter in characterizing reduction rings by adding additional axioms to the ring axioms ([St85, St87]). Further characterizations of such reduction rings were provided by Kapur and Narendran ([KaNa85]) and Madlener ([Ma86]).

Besides these theoretical studies of reduction rings, the Gröbner basis theory has been extended to commutative polynomial rings over coefficient domains other than fields. It was shown by authors as Buchberger, Kandri-Rody, Kapur, Narendran, Lauer, Stifter and Weispfenning that Buchberger's approach remains valid for polynomial rings over the integers, or even Euclidean rings, and over regular rings and reduction rings (see e.g. [Bu83, Bu85, KaKa84, KaKa88, KaNa85, La76, St85, We87]).

Since the development of computer algebra systems for commutative algebras enabled to perform tedious calculations using computers, attempts to generalize such systems and especially Buchberger's ideas to non-commutative algebras followed. Originating from special problems in physics, Lassner in [La85] suggested how to extend existing computer algebra systems in order to handle special classes of non-commutative algebras, e.g. Weyl algebras. He studied structures where the elements could be represented using the usual representation of polynomials in commutative variables and the non-commutative multiplication could be performed by a so-called "twisted product" which required only procedures involving commutative algebra operations and differentiation. His extensions could be incorporated into computer algebra systems to solve tasks of interest to physicists. Later on together with Apel he extended Buchberger's algorithm to enveloping fields of Lie algebras (see [ApLa88]). Because these ideas use representations by commutative polynomials, Dickson's lemma can be carried over.

The existence and construction of Gröbner bases for finitely generated left ideals is ensured. On the other hand, Mora gave a concept of Gröbner bases for a class of non-commutative algebras by saving an other property of the polynomial ring while losing the validity of Dickson's lemma. The usual polynomial ring can be viewed as a monoid ring where the monoid is a finitely generated free commutative monoid. Mora studied the class where the free commutative monoid is substituted by a free monoid - the class of finitely generated free monoid rings (compare e.g. [Mo85, Mo94]). The ring operations are mainly performed in the coefficient domain while the terms are treated like words, i.e., the variables no longer commute with each other. The definitions of (one- and two-sided) ideals, reduction and Gröbner bases are carried over from the commutative case to establish a similar theory of Gröbner bases in "free non-commutative polynomial rings over fields". But these rings are no longer Noetherian if they are generated by more than one variable. Moreover, the word problem for semi-Thue systems can be reduced to the membership problem for two-sided ideals. Mora presented a terminating completion procedure for finitely generated one-sided ideals and an enumeration procedure for finitely generated two-sided ideals with respect to some term ordering in free monoid rings.

Another class of non-commutative rings where the elements can be represented by the usual polynomials and which allow the construction of finite Gröbner bases for arbitrary ideals are the so-called solvable rings, a class intermediate between commutative and general non-commutative polynomial rings. They were studied by Kandri-Rody, Weispfenning and Kredel ([KaWe90, Kr93]). Solvable polynomial rings can be described by ordinary polynomial rings $\mathbf{K}[X_1, \ldots, X_n]$ provided with a "new" definition of multiplication which coincides with the ordinary multiplication except for the case that a variable X_j is multiplied with a variable X_i with lower index, i.e., $i < j$. In the latter case multiplication can be defined by equations

$$X_j \star X_i = c_{ij} X_i X_j + p_{ij}$$

where $c_{ij} \in \mathbf{K}^* = \mathbf{K} \backslash \{0\}$ and p_{ij} is a polynomial "smaller" than $X_i X_j$ with respect to a fixed admissible term ordering on the polynomial ring.

In [We92] Weispfenning showed the existence of finite Gröbner bases for arbitrary finitely generated ideals in non-Noetherian skew polynomial rings over two variables X, Y where a "new" multiplication $\star$ is introduced such that $X \star Y = XY$ and $Y \star X = X^e Y$ for some fixed $e \in \mathbf{N}^+$.

Most of the approaches mentioned so far fulfill the following requirements:

- The rings allow admissible well-founded orderings.
- If a polynomial can be reduced to zero by a set of polynomials, so can a multiple of this polynomial by a monomial.
- The translation lemma holds, i.e., if the difference of two polynomials can be reduced to zero using a set of polynomials, then the two polynomials are joinable using the same set of polynomials for reduction.

- Two polynomials give rise to finitely many s-polynomials only, in general at most one.

These statements can be used to characterize Gröbner bases in the respective ring with respect to the corresponding reduction in a finitary manner and it is decidable whether a finite set is a Gröbner basis by checking whether the s-polynomials are reducible to zero[2].

There are rings combined with reduction where these statements cannot be accomplished and therefore other concepts to characterize Gröbner bases have been developed. For example in case the ring contains zero-divisors a well-founded ordering on the ring is no longer compatible with the ring multiplication[3]. This phenomenon has been studied for the case of zero-divisors in the coefficient domain by Kapur and Madlener ([KaMa86]) and by Weispfenning for the special case of regular rings ([We87]). In his PhD thesis [Kr93], Kredel mentioned that in dropping the axioms guaranteeing the existence of admissible orderings in the theory of solvable polynomial rings by allowing $c_{ij} = 0$ in the defining equations above, the properties mentioned above need no longer hold. He sketched the idea of using saturation to repair some of the problems occurring and for special cases, e.g. for the Grassmann (exterior) algebras, positive results can be achieved (compare the paper of Stokes [St90]).

Starting point of the current work was the idea to study arbitrary finitely generated monoid rings similar to Mora's approach to free monoid rings. Since we want to treat rings with well-founded but no longer admissible orderings, we mainly have to deal with the fact that many of the properties used to give a characterization of a Gröbner basis as in the classical case no longer hold. We show that there are weaker requirements that still enable characterizations of Gröbner bases in terms of s-polynomials in case we use appropriate reductions combined with appropriate concepts of saturation. For special reductions we can even give a characterization where localization of critical situations to one s-polynomial for each pair of polynomials is possible.

Our approach can be characterized by the following tasks:

- Combine string rewriting and polynomial rewriting in the field of monoid rings.
- Generalize the concept of Gröbner bases to arbitrary monoid rings.
- Find classes of monoids and groups that allow the construction of finite Gröbner bases for finitely generated one- or even two-sided ideals.

The thesis organizes as follows:

Chapter 2 introduces some of the basic themes of this work. We need some definitions and notions from algebra and the theory of rewriting systems. Furthermore, as this work is based on Buchberger's ideas, a short summary of the theory of Gröbner bases and Buchberger's algorithm are given.

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

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

Chapter 3 gives a short outline on introducing Gröbner bases to non-commutative structures by sketching Mora's approach to free monoid rings and Weispfenning's approach to skew polynomial rings. We prove that the word problem for semi-Thue systems is equivalent to a restricted version of the membership problem for free monoid rings and similarly that the word problem for group presentations is equivalent to a restricted version of the membership problem for free group rings. Hence for free monoids respectively free groups with more than one generator the ideal membership problem is undecidable. (It is decidable for one generator.) Further we show that it is undecidable whether a finite Gröbner basis in a free monoid ring generated by more than one generator exists.

Chapter 4 gives different approaches to define reduction in monoid rings. Since monoid rings in general are not commutative, we are mainly interested in right ideals. A well-founded ordering on terms is used to split a polynomial into a head monomial (the largest monomial) and a reduct. A natural way to define reduction is to use a multiple of a polynomial to replace a monomial in another polynomial in case the result is smaller. This is the case if the head term of the multiple equals the term of the removed monomial. This reduction is called strong reduction and can be used to express the congruence of a right ideal. Although a characterization of Gröbner bases with respect to this reduction in terms of strong s-polynomials is possible, this characterization is not finitary and it cannot be used to decide whether a finite set of polynomials is a strong Gröbner basis. One idea to localize a confluence test, i.e., reduce the number of s-polynomials to be considered, is to weaken reduction. The first weakening studied is restricting the multiples of polynomials used to stable ones, i.e., multiples where the new head term results from the original head term of the polynomial. The first problem is that the expressiveness of a right ideal congruence by reduction using an arbitrary set of generators of the right ideal is lost. This can be regained using a concept called saturation (e.g. mentioned in [Kr93]), which enlarges the set of polynomials used for reduction. But such saturating sets need not be finite. For saturated sets a characterization of Gröbner bases with respect to right reduction in terms of right s-polynomials is provided which is still not finitary. Therefore, two weakenings involving syntactical information on the representatives of the monoid elements (the terms) are given – prefix reduction for arbitrary monoid rings and commutative reduction for Abelian monoid rings. Saturation concepts with respect to these reductions are provided and for saturated sets now a finitary characterization of the respective Gröbner bases in terms of special s-polynomials is possible. The characterization of prefix Gröbner bases can be used to give an enumerating procedure for such a basis which terminates in case a finite prefix Gröbner basis exists. For Abelian monoid rings a terminating procedure to complete a finite set of polynomials is provided. Furthermore, we introduce interreduction to both approaches and the existence of unique monic reduced Gröbner bases with respect to the respective ordering on the monoid is shown.

In chapter 5 we show that the subgroup problem for a group is equivalent to a restricted version of the right ideal membership problem in the corresponding group ring. Hence, only groups with solvable subgroup problem can be expected to allow the construction of finite Gröbner bases. We apply the concept of prefix reduction to the classes of free, plain respectively context-free groups and give algorithms to compute finite reduced prefix Gröbner bases for finitely generated right ideals. Furthermore, a generalization of commutative reduction to nilpotent groups, namely quasi-commutative reduction, is given and a finitary characterization of Gröbner bases in this setting is provided. A procedure to compute finite Gröbner bases with respect to this reduction for finitely generated right ideals is given.

Chapter 6 gives a sketch how the ideas of chapter 4 can be carried over to monoid rings over reduction rings.

We close this introduction by giving a brief overview on the main results of this thesis: String rewriting and polynomial rewriting have been combined to transfer Buchberger's ideas to monoid rings. Different definitions of reduction have been studied and Gröbner bases have been defined in the respective settings. The existence of finite Gröbner bases for finitely generated right ideals has been ensured and procedures for finding them have been given for the following classes: the class of finite monoids, the class of free monoids, the class of Abelian[4] monoids, the class of finite groups, the class of free groups, the class of plain groups, the class of context-free groups, and the class of nilpotent groups[4].

[4]Here we can successfully treat the case of ideals.

Chapter 2

Basic Definitions

Content, if hence th' unlearn'd their wants may view
The learn'd reflect on what before they knew

POPE

The main task of this thesis is to combine string rewriting and polynomial rewriting in the field of monoid rings. In this chapter we hence embark on the basic notions and ideas combined in our approach to generalize Buchberger's ideas to the more general setting of monoid rings.

Section 2.1: Some of the important algebraic systems – monoids, groups, rings and fields – are introduced and studied. Further the main objects of this thesis, ideals in monoid and group rings are specified.

Section 2.2: Rewriting is a technique that can be used as means of presenting structures as well as for reasoning in structures. This will be the foundation for both, representing our monoids and the right ideal congruence in our rings later on. Hence we introduce an abstract concept of rewriting including normalforms, confluence, termination, completion and the ideas related to these terms.

Section 2.3: Buchberger introduced the ideas of rewriting to commutative polynomial rings. We sketch how a polynomial can be used as a rule and how reduction using a set of polynomials describes the congruence of the ideal generated by the polynomials. Critical pairs of Buchberger's reduction can be localized to a special overlap of the head terms of the two polynomials involved, namely the least common multiple of the terms. This leads to the definition of s-polynomials and Gröbner bases can be characterized as sets of polynomials where all s-polynomials related to pairs of the polynomials in the set can be reduced to zero. This characterization provides a test whether a finite set is a Gröbner basis which can be used to give a terminating completion procedure called Buchberger's algorithm.

Section 2.4: A means of presenting monoids and groups are semi-Thue systems and semi-Thue systems modulo commutativity. We give definitions of such systems and distinguish finite complete systems for presenting special classes of monoids and groups, namely the classes of finite, free or Abelian monoids and the classes of finite, free, plain, context-free, Abelian or nilpotent groups. In using complete presentations, the elements of the respective structures have unique representatives and computation in the monoid is possible. The equivalence between the irreducible elements of the presenting system and the presented structure will be even more important for the definition of the ordering of the monoid, which will be assumed to be induced by the completion ordering of the presentation. This leads to syntactical weakenings of reduction in special monoid rings that will be studied in chapter 4.

For more information on algebra and group theory the reader is e.g. referred to the books of Herstein [He64] or Kargapolov and Merzljakov [KaMe79]. A detailed description on the subject of Gröbner bases can be found for example in the books of Becker and Weispfenning [BeWe92] and Geddes, Czapor and Labahn [GeCzLa92]. A good source on rewriting and monoid presentations is the work of Book and Otto in [BoOt93].

2.1 Algebra

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

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

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

For simplicity of notation we will henceforth drop the index $\mathcal{M}$ and write $\circ$ respectively $=$ if no confusion is likely to arise. Furthermore, we will often talk about a monoid without mentioning its binary operation explicitly. The monoid operation will often be called multiplication or addition. Since the algebraic operation is associative we can omit brackets, hence the product $a_1 \circ \ldots \circ a_n$ is uniquely defined. The product of $n \in \mathbf{N}$[1] times the same element a is called the **n-th power of** a and will be denoted by a^n, where $a^0 = \lambda$.

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

Definition 2.1.2
An element a of a monoid $\mathcal{M}$ is said to have **infinite order** in case for all $n, m \in \mathbf{N}$, $a^n = a^m$ implies $n = m$. We say that a has **finite order** in case the set $\{a^n \mid n \in \mathbf{N}^+\}$ is finite and the cardinality of this set is then called the order of a. $\diamond$

Definition 2.1.3
For a subset S of a monoid $\mathcal{M}$ we call

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

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

A monoid $\mathcal{M}$ is called **commutative (Abelian)** if we have $a \circ b = b \circ a$ for all elements a, b in $\mathcal{M}$. A natural example for a commutative monoid are the integers together with multiplication or addition.

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

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

Definition 2.1.4
A monoid $\mathcal{M}$ together with its binary operation $\circ$ is said to form a **group** if additionally

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

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

For n-th powers in groups we can set $(\mathsf{inv}(a))^n = \mathsf{inv}(a^n)$. If for a non-identity element $a \in \mathcal{G}$ there exists an element $n \in \mathbf{N}$ such that $a^n = 1$ we call the smallest such number the **order** of the element a in the group $\mathcal{G}$. Otherwise the order of a is said to be infinite. A group will be called **torsion-free** if every non-identity element of $\mathcal{G}$ has infinite order.

Definition 2.1.5
A subset $\mathcal{H}$ of a group $\mathcal{G}$ is called a **subgroup** of $\mathcal{G}$ if $\mathcal{H}$ itself forms a group with respect to the binary operation on $\mathcal{G}$. The operation on $\mathcal{H}$ is then said to be **induced** by the operation on $\mathcal{G}$. We will write $\mathcal{H} \leq \mathcal{G}$ and in case $\mathcal{H}$ is a proper subset $\mathcal{H} < \mathcal{G}$. $\diamond$

Since intersections of subgroups are again subgroups, we can define a group in terms of generators as follows: Given an arbitrary subset $S \subseteq \mathcal{G}$ we define $\langle S \rangle$ to be the intersection of all subgroups of $\mathcal{G}$ containing S. Then $\langle S \rangle$ is a subgroup of $\mathcal{G}$ and S is called a **generating set** for $\langle S \rangle$. In case a group can be generated by some finite subset we call it **finitely generated**. For example, a cyclic group can be finitely generated by one element. The following theorem gives a constructive description of this generating process.

Theorem 2.1.6
If S is a subset of a group $\mathcal{G}$ then

$$\langle S \rangle = \{s_1 \circ \ldots \circ s_n \mid n \in \mathbf{N}, s_i \in S \cup \{\mathsf{inv}(s) | s \in S\}\}.$$

$\square$

Given a subgroup $\mathcal{H}$ of a group $\mathcal{G}$, for each element g in $\mathcal{G}$ we can define special subsets of $\mathcal{G}$, the **left coset** $g\mathcal{H} = \{g \circ h \mid h \in \mathcal{H}\}$ and the **right coset** $\mathcal{H}g = \{h \circ g \mid h \in \mathcal{H}\}$. Note that for two elements g_1, g_2 in $\mathcal{G}$ we have $g_1\mathcal{H} = g_2\mathcal{H}$ if and only if $\mathsf{inv}(g_1) \circ g_2 \in \mathcal{H}$ respectively $\mathcal{H}g_1 = \mathcal{H}g_2$ if and only if $g_1 \circ \mathsf{inv}(g_2) \in \mathcal{H}$. Thus a subgroup $\mathcal{H}$ defines a left respectively right congruence by setting $g_1 \sim^l_{\mathcal{H}} g_2$ if and only if $\mathsf{inv}(g_1) \circ g_2 \in \mathcal{H}$, respectively $g_1 \sim^r_{\mathcal{H}} g_2$ if and only if $g_1 \circ \mathsf{inv}(g_2) \in \mathcal{H}$. It can be shown that the sets of all left respectively right cosets are isomorphic. Their cardinality is called the **index** of $\mathcal{H}$ in $\mathcal{G}$, denoted by $|\mathcal{G} : \mathcal{H}|$.

In group theory a particularly important role is played by a special kind of subgroup.

Definition 2.1.7
A subgroup $\mathcal{N}$ of a group $\mathcal{G}$ is called **normal** if for each g in $\mathcal{G}$, we have $g\mathcal{N} = \mathcal{N}g$. We denote this by $\mathcal{N} \trianglelefteq \mathcal{G}$ or $\mathcal{N} \triangleleft \mathcal{G}$ in case $\mathcal{N}$ is a proper subgroup. $\diamond$

We call two elements g, h of a group **conjugate** if there exists an element a in the same group such that $g = \mathsf{inv}(a) \circ h \circ a$ which is sometimes abbreviated by $g = h^a$. Obviously, $\mathcal{N} \trianglelefteq \mathcal{G}$ implies that for every $g \in \mathcal{G}$ and $h \in \mathcal{N}$, $\mathsf{inv}(g) \circ h \circ g \in \mathcal{N}$. Of course every group contains $\{\lambda\}$ and itself as trivial normal subgroups. A group containing only these normal subgroups is called **simple**. For example finite cyclic groups of prime order are simple.

The importance of normal subgroups in group theory stems from the fact that they can be used in various ways to built new groups.

Theorem 2.1.8
The **quotient** *or* **factor group** *of two groups $\mathcal{G}$ and $\mathcal{N}$, where $\mathcal{N}$ is a normal subgroup of $\mathcal{G}$, is defined by*

$$\mathcal{G}/\mathcal{N} = \{g\mathcal{N} \mid g \in \mathcal{G}\}$$

with multiplication

$$g\mathcal{N} \circ_{\mathcal{G}/\mathcal{N}} h\mathcal{N} = (g \circ_{\mathcal{G}} h)\mathcal{N}.$$

□

Moreover, this theorem is closely related to a group construction method as $\mathcal{G}$ can be seen as an extension of its normal subgroup $\mathcal{N}$.

Definition 2.1.9
A group $\mathcal{G}$ is said to be an **extension** of a group $\mathcal{N}$ by a group $\mathcal{H}$ if

1. $\mathcal{N} \lhd \mathcal{G}$ and
2. $\mathcal{G}/\mathcal{N} \cong \mathcal{H}$. ◇

Thus for two groups $\mathcal{N} \lhd \mathcal{G}$ as described in theorem 2.1.8, $\mathcal{G}$ is an extension of $\mathcal{N}$ by the quotient $\mathcal{G}/\mathcal{N}$. Of course such extensions need not be unique: $\mathbf{Z}_4$ (which is isomorphic to the structure $\{0,1,2,3\}$ with addition modulo 4) as well as the direct product $\mathbf{Z}_2 \times \mathbf{Z}_2$ (which is isomorphic to the structure $\{(0,0),(0,1),(1,0),(1,1)\}$ with component wise addition modulo 2) are both extensions of $\mathbf{Z}_2$ by $\mathbf{Z}_2$ but not isomorphic. The next definition gives a characterization of groups that are finite extensions of free groups[2].

Definition 2.1.10
A finitely generated group $\mathcal{G}$ is called **context-free** if it contains a free normal subgroup of finite index. ◇

Another familiar means to construct new groups are products and we will give two such constructions that will be of use later on.

Theorem 2.1.11
The **direct** *or* **Cartesian product** *of two groups $\mathcal{G}$ and $\mathcal{H}$ defined by*

$$\mathcal{G} \times \mathcal{H} = \{(g,h) \mid g \in \mathcal{G}, h \in \mathcal{H}\}$$

with component wise multiplication

$$(g,h) \circ_{\mathcal{G}\times\mathcal{H}} (g',h') = (g \circ_{\mathcal{G}} g', h \circ_{\mathcal{H}} h')$$

is a group. □

[2] A free group in this context is a group where no additional algebraic laws hold except the group axioms. A more specific definition will be given later on.

It can be shown that the direct product is the unique answer to the following question: Given two groups $\mathcal{G}$ and $\mathcal{H}$, does there exist a group $\mathcal{N}$ and homomorphisms $\phi_1 : \mathcal{N} \longrightarrow \mathcal{G}$, $\phi_2 : \mathcal{N} \longrightarrow \mathcal{H}$ such that for any group $\mathcal{M}$ and any homomorphisms $\psi_1 : \mathcal{M} \longrightarrow \mathcal{G}$, $\psi_2 : \mathcal{M} \longrightarrow \mathcal{H}$, there is a unique homomorphism $\theta : \mathcal{M} \longrightarrow \mathcal{N}$ such that $\theta \circ \phi_1 = \psi_1$ and $\theta \circ \phi_2 = \psi_2$? This corresponds to the following diagram:

$$\begin{tikzcd}
 & \mathcal{G} \\
\mathcal{M} \arrow[ur, "\psi_1"'] \arrow[r, "\theta"'] \arrow[dr, "\psi_2"'] & \mathcal{N} \arrow[u, "\phi_1"'] \arrow[d, "\phi_2"] \\
 & \mathcal{H}
\end{tikzcd}$$

The answer to the dual question as illustrated in the next diagram is again a unique group called the **free product** of $\mathcal{G}$ and $\mathcal{H}$.

$$\begin{tikzcd}
\mathcal{G} \arrow[d, "\phi_1"] \arrow[dr, "\psi_1"] & \\
\mathcal{N} \arrow[r, "\theta"'] & \mathcal{M} \\
\mathcal{H} \arrow[u, "\phi_2"'] \arrow[ur, "\psi_2"'] &
\end{tikzcd}$$

A very simple type of groups can be built using free products.

Definition 2.1.12
A **plain group** is a free product of finitely many finite and free groups. $\diamond$

One way to learn something about a group is to study subgroups it can be built from. This can sometimes be done by looking at special chains of subgroups of the group. Every subgroup $\mathcal{H}$ of a group $\mathcal{G}$ determines a chain $\{\lambda\} \leq \mathcal{H} \leq \mathcal{G}$. A finite chain

$$\{\lambda\} = \mathcal{G}_0 \leq \ldots \leq \mathcal{G}_k = \mathcal{G}$$

is called a **normal series of length** k for the group $\mathcal{G}$ if for each $1 \leq i \leq k-1$ we have $\mathcal{G}_i \trianglelefteq \mathcal{G}$. In case we only require $\mathcal{G}_i \trianglelefteq \mathcal{G}_{i+1}$ for all $1 \leq i \leq k-1$ such a chain is called a **subnormal series** of the group $\mathcal{G}$. The factor groups $\mathcal{G}_{i+1}/\mathcal{G}_i$ of such a subnormal series are called **factors**. A subnormal series is called **polycyclic** if all factors are cyclic and a group possessing a polycyclic subnormal series is called **polycyclic**. A group is called **polycyclic-by-finite** if it has a polycyclic normal subgroup $\mathcal{N}$ of finite index.

In order to characterize an interesting subclass of the polycyclic groups we need some more definitions. The following facts are taken from [Ha59] and [KaMe79].

The **center** of a group $\mathcal{G}$ is defined as $\mathcal{C}(\mathcal{G}) = \{g \in \mathcal{G} \mid h \circ g = g \circ h \text{ for all } h \in \mathcal{G}\}$ and is a characteristic Abelian subgroup of $\mathcal{G}$. For two elements g, h of a group their **commutator** is defined as $[g, h] = \mathsf{inv}(g) \circ \mathsf{inv}(h) \circ g \circ h$. The **commutator** of two subsets S_1, S_2 of a group $\mathcal{G}$ is denoted by $[S_1, S_2] = \{[g, h] \mid g \in S_1, h \in S_2\}$. The special commutator $[\mathcal{G}, \mathcal{G}] = \{[g, h] \mid g, h \in \mathcal{G}\}$ is a subgroup of $\mathcal{G}$ called the **derived group** of $\mathcal{G}$. A normal series of a group $\mathcal{G}$

$$\{\lambda\} = \mathcal{G}_0 \leq \ldots \leq \mathcal{G}_k = \mathcal{G}$$

is called **central** if all of its factors are **central**, i.e., if

$$\mathcal{G}_{i+1}/\mathcal{G}_i \leq \mathcal{C}(\mathcal{G}/\mathcal{G}_i) \text{ for all } 1 \leq i \leq k-1$$

or equivalently

$$[\mathcal{G}_{i+1}, \mathcal{G}] \leq \mathcal{G}_i \text{ for all } 1 \leq i \leq k-1.$$

A group having a (finite) central series is called **nilpotent**. The length of the shortest of all such series for a group is called its **nilpotency class**. Note that the Abelian groups are exactly the nilpotent groups of class less or equal to 1. We get the following classification of polycyclic groups by nilpotent groups.

Theorem 2.1.13
Every polycyclic group $\mathcal{G}$ has a normal subgroup $\mathcal{H}$ of finite index such that $\mathcal{H}$ is nilpotent-by-Abelian, i.e., $\mathcal{H}$ has a normal subgroup $\mathcal{N}$ such that $\mathcal{N}$ is nilpotent and $\mathcal{H}/\mathcal{N}$ is Abelian. □

Given a nilpotent group $\mathcal{G}$ we can construct a special central series called the **lower central series of** $\mathcal{G}$ by setting:

$$\gamma_1(\mathcal{G}) := \mathcal{G} \text{ and } \gamma_i(\mathcal{G}) := [\gamma_{i-1}(\mathcal{G}), \mathcal{G}] \text{ for } i \geq 2.$$

This gives us a normal series $\ldots \leq \gamma_i(\mathcal{G}) \leq \ldots \leq \gamma_1(\mathcal{G}) = \mathcal{G}$. If $\gamma_c(\mathcal{G}) \neq \{\lambda\}$ and $\gamma_{c+1}(\mathcal{G}) = \{\lambda\}$ then $\mathcal{G}$ is nilpotent of class c. A group $\mathcal{G}$ then is nilpotent if $\mathcal{G} = \{\lambda\}$ or there is a $c \in \mathbf{N}$ such that $\mathcal{G}$ is nilpotent of class c.

The following theorem shows how nilpotent groups can be regarded as polycyclic groups as it establishes the existence of a subnormal series with cyclic factors.

Theorem 2.1.14
A finitely generated group $\mathcal{G}$ is nilpotent if and only if there exist $\mathcal{G}_0, \ldots, \mathcal{G}_k \leq \mathcal{G}$ and $g_1, \ldots, g_k \in \mathcal{G}$ such that the following statements hold:

1. *$\mathcal{G}_0 = \{\lambda\}$, $\mathcal{G}_k = \mathcal{G}$ and $\mathcal{G}_i \lhd \mathcal{G}_{i+1}$ for $1 \leq i \leq k-1$,*
2. *$\mathcal{G}_{i+1} = \langle \{g_i\} \cup \mathcal{G}_i \rangle$ for $1 \leq i \leq k-1$, and*

3. $\mathcal{G}_{i+1}/\mathcal{G}_i \leq \mathcal{C}(\mathcal{G}/\mathcal{G}_i)$ *for* $1 \leq i \leq k-1$. □

In case we have a finitely generated nilpotent group that is additionally torsion-free, even a central series with infinite cyclic factors exits. Moreover, arbitrary finitely generated nilpotent groups are finite extensions of torsion-free ones (compare theorem 17.2.2 in [KaMe79]).

Theorem 2.1.15
Every finitely generated nilpotent group has a normal subgroup of finite index that is torsion-free. □

This theorem also holds for finitely generated polycyclic groups.

Up to this point we have seen that besides the class of all groups there are many interesting subclasses that have become the objects of study in various theories: the class of finite groups, the class of Abelian groups, the class of context-free groups, the class of plain groups, the class of nilpotent groups, and the class of polycyclic groups. We move on now to introduce the concept of free groups. A group $\mathcal{F}$ belonging to a class of groups $\mathfrak{C}$ is called **free in the class $\mathfrak{C}$, freely generated by the set** $X = \{x_i \mid i \in I\}$, if for every group $\mathcal{G} \in \mathfrak{C}$ every mapping $\phi : X \longrightarrow \mathcal{G}$ uniquely extends to a homomorphism $\Phi : \mathcal{F} \longrightarrow \mathcal{G}$. We will write $\mathcal{F}(X)$ if we want to indicate the generating set. The cardinality of the index set $|I|$ is called the **rank** of $\mathcal{F}$ and the set X its **basis**. Notice that not all classes of groups contain free groups, e.g. the class of finite groups. To give more insight into this concept, we will inspect some classes with free groups. Let us start by showing the existence of free groups in the class of all groups. Informally, a group $\mathcal{F}$ on a set of generators X is free in the class of all groups if only the trivial relations hold among these generators, i.e., only the relations $x \circ \mathsf{inv}(x) = \lambda = \mathsf{inv}(x) \circ x$ hold for $x \in X$. More precisely we can restate the definition given above for the class of all groups as follows.

Definition 2.1.16
A group $\mathcal{F}$ is called a **free group in the class of all groups generated by a set** $X \subseteq \mathcal{F}$ provided the following holds: If ϕ is a mapping from X into an arbitrary group $\mathcal{G}$, then there exists a unique extension of ϕ to a homomorphism from $\mathcal{F}$ into $\mathcal{G}$. ◇

We will only sketch how the existence of free groups can be shown. For more details the reader is referred to [LySch77, KaMe79].

Given a set of generators X we add a "copy" X^{-1} of X containing the **formal inverses** of the generators, i.e., for each $x \in X$ there is an element $x^{-1} \in X^{-1}$. We can set $\Sigma = X \cup X^{-1}$ and call the elements of this set **letters**. A **word** w is a finite sequence of letters and the **empty word** is denoted by λ. An **elementary transformation** of a word w consists of an application of a relation $xx^{-1} = \lambda = x^{-1}x$ for $x \in X$. Now we can state that two words w_1, w_2 are equivalent, denoted by $w_1 \sim w_2$, if there is a chain of elementary transformations leading from w_1 to w_2. Let Σ^* denote the set of all words generated by the letters of Σ. Then one can show that the quotient $\mathcal{F} = \Sigma^*/\sim$ is in fact a free group in the class of all groups. This factor group will be denoted by $\mathcal{F}(X)$ and multiplication is defined by $[w_1]_\sim \circ_\mathcal{F} [w_2]_\sim = [w_1 w_2]_\sim$.

Theorem 2.1.17
All bases for a given free group have the same cardinality which is equal to the rank of the free group. □

Theorem 2.1.18
If a group is generated by a set of n elements (n finite or infinite), then it is a quotient of a free group of rank n. □

Moreover, if the group $\mathcal{G}$ is generated by a set $S = \{g_i \mid i \in I\}$ and $X = \{x_i \mid i \in I\}$ is an alphabet, then the mapping $\phi : X \longrightarrow S$ defined by $\phi(x_i) = g_i$ extends to a unique epimorphism $\Phi : \mathcal{F}(X) \longrightarrow \mathcal{G}$ and the elements of the kernel $\mathcal{R}$ of this epimorphism are called the **relators** of $\mathcal{G}$ in terms of alphabet S. If a subset R of $\mathcal{R}$ is such that the smallest normal subgroup containing R is $\mathcal{R}$ itself, then we call R a **set of defining relators** in the alphabet S. This is a way to determine a group completely (up to isomorphism). We call the pair (S, R) a **presentation** of $\mathcal{G}$. A group can have several presentations. In case there exists a presentation where the sets S and R are finite we call the group **finitely presented**. For example the finite cyclic group of order 3 can be presented by $(\{a\}, a^3 = \lambda)$ or $(\{a, b\}, a^2b^{-1} = ab = ba = \lambda)$.

Before we continue with the study of free groups in other classes of groups, we briefly introduce the concept of varieties, as it provides an elegant way of describing special classes of groups together with their free groups. Let $\{\mathrm{x}_i, \mathrm{x}_i^{-1} \mid i \in \mathbf{N}\}$ be a set of variables. A word w in those letters is called a **law** in a class $\mathfrak{C}$ of groups, if for every group $\mathcal{G} \in \mathfrak{C}$, w becomes trivial for all assignments $\{\mathrm{x}_i \mid i \in \mathbf{N}\} \longrightarrow \mathcal{G}$, i.e., if w contains the variables $\mathrm{x}_1, \ldots, \mathrm{x}_n$ we get $w(g_1, \ldots, g_n) = \lambda$ for all possible assignments of elements $g_i \in \mathcal{G}$ to the variables. Note that laws are just elements of the free group generated by the set $\{\mathrm{x}_i \mid i \in \mathbf{N}\}$. Given a set V of laws and an arbitrary group $\mathcal{G}$ (not necessarily in $\mathfrak{C}$) we can define

$$V(\mathcal{G}) = \langle v_j(g_1, \ldots, g_{n_j}) \mid v_j \in V, g_i \in \mathcal{G}, n_j \in \mathbf{N}\rangle^3$$

and $V(\mathcal{G})$ is a subgroup of $\mathcal{G}$ and in some sense $V(\mathcal{G})$ "measures" the deviation of $\mathcal{G}$ from the laws in V. For example the law $\mathrm{x}_1^{-1}\mathrm{x}_2^{-1}\mathrm{x}_1\mathrm{x}_2$ derived from the equation $\mathrm{x}_1\mathrm{x}_2 = \mathrm{x}_2\mathrm{x}_1$ specifies the class of Abelian groups. The center and the derived subgroup of a group give a "measure" for the departure from commutativity, i.e., the bigger the center and the smaller the derived subgroup, the nearer the group is to being commutative.

We proceed now to establish the existence of free groups in classes of groups that are **varieties**, i.e., can be defined by a set of laws.

Theorem 2.1.19
For a variety $\mathfrak{V}$ of groups defined by a set of laws V and for any alphabet $X = \{\mathrm{x}_i \mid i \in I\}$, define

$$\mathcal{F}_V(X) = \mathcal{F}(X)/V(\mathcal{F}(X)).$$

Then these quotient groups are free in the variety $\mathfrak{V}$. In particular, every free group in $\mathfrak{V}$ is isomorphic to some $\mathcal{F}_V(X)$. □

[3] We assume that the word v_j contains n_j variables.

Obviously, the class of all groups is a trivial variety defined by the empty set of laws and the free groups described by this theorem coincide with the free groups $\mathcal{F}$ as specified before.

Since the class of Abelian groups is a variety defined by $V = \{\mathrm{x}_1^{-1}\mathrm{x}_2^{-1}\mathrm{x}_1\mathrm{x}_2\}$ we can apply theorem 2.1.19 to characterize the free groups in this class. Let $S = \{a_1, \ldots, a_n\}$ be a finite[4] set of generators. Then the set of all ordered group words on S is a free group in the class of Abelian groups: $\mathcal{F}_V(S) \cong \{a_1^{i_1} \ldots a_n^{i_n} \mid i_j \in \mathbf{Z}\}$.

The class of nilpotent groups of class $\leq s$ can also be defined as a variety. Remember that $\mathcal{G}$ is nilpotent of class $\leq s$ if and only if $\gamma_{s+1}(\mathcal{G}) = \{\lambda\}$ in the lower central series of $\mathcal{G}$. Hence we get the commutator equation $[\mathrm{x}_1, \ldots, \mathrm{x}_{s+1}] = [\ldots[\mathrm{x}_1, \mathrm{x}_2], \ldots, \mathrm{x}_{s+1}] = \lambda$ and thus $V = \{[\mathrm{x}_1, \ldots, \mathrm{x}_{s+1}]\}$. The free groups in the class of nilpotent groups of class $\leq s$ can be specified by theorem 2.1.19 but have no such nice characterization as in the Abelian case as the quotient involves the commutator equation for all generators. Therefore, we only give an example for a free nilpotent group.

Example 2.1.20
Let $\mathcal{G}$ be the free nilpotent group of class 2 with the generators a and b. Further we set $c = [a, b]$. Then every element $g \in \mathcal{G}$ can be uniquely written as $g \equiv a^{i_1} b^{i_2} c^{i_3}$ for some $i_1, i_2, i_3 \in \mathbf{Z}$ and multiplication in $\mathcal{G}$ is given by

$$a^{i_1} b^{i_2} c^{i_3} \circ a^{j_1} b^{j_2} c^{j_3} = a^{i_1+j_1} b^{i_2+j_2} c^{i_3+j_3+i_2 \cdot j_1}.$$

$\diamond$

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

Definition 2.1.21
A nonempty set $\mathcal{R}$ is called an **(associative) ring (with unit element)** if there are two binary operations $+$ (addition) and $*$ (multiplication) such that for all a, b, c in $\mathcal{R}$

1. $\mathcal{R}$ together with $+$ is an Abelian group with zero element 0 and inverse $-a$,
2. $\mathcal{R}$ is closed under $*$, i.e., $a * b \in \mathcal{R}$,
3. $*$ is associative, i.e., $a * (b * c) = (a * b) * c$,
4. the distributive laws hold, i.e., $a*(b+c) = a*b+a*c$ and $(b+c)*a = b*a+c*a$,
5. there is an element $1 \in \mathcal{R}$ (called **unit**) such that $1 * a = a * 1 = a$. $\diamond$

A ring is called **commutative (Abelian)** if $a * b = b * a$ for all $a, b \in \mathcal{R}$. The integers together with addition and multiplication are a well-known example. A commutative ring $\mathcal{R}$ is said to contain **zero-divisors**, if there exist not necessarily different elements a, b in $\mathcal{R}$ such that $a \neq 0$ and $b \neq 0$, but $a * b = 0$.

[4]The same approach is possible for infinite generating sets.

Definition 2.1.22
A commutative ring is called a **field** if its non-zero elements form a group under multiplication. $\diamond$

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

1. U is a subgroup of $(R, +)$, i.e., for $a, b \in U$ we have $a - b \in U$, and
2. for all $a, b \in U$ we have $a * b \in U$.

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

Definition 2.1.23
A nonempty subset $\mathfrak{i}$ of a ring $\mathcal{R}$ is called a **right (left) ideal** of $\mathcal{R}$, if

1. for all $a, b \in \mathfrak{i}$ we have $a - b \in \mathfrak{i}$, and
2. for every $a \in \mathfrak{i}$ and $r \in \mathcal{R}$, the element $a * r$ (respectively $r * a$) lies in $\mathfrak{i}$.

A subset that is both, a right and a left ideal, is called a **(two-sided) ideal** of $\mathcal{R}$. $\diamond$

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

Lemma 2.1.24
Let A be a non-empty subset of $\mathcal{R}$. Then

1. $\mathsf{ideal}(A) = \{\sum_{i=1}^{n} r_i * a_i * s_i \mid a_i \in A, r_i, s_i \in \mathcal{R}, n \in \mathbf{N}\}$ *is an ideal of* $\mathcal{R}$,
2. $\mathsf{ideal}_r(A) = \{\sum_{i=1}^{n} a_i * r_i \mid a_i \in A, r_i \in \mathcal{R}, n \in \mathbf{N}\}$ *is a right ideal of* $\mathcal{R}$, *and*
3. $\mathsf{ideal}_l(A) = \{\sum_{i=1}^{n} r_i * a_i \mid a_i \in A, r_i \in \mathcal{R}, n \in \mathbf{N}\}$ *is a left ideal of* $\mathcal{R}$. $\square$

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

We move on now to combine the algebraic structures introduced so far to define the rings we are interested in, namely monoid and group rings.

Definition 2.1.25
Let $\mathbf{K}$ be a field with multiplication denoted by $\cdot$ and addition denoted by $+$ and let $\mathcal{M}$ be a monoid. Further let $\mathbf{K}[\mathcal{M}]$ denote the set of all mappings $f : \mathcal{M} \to \mathbf{K}$ where the sets $\mathsf{supp}(f) = \{m \in \mathcal{M} \mid f(m) \neq 0\}$ are finite and let $f, g \in \mathbf{K}[\mathcal{M}]$. Then the **sum** of f and g is denoted by $f +_{\mathbf{K}[\mathcal{M}]} g$, where $(f +_{\mathbf{K}[\mathcal{M}]} g)(m) = f(m) + g(m)$ and the **product** is denoted by $f *_{\mathbf{K}[\mathcal{M}]} g$, where $(f *_{\mathbf{K}[\mathcal{M}]} g)(m) = \sum_{x \circ y = m \in \mathcal{M}} f(x) \cdot g(y)$. Notice that $\mathcal{M}$ can be "embedded" into $\mathbf{K}[\mathcal{M}]$ by assigning to every $m \in \mathcal{M}$ a characteristic function $\chi_m : \mathcal{M} \longrightarrow \mathbf{K}$ with $\chi_m(m) = 1$ and $\chi_m(m') = 0$ for $m' \in \mathcal{M} \backslash \{m\}$. $\diamond$

We will henceforth drop the suffixes of $+$ and $*$ if no confusion is likely to arise. Abbreviating $f(m)$ by $\alpha_m \in \mathbf{K}$ we can express f by the more convenient concept of "polynomials", i.e., $f = \sum_{m \in \mathcal{M}} \alpha_m \cdot m$. Notice that since $\mathsf{supp}(f)$ is finite this sum again is finite. This notation now gives us a shorthand for addition and multiplication in $\mathbf{K}[\mathcal{M}]$, namely for $f = \sum_{m \in \mathcal{M}} \alpha_m \cdot m$ and $g = \sum_{m \in \mathcal{M}} \beta_m \cdot m$, we get $f + g = \sum_{m \in \mathcal{M}} (\alpha_m + \beta_m) \cdot m$ and $f * g = \sum_{m \in \mathcal{M}} \gamma_m \cdot m$ with $\gamma_m = \sum_{x \circ y = m \in \mathcal{M}} \alpha_x \cdot \beta_y$. $\mathbf{K}[\mathcal{M}]$ is indeed a ring[5] and we call $\mathbf{K}[\mathcal{M}]$ the **monoid ring** of $\mathcal{M}$ over $\mathbf{K}$, or in case $\mathcal{M}$ is a group the **group ring** or **group algebra** of $\mathcal{M}$ over $\mathbf{K}$.

Remark 2.1.26
If $\mathcal{M}$ is not cancellative $\mathbf{K}[\mathcal{M}]$ may contain zero-divisors. To see this let $\Sigma = \{a, b, c\}$ be the generators of a monoid $\mathcal{M}$ together with the relations $ab = c$ and $ac = b$. Then the elements $a^2 - 1, c \in \mathbf{Q}[\mathcal{M}]$ are non-zero, but $(a^2 - 1) * c = c - c = 0$. $\diamond$

Example 2.1.27
The polynomial ring over a field $\mathbf{K}$ in the variables $X_1, \ldots, X_n$ is a well-known ring which is also a monoid ring, namely the monoid ring of the free commutative monoid generated by $X_1, \ldots, X_n$ over $\mathbf{K}$. $\diamond$

Since our main interest will be in ideals we give a short description of their structure in $\mathbf{K}[\mathcal{M}]$ in terms of generating sets as described in lemma 2.1.24. For a non-empty set of polynomials F in $\mathbf{K}[\mathcal{M}]$ we get

$$\begin{aligned}
\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F) &= \{\textstyle\sum_{i=1}^{n} \alpha_i \cdot m_i * p_i * m_i' \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, p_i \in F, m_i, m_i' \in \mathcal{M}\}, \\
\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F) &= \{\textstyle\sum_{i=1}^{n} \alpha_i \cdot p_i * m_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, p_i \in F, m_i \in \mathcal{M}\}, \text{ and} \\
\mathsf{ideal}_l^{\mathbf{K}[\mathcal{M}]}(F) &= \{\textstyle\sum_{i=1}^{n} \alpha_i \cdot m_i * p_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, p_i \in F, m_i \in \mathcal{M}\}.
\end{aligned}$$

We will simply write $\mathsf{ideal}(F)$, $\mathsf{ideal}_r(F)$ and $\mathsf{ideal}_l(F)$ if the context is clear. Many algebraic problems for rings are related to ideals and we will close this section by stating two of them[6].

The Membership Problem

Given: A polynomial $g \in \mathbf{K}[\mathcal{M}]$ and a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$.
Question: Is g in the ideal generated by F?

Definition 2.1.28
Two elements $f, g \in \mathbf{K}[\mathcal{M}]$ are said to be **congruent modulo** $\mathsf{ideal}(F)$, denoted by $f \equiv_{\mathsf{ideal}(F)} g$, if $f = g + h$ for some $h \in \mathsf{ideal}(F)$, i.e., $f - g \in \mathsf{ideal}(F)$. $\diamond$

[5] All operations mainly involve operations on the coefficients in the field $\mathbf{K}$.

[6] For more information on such problems in the special case of commutative polynomial rings see [Bu87].

The Congruence Problem

Given: Two polynomials $f, g \in \mathbf{K}[\mathcal{M}]$ and a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$.
Question: Are f and g congruent modulo the ideal generated by F?

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

2.2 The Notion of Reduction

This section summarizes some important notations and definitions of reduction relations and basic properties related to them, as can be found more explicitly for example in the work of Huet or Book and Otto ([Hu80, Hu81, BoOt93]).

Let $\mathcal{E}$ be a set of elements and $\longrightarrow$ a binary relation on $\mathcal{E}$ called **reduction**. For $a, b \in \mathcal{E}$ we will write $a \longrightarrow b$ in case $(a, b) \in \longrightarrow$. A pair $(\mathcal{E}, \longrightarrow)$ will be called a **reduction system**. Then we can expand the binary relation as follows:

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

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

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

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

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

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

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

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

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

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

Convergent reduction systems with effective[7] reduction relations have solvable word problem, as every element has a unique normal form and two elements are equal if and only if their normal forms are equal. Of course we cannot always expect $(\mathcal{E}, \longrightarrow)$ to be convergent. Even worse, both properties are undecidable in general. Nevertheless, there are weaker conditions which guarantee convergence.

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

Before stating Newman's lemma which gives a connection between confluence and local confluence, we introduce the notion of Noetherian induction that we will use in the proof of the lemma.

Definition 2.2.6
Let $(\mathcal{E}, \longrightarrow)$ be a reduction system. A predicate $\mathcal{P}$ on $\mathcal{E}$ is called **$\longrightarrow$-complete**, in case for every $a \in \mathcal{E}$ the following implication holds: if $\mathcal{P}(b)$ is true for all proper successors of a, then $\mathcal{P}(a)$ is true. $\diamond$

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

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

Lemma 2.2.7 (Newman)
Let $(\mathcal{E}, \longrightarrow)$ be a Noetherian reduction system. Then $(\mathcal{E}, \longrightarrow)$ is confluent if and only if $(\mathcal{E}, \longrightarrow)$ is locally confluent.

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

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

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

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

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

q.e.d.

Therefore, if the reduction system is terminating, a check for confluence can be reduced to a check for local confluence. It remains to look for conditions ensuring $(\mathcal{E}, \longrightarrow)$ to be Noetherian.

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

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

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

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

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

q.e.d.

We will later on see how a reduction system with a reduction relation fulfilling the requirements of this lemma can be made convergent by introducing "completion". The partial ordering is then called the completion ordering of the reduction system.

The ideas introduced in this section will be specified to special reduction systems, namely semi-Thue systems to present monoids or groups and polynomial reduction to present the ideal respectively right ideal congruence in rings.

2.3 Gröbner Bases in Polynomial Rings

The main interest in this section is the study of ideals in polynomial rings over fields. Let $\mathbf{K}[X_1, \ldots, X_n]$ denote a polynomial ring over the (ordered) variables $X_1, \ldots, X_n$. By $\mathcal{T} = \{X_1^{i_1} \ldots X_n^{i_n} \mid i_1, \ldots i_n \in \mathbf{N}\}$ we define the set of **terms** in this structure. We recall that a subset F of $\mathbf{K}[X_1, \ldots, X_n]$ generates an ideal $\mathsf{ideal}(F) = \{\sum_{i=1}^{k} f_i * g_i \mid k \in \mathbf{N}, g_i \in \mathbf{K}[X_1, \ldots, X_n]\}$ and F is called a basis of this ideal. It was shown by Hilbert that every ideal in $\mathbf{K}[X_1, \ldots, X_n]$ in fact has a finite basis, but such a generating set need not allow algorithmic solutions for the membership or congruence problem related to the ideal. It was Buchberger who developed a special type of basis, namely the Gröbner basis, which allows algorithmic solutions for several algebraic problems concerning ideals. He introduced reduction to $\mathbf{K}[X_1, \ldots, X_n]$ by transforming polynomials into "rules" and gave a terminating procedure to "complete" an ideal basis taken as a reduction system. This procedure is called Buchberger's algorithm. We will give a sketch of his approach below.

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

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

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

Definition 2.3.2
Let $p = \sum_{i=1}^k \alpha_i \cdot t_i$ be a non-zero polynomial in $\mathbf{K}[X_1, \dots, X_n]$ such that $\alpha_i \in \mathbf{K}^* = \mathbf{K} \backslash \{0\}$, $t_i \in \mathcal{T}$ and $t_1 \succ \dots \succ t_n$. Then we let $\mathsf{HM}(p) = \alpha_1 \cdot t_1$ denote the **head monomial**, $\mathsf{HT}(p) = t_1$ the **head term** and $\mathsf{HC}(p) = \alpha_1$ the **head coefficient** of p. $\mathsf{RED}(p) = p - \mathsf{HM}(p)$ stands for the **reduct** of p. We call p **monic** in case $\mathsf{HC}(p) = 1$. $\diamond$

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

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

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

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

Definition 2.3.4
Let p, f be two polynomials in $\mathbf{K}[X_1, \dots, X_n]$. We say f **reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\mathrm{b}} q$, if

(a) $\mathsf{HT}(f) \circ u = t$ for some $u \in \mathcal{T}$[8], and

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

[8] I.e., $\mathsf{HT}(f)$ divides t.

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

Note that if f **reduces** p to q at a monomial $\alpha \cdot t$ then t is no longer among the terms of q. We call a set of polynomials $F \subseteq \mathbf{K}[X_1, \ldots, X_n]$ **interreduced**, if no $f \in F$ is reducible by a polynomial in $F \backslash \{f\}$. Notice that we have $\longrightarrow \subseteq >$ and indeed one can show that reduction on $\mathbf{K}[X_1, \ldots, X_n]$ is Noetherian. Therefore, we can restrict ourselves to ensuring local confluence when describing a completion procedure to compute Gröbner bases later on.

Definition 2.3.5
A set $G \subseteq \mathbf{K}[X_1, \ldots, X_n]$ is said to be a **Gröbner basis**, if

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

The first statement expresses that reduction describes the ideal congruence and the second one ensures the existence of unique normal forms. If we additionally require a Gröbner basis to be interreduced, such a basis is unique in case we assume that the polynomials are monic. The following lemma gives some properties of reduction, which are essential in giving a constructive description of a Gröbner basis.

Lemma 2.3.6
Let F be a set of polynomials and p, q, h some polynomials in $\mathbf{K}[X_1, \ldots, X_n]$. Then the following statements hold:

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

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

Of course we cannot expect an arbitrary ideal basis to be complete[9]. But Buchberger was able to show that in order to "complete" a given basis one only has to add finitely many special polynomials which arise from critical situations as described in the context of reduction in the previous section.

Definition 2.3.7
The **s-polynomial** for two non-zero polynomials $p, q \in \mathbf{K}[X_1, \ldots, X_n]$ is defined as

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

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

An s-polynomial will be called non-trivial in case it is not zero and notice that for non-trivial s-polynomials we always have $\mathsf{HT}(\mathsf{spol}(p,q)) \prec \mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q))$.

The following theorem now gives a constructive characterization of Gröbner bases.

Theorem 2.3.8
For a set of polynomials F in $\mathbf{K}[X_1, \ldots, X_n]$, the following statements are equivalent:

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

Proof :
$1 \Longrightarrow 2$: Let F be a Gröbner basis and $g \in \mathsf{ideal}(F)$. Then g is congruent to 0 modulo the ideal generated by F, i.e., $g \xleftrightarrow{*}{}^{\mathrm{b}}_{F} 0$. Thus, as 0 is irreducible we get $g \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$.

$2 \Longrightarrow 1$: We have to show that reduction with respect to F is confluent. Since our reduction is terminating it is sufficient to show local confluence. Thus, suppose there are three different polynomials g, h_1, h_2 such that $g \longrightarrow^{\mathrm{b}}_{F} h_1$ and $g \longrightarrow^{\mathrm{b}}_{F} h_2$. Then we know $h_1 \equiv_{\mathsf{ideal}(F)} g \equiv_{\mathsf{ideal}(F)} h_2$ and hence $h_1 - h_2 \in \mathsf{ideal}(F)$. Now by lemma 2.3.6 (the translation lemma), $h_1 - h_2 \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ implies the existence of a polynomial $h \in \mathbf{K}[X_1, \ldots, X_n]$ such that $h_1 \xrightarrow{*}{}^{\mathrm{b}}_{F} h$ and $h_2 \xrightarrow{*}{}^{\mathrm{b}}_{F} h$. Hence, h_1 and h_2 are joinable.

$2 \Longrightarrow 3$: By definition 2.3.7 the s-polynomial for two non-zero polynomials $f_k, f_l \in \mathbf{K}[X_1, \ldots, X_n]$ is defined as

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

where $\mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)) = \mathsf{HT}(p) \circ u = \mathsf{HT}(q) \circ v$ and, hence, $\mathsf{spol}(f_k, f_l) \in \mathsf{ideal}(F)$. Therefore, $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ follows immediately.

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

$3 \Longrightarrow 2$: We have to show that every $g \in \mathsf{ideal}(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{b}}_{F}$-reducible to zero. Remember that for $h \in \mathsf{ideal}(F)$, $h \longrightarrow^{\mathrm{b}}_{F} h'$ implies $h' \in \mathsf{ideal}(F)$. As $\longrightarrow^{\mathrm{b}}_{F}$ is Noetherian, thus it suffices to show that every $g \in \mathsf{ideal}(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{b}}_{F}$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be an arbitrary representation of g with $\alpha_j \in \mathbf{K}^*$, $f_j \in F$, and $w_j \in \mathcal{T}$. Depending on this representation of g and a total well-founded admissible ordering $\succeq$ on $\mathcal{T}$ we define $t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{b}}_{F}$-reducible. Thus we will prove that g has a representation where every occurring term is less or equal to $\mathsf{HT}(g)$, i.e., there exists a representation such that $t = \mathsf{HT}(g)$[10]. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[11]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[12] such that $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l = t$. By definition 2.3.7 we have an s-polynomial $\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * z_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * z_l$ such that $\mathsf{HT}(f_k) \circ z_k = \mathsf{HT}(f_l) \circ z_l = \mathsf{LCM}(\mathsf{HT}(f_k), \mathsf{HT}(f_l))$. Since $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l$ there exists an element $z \in \mathcal{T}$ such that $w_k = z_k \circ z$ and $w_l = z_l \circ z$. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume that $\mathsf{spol}(f_k, f_l)$ is not trivial[13]. Then the reduction sequence $\mathsf{spol}(f_k, f_l) \xrightarrow{*}^{\mathrm{b}}_{F} 0$ results in a representation of the form $\mathsf{spol}(f_k, f_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbf{K}^*, h_i \in F, v_i \in \mathcal{T}$. As the h_i are due to the reduction of the s-polynomial, all terms occurring in the sum are bounded by the term $\mathsf{HT}(\mathsf{spol}(f_k, f_l))$. Moreover, since $\succeq$ is admissible on $\mathcal{T}$ this implies that all terms of the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * z$ are bounded by $\mathsf{HT}(\mathsf{spol}(f_k, f_l)) \circ z \prec t$, i.e., they are strictly bounded by t[14]. We can now do the following transformations:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \; & \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \; & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}(f_k, f_l) * z} \\
= \; & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * (v_i \circ z)) \qquad (2.1)
\end{aligned}$$

where, $\beta_k = \mathsf{HC}(f_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l)^{-1}$, and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (2.1) in our

[10] Such representations are often called standard representations in literature (compare [BeWe92]).

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

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

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

[14] This can also be concluded by statement four of lemma 2.3.6 since $\mathsf{spol}(f_k, f_l) \xrightarrow{*}^{\mathrm{b}}_{F} 0$ implies $\mathsf{spol}(f_k, f_l) * z \xrightarrow{*}^{\mathrm{b}}_{F} 0$ and $\mathsf{HT}(\mathsf{spol}(f_k, f_l) * z) \prec t$.

representation of g either t disappears or K is decreased.

q.e.d.

Remark 2.3.9
A closer inspection of the proof of $3 \Longrightarrow 2$ given above reveals a concept that will be initial to the proofs of similar theorems for specific monoid rings in the following chapter. The heart of this proof consists in transforming an arbitrary representation of an element g belonging to the ideal generated by the set F in such a way that we can deduce a top reduction sequence for g to zero, i.e., a reduction sequence where the reductions only take part at the respective head term. Such a representation of g then is a standard representation and hence this technique is closely related to the concept of standard bases as given for example in [BeWe92]. $\diamond$

As a consequence of theorem 2.3.8 it is decidable whether a finite set of polynomials is a Gröbner basis. Moreover, this theorem gives rise to the following completion procedure for sets of polynomials called Buchberger's Algorithm.

Procedure: BUCHBERGER'S ALGORITHM

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

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

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

2.4 Semi-Thue Systems

In this section we introduce the structures we shall use to present our monoids and groups, namely **semi-Thue systems** (also called **string-rewriting systems**). Let us start with some basic definitions.

Definition 2.4.1
Let Σ be a finite alphabet.

1. By Σ^* we will denote the set of all **words** over the alphabet Σ where λ presents the **empty word**, i.e., the word of length zero. $\equiv$ will denote the **identity** on Σ^*.

2. Let u, v be words in Σ^*. u is said to be a **prefix** of v, if there exists $w \in \Sigma^*$ such that $v \equiv uw$. w is then called a **suffix** of v. In case $w \not\equiv \lambda$ or $u \not\equiv \lambda$ we will speak of **proper prefixes** respectively **proper suffixes**.

3. The **length** of a word is the number of letters it contains, i.e., $|\lambda| = 0$ and $|wa| = |w| + 1$ for all $w \in \Sigma^*$, $a \in \Sigma$.

4. We can define a mapping $\mathsf{conc} : \Sigma^* \times \Sigma^* \longrightarrow \Sigma^*$ by $\mathsf{conc}(u, v) \equiv uv$ for $u, v \in \Sigma^*$ which will be called **concatenation**. Then conc is an associative binary operation on Σ^* with identity λ. Thus Σ^* together with conc and λ is a monoid, namely the **free monoid generated by** Σ.

5. For an element $w \in \Sigma^*$ we define

$$\ell(w) = \begin{cases} \lambda & \text{if } w \equiv \lambda \\ a & \text{if } w \equiv ua, u \in \Sigma^*, a \in \Sigma, \end{cases}$$

i.e., $\ell(w)$ is the last letter of w in case w is not the empty word. $\diamond$

Definition 2.4.2
Let Σ be a finite alphabet.

1. A **semi-Thue system** T over Σ is a subset of $\Sigma^* \times \Sigma^*$. The elements (l, r) of T are called **rules** and will often be written as $l \longrightarrow r$.

2. The **single-step reduction relation** on Σ^* induced by a semi-Thue system T is defined as follows: For any u, v in Σ^*, $u \longrightarrow_T v$ if and only if there exist x, y in Σ^* and (l, r) in T such that $u \equiv xly$ and $v \equiv xry$. The **reduction relation** on Σ^* induced by T is the reflexive transitive closure of $\longrightarrow_T$ and is denoted by $\stackrel{*}{\longrightarrow}_T$. The reflexive transitive symmetric closure is defined as usual and denoted by $\stackrel{*}{\longleftrightarrow}_T$. ◇

Recalling section 2.2 we find that the pair $(\Sigma^*, \longrightarrow_T)$ is a reduction system which is specified by Σ and T.

Definition 2.4.3
A semi-Thue system is called **normalized** or **reduced** in case the left hand sides of the rules can only be reduced by the rule itself and the right hand sides are irreducible. ◇

Notice that one can even assume that a reduced semi-Thue system does not contain rules of the form $a \longrightarrow b$ or $a \longrightarrow \lambda$ where $a, b \in \Sigma$[15].

Definition 2.4.4
Let Σ be an alphabet. A mapping $\imath : \Sigma \longrightarrow \Sigma$ is called an **involution** if $\imath(\imath(a)) = a$ for all $a \in \Sigma$. A semi-Thue system is called a **group system** if there exists an involution $\imath$ such that for all $a \in \Sigma$ the rules $(\imath(a)a, \lambda)$ and $(a\imath(a), \lambda)$ are included in T. ◇

Note that sometimes we will assume that $\Sigma = \Gamma \cup \Gamma^{-1}$ where $\Gamma^{-1} = \{a^{-1} \mid a \in \Gamma\}$ contains the formal inverses of Γ and T contains the rules corresponding to the trivial relations in a group, namely $\{(aa^{-1}, \lambda), (a^{-1}a, \lambda) \mid a \in \Gamma\}$.

An equivalence relation on Σ^* is said to be a congruence relation in case it is admissible, i.e., compatible with concatenation. Since this is obviously true for the reduction relation induced by a semi-Thue system T, the reflexive transitive symmetric closure $\stackrel{*}{\longleftrightarrow}_T$ is a congruence relation on the set Σ^*, the **Thue congruence**. Two semi-Thue systems on the same alphabet are called **equivalent** if they generate the same Thue congruence. The congruence classes are denoted by $[w]_T = \{v \in \Sigma^* \mid v \stackrel{*}{\longleftrightarrow}_T w\}$ and we can set $\mathfrak{M}_T = \{[w]_T \mid w \in \Sigma^*\}$. In fact $\mathfrak{M}_T$ is the factor monoid of the free monoid Σ^* modulo the congruence induced by T as the following lemma establishes.

Lemma 2.4.5
Let (Σ, T) be a semi-Thue system.

1. *The set $\mathfrak{M}_T$ together with the binary operation $\circ : \mathfrak{M}_T \times \mathfrak{M}_T \longrightarrow \mathfrak{M}_T$ defined by $[u]_T \circ [v]_T = [uv]_T$ and the identity $[\lambda]_T$ is a monoid, called the* **factor!monoid** *of Σ^* and $\stackrel{*}{\longleftrightarrow}_T$.*

[15] Such rules can be removed using Tietze transformations which are a means to change presentations without changing the monoid presented.

2. *In case T is a group system, the set $\mathfrak{M}_T$ together with $\circ$, $[\lambda]_T$ and* inv *is a group, where* $\mathsf{inv}([w]_T) = [\mathrm{inv}(w)]_T$, *and* $\mathrm{inv}(\lambda) = \lambda$, $\mathrm{inv}(wa) = \imath(a)\mathrm{inv}(w)$ *for all* $w \in \Sigma^*$, $a \in \Sigma$. $\square$

Hence, semi-Thue systems are means for presenting monoids and groups. The following definitions are closely related to describing monoids and groups in terms of generators and defining relations as given in section 2.1. We call a pair (Σ, T) a **presentation** of a monoid (group) $\mathcal{M}$ if $\mathcal{M} \cong \mathfrak{M}_T$. Note that every monoid can be presented by a (even convergent) semi-Thue system. Just let Σ be the set of all elements and T the multiplication table. The problem is that this presentation in general is neither finite nor recursive. We call a monoid (group) $\mathcal{M}$ **finitely generated**, if $\mathcal{M}$ has a presentation (Σ, T) such that Σ is finite. $\mathcal{M}$ is said to be **finitely presented**, if additionally T is finite. In order to do effective computations in our monoid or group we have to be able to compute representatives for the congruence classes of the elements. A very nice solution occurs in case we are able to give a convergent finite semi-Thue system as a presentation, since then every congruence class has a unique representative and many problems, e.g. the word problem, are algorithmically solvable.

After distinguishing some syntactically restricted semi-Thue systems we will conclude this section by giving characterizations of certain classes of groups and monoids as mentioned in section 2.1 by special presentations they allow. A survey on groups allowing convergent presentations can be found in [MaOt89]

Definition 2.4.6
Let T be a semi-Thue system on Σ.

1. T is said to be **length-reducing** if for all $(l, r) \in T$, $|l| > |r|$.

2. T is said to be **monadic** if for all $(l, r) \in T$, $r \in \Sigma \cup \{\lambda\}$ and $|l| \geq |r|$.

3. T is said to be **2-monadic** if for all $(l, r) \in T$, $r \in \Sigma \cup \{\lambda\}$ and $2 \geq |l| \geq |r|$. $\diamond$

We next introduce length-lexicographical orderings which can be used for orienting these rule systems. Then obviously the reduction relation induced by them is Noetherian.

Definition 2.4.7
Let Σ be an alphabet and $\succ$ a partial ordering on Σ called precedence. Further let $u \equiv a_1 \dots a_n$ and $v \equiv b_1 \dots b_m$ be two words in Σ^*.

1. We can define a **lexicographical ordering** based on $\succ$ by setting $u >^{\mathrm{lex}} v$ if and only if there exists an index $k \in \{1, \dots, \min\{n, m\}\}$ such that $a_i = b_i$ for all $1 \leq i < k$ and $a_k \succ b_k$.

2. We can define a **length-lexicographical ordering** based on $\succ$ and $>^{\mathrm{lex}}$ by setting $u >^{\mathrm{llex}} v$ if and only if $|u| > |v|$ or ($|u| = |v|$ and $u >^{\mathrm{lex}} v$). $\diamond$

Let us continue with a property of orderings which holds e.g. for pure lexicographical and length-lexicographical orderings.

Definition 2.4.8
A partial ordering $\preceq$ on Σ^* is called **admissible** (with respect to conc) if for all u, v, x, y in Σ^* we have

1. $1 \preceq u$, and
2. $u \prec v$ implies $xuy \prec xvy$. $\diamond$

In case $\preceq$ is an admissible well-founded total ordering, then for a proper subword u of v (and hence a proper divisor in Σ^*) we have $u \prec v$. This is due to the fact that otherwise $u \succ v \equiv xuy \succ x^2uy^2 \succ \ldots$ would give us an infinite descending chain, contradicting that $\preceq$ is supposed to be well-founded on Σ^*. Therefore, in case a monoid $\mathcal{M}$ is presented by a semi-Thue system (Σ, T) which is convergent with respect to an admissible well-founded total ordering $\succeq$ this yields $uv \succeq u \circ_{\mathcal{M}} v$.

By Newman's lemma we know that under the hypothesis that a reduction relation is Noetherian, a reduction system is confluent if and only if it is locally confluent. For semi-Thue systems the global property of being locally confluent can be localized to enable a confluence test. We will now sketch how a finite presentation (Σ, T) of a monoid can be completed in case we have a total admissible well-founded ordering $\succeq$ on Σ^* such that for all $(l, r) \in T$ we have $l \succ r$. This ordering then will be called a **completion ordering** and the process of transforming (Σ, T) into a (not necessarily finite) convergent presentation of the same monoid is called **completion**. Important is that in order to check a finite set T for confluence we only have to look at a finite set of critical situations: for $(l_1, r_1), (l_2, r_2) \in T$ the set of **critical pairs** is $\{\langle xr_1, r_2y\rangle \mid \text{there are } x, y \in \Sigma^*, xl_1 \equiv l_2y, |x| < |l_2|\} \cup \{\langle r_1, xr_2y\rangle \mid \text{there are } x, y \in \Sigma^*, l_1 \equiv xl_2y, |x| < |l_1|\}$. Now given a finite semi-Thue system (Σ, T) with a completion ordering $\succeq$ we can give a completion process as follows:

Procedure: Knuth Bendix Completion

Given: $(\Sigma, T), \succeq$ as described above.

$R_0 := T$;
$i := -1$;
repeat
    $i := i + 1$;
    $R_{i+1} := \emptyset$;
    $B :=$ critical.pairs(R_i);
    % Compute the critical pairs of all $(l_1, r_1), (l_2, r_2) \in T$ as described above
    while $B \neq \emptyset$ **do**
        $\langle z_1, z_2\rangle :=$ remove(B);
        % Remove an element using a fair strategy
        $z_1' :=$ normalform(z_1, $\longrightarrow_T$);

$z_2' :=$ normalform(z_2, $\longrightarrow_T$);
case $z_1' \succ z_2'$: $R_{i+1} := R_{i+1} \cup \{(z_1', z_2')\}$;
case $z_2' \succ z_1'$: $R_{i+1} := R_{i+1} \cup \{(z_2', z_1')\}$;
endwhile
case $R_{i+1} \neq \emptyset$: $R_{i+1} := R_i \cup R_{i+1}$;
until $R_{i+1} = \emptyset$

Since the word problem for semi-Thue systems is unsolvable, this procedure in general will not terminate. Nevertheless, using a fair startegy to remove elements from the set B, it always enumerates a convergent semi-Thue system presenting the same monoid as the input system.

In the following we will study monoids where finite convergent presentations exist. Our interest will be in subclasses of the class of finitely presented monoids and groups only and the assumption of being finitely presented will often be included without being mentioned explicitly.

A very simple subclass of finitely presented monoids is the class of finite monoids. Obviously every finite monoid $\mathcal{M}$ can be presented by its elements and their multiplication table. This presentation will be denoted by $(\mathcal{M}, M_{\mathcal{M}})$ and in fact this gives us presentations for finite monoids by 2-monadic convergent semi-Thue systems. The same is true for finite groups and we even have finite 2-monadic convergent group presentations.

In case (Σ', T) is a semi-Thue system presenting a free monoid $\mathcal{M}$, then there is a subset Σ of Σ' such that $\mathcal{M}$ is freely generated by Σ, i.e., $\mathcal{M} \cong \Sigma^*$ and $(\Sigma, \emptyset)$ is also a presentation of $\mathcal{M}$ and obviously a convergent one. Of similar simplicity is the characterization of free groups in the class of finitely generated groups. Let $\mathcal{F}$ be a free group generated by $X = \{x_1, \ldots, x_n\}$. Then the semi-Thue system $(X \cup X^{-1}, I)$ where $I = \{x_i x_i^{-1} \longrightarrow \lambda, x_i^{-1} x_i \longrightarrow \lambda \mid 1 \leq i \leq n\}$ is a presentation of $\mathcal{F}$ which is 2-monadic and convergent.

Presentations for the groups in the class of plain groups can easily be constructed from finite and free presentations by using how presentations of groups can be combined in order to present free products of these groups. Let $\mathcal{G}_1, \mathcal{G}_2$ be two groups with presentations $(\Sigma_1, T_1), (\Sigma_2, T_2)$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$[16]. Then $(\Sigma_1 \cup \Sigma_2, T_1 \cup T_2)$ is a presentation of the free product $\mathcal{G}_1 * \mathcal{G}_2$. As plain groups are finite free products of finite and free groups, this process results in 2-monadic convergent presentations for plain groups. On the other hand it has been shown (compare [AvMaOt86]) that the class of plain groups is exactly the class of groups allowing finitely generated 2-monadic convergent presentations. It is obvious that the classes of finite groups and free groups are subclasses of this class.

Another combination of finite and free groups occurs in the description of context-free groups. A context-free group $\mathcal{G}$ has a free normal subgroup $\mathcal{F}$ of finite index. Let the free group $\mathcal{F}$ be generated by $X = \{x_1, \ldots, x_n\}$ and let $\mathcal{E}$ be a finite group

[16] This can always be achieved by renaming the elements of Σ_1 or Σ_2.

such that $\mathcal{E} \cong \mathcal{G}/\mathcal{F}$ and $(\mathcal{E}\backslash\{\lambda\}) \cap (X \cup X^{-1}) = \emptyset$. Then we can assume that an element $g \in \mathcal{G}$ can be presented as $g \equiv ew$ for some $e \in \mathcal{E}$, $w \in \mathcal{F}$. For all $e \in \mathcal{E}$ let $\phi_e : X \cup X^{-1} \longrightarrow \mathcal{F}$ be a function such that ϕ_λ is the inclusion and for all $x \in X \cup X^{-1}$, $\phi_e(x) = \mathsf{inv}(e) \circ_{\mathcal{G}} x \circ_{\mathcal{G}} e$, i.e., ϕ_e is a conjugation homomorphism. For all $e_1, e_2 \in \mathcal{E}$ let $z_{e_1,e_2} \in \mathcal{F}$ such that $z_{e_1,\lambda} \equiv z_{\lambda,e_1} \equiv \lambda$ and for all $e_1, e_2 \in \mathcal{E}$ with $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$, let $e_1 \circ_{\mathcal{G}} e_2 \equiv e_3 z_{e_1,e_2}$. Then we can set $\Sigma = (\mathcal{E}\backslash\{\lambda\}) \cup X \cup X^{-1}$ and let T consist of the following rules:

$$\begin{array}{lll}
xx^{-1} & \longrightarrow \lambda & \text{and} \\
x^{-1}x & \longrightarrow \lambda & \text{for all } x \in X, \\
e_1 e_2 & \longrightarrow e_3 z_{e_1,e_2} & \text{for all } e_1, e_2 \in \mathcal{E}\backslash\{\lambda\}, e_3 \in \mathcal{E} \text{ such that } e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3, \\
xe & \longrightarrow e\phi_e(x) & \text{and} \\
x^{-1}e & \longrightarrow e\phi_e(x^{-1}) & \text{for all } e \in \mathcal{E}\backslash\{\lambda\}, x \in X.
\end{array}$$

(Σ, T) is called a **virtually free presentation** and is convergent (compare [CrOt94]). In fact it can be shown that a group $\mathcal{G}$ has a virtually free presentation if and only if it is context-free.

Another class of groups allowing special presentations we want to present here are the polycyclic groups, which include the Abelian and nilpotent groups (compare [Wi89]).

Let $\Sigma = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$ be a finite alphabet and for $1 \leq k \leq n$ we define the subsets $\Sigma_k = \{a_i, a_i^{-1} \mid k \leq i \leq n\}$, $\Sigma_{n+1} = \emptyset$. We first distinguish several particular classes of rules over Σ.

Definition 2.4.9
Let $i, j \in \{1, \ldots, n\}$, $j > i$ and $\delta, \delta' \in \{1, -1\}$.

1. A rule $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta}$ is called a **CAB-rule**.
2. A rule $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta} z$, $z \in \Sigma_{j+1}^*$ is called a **CNI-rule**.
3. A rule $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} z$, $z \in \Sigma_{i+1}^*$ is called a **CP-rule**. ◇

Definition 2.4.10
For X $\in$ {AB, NI, P} a subset C of $\Sigma^* \times \Sigma^*$ is called a **commutation-system** if

1. C contains only CX-rules, and
2. for all $1 \leq i < j \leq n$ and for all $\delta, \delta' \in \{1, -1\}$ there is exactly one rule $a_j^{\delta} a_i^{\delta'} \longrightarrow r$ in C. ◇

Definition 2.4.11
For $1 \leq i \leq n$ a rule $a_i^m \longrightarrow r$ where $m \geq 1$, $r \in \Sigma_{i+1}^*$ is called a **positive P-rule** and a rule $a_i^{-1} \longrightarrow uv$ where $u \in \{a_i\}^*$ and $v \in \Sigma_{i+1}^*$ is called a **negative P-rule**. Then a subset P of $\Sigma^* \times \Sigma^*$ is called a **power system** if

1. P contains only positive and negative P-rules.

2. For all $1 \leq i \leq n$ there is a negative P-rule $a_i^{-1} \longrightarrow uv$ in P if and only if there also is a positive P-rule of the form $a_i^m \longrightarrow r$ with $m \geq 1$ in P.

3. For all $1 \leq i \leq n$ there is at most one negative P-rule $a_i^{-1} \longrightarrow uv$ and at most one positive P-rule $a_i^m \longrightarrow r$ in P. $\diamond$

In combining these rule systems we can characterize special group presentations. Let $\mathrm{X} \in \{\mathrm{AB}, \mathrm{NI}, \mathrm{P}\}$. A presentation (Σ, T) is called a **CX-string-rewriting system** (CX-system) if $T = C \cup I$ where C is a commutation system and I contains the trivial rules, i.e., $I = \{a_i a_i^{-1} \longrightarrow \lambda, a_i^{-1} a_i \longrightarrow \lambda | 1 \leq i \leq n\}$. It is called a **PCX-string-rewriting system** (PCX-system) if $T = C \cup P \cup I$ where T additionally includes a power system P. The motivation for such presentations stems from the fact that they can be used to characterize special classes of groups.

Theorem 2.4.12
For a finitely presented group $\mathcal{G}$ the following statements hold:

1. *$\mathcal{G}$ is Abelian if and only if there is a PCAB-system presenting $\mathcal{G}$.*

2. *$\mathcal{G}$ is nilpotent if and only if there is a PCNI-system presenting $\mathcal{G}$.*

3. *$\mathcal{G}$ is polycyclic if and only if there is a PCP-system presenting $\mathcal{G}$.* $\square$

Using a **syllable ordering** Wißmann has shown that a PCX-system (Σ, T) is a Noetherian string-rewriting system and he gave a completion procedure for such systems which terminates with an output that is again a PCX-system of the same type.

Definition 2.4.13
Let Σ be an alphabet and $\succ$ a partial ordering on Σ^*. We define an ordering $\succ^{\mathrm{lex}}$ on m-tuples over Σ^* as follows:

$$(u_0, \ldots, u_m) \succ^{\mathrm{lex}} (v_0, \ldots, v_m)$$

if and only if

there exists $0 \leq k \leq m$ such that $u_i = v_i$ for all $0 \leq i < k$ and $u_k \succ v_k$.

Let $a \in \Sigma$. Then every $w \in \Sigma^*$ can be uniquely decomposed with respect to a as $w \equiv w_0 a w_1 \ldots a w_k$, where $|w|_a = k \geq 0$ and $w_i \in (\Sigma \backslash \{a\})^*$. Given a total precedence[17] $\triangleright$ on Σ we can define a **syllable ordering** by

$$u >_{\mathrm{syll}(\Sigma)} v$$

if and only if

$|u|_a > |v|_a$ or

[17] By a precedence on an alphabet we mean a partial ordering on its letters.

$$|u|_a = |v|_a \text{ and } (u_0, \ldots, u_m) >^{\mathrm{lex}}_{\mathrm{syll}(\Sigma\backslash\{a\})} (v_0, \ldots, v_m)$$

where a is the largest letter in Σ according to $\triangleright$ and $(u_0, \ldots, u_m)$, $(v_0, \ldots, v_m)$ are the decompositions of u and v with respect to a in case $|u|_a = |v|_a = m$. In case we compare the tuples in reverse order, i.e.,

$$(u_m, \ldots, u_0) >^{\mathrm{lex}}_{\mathrm{syll}(\Sigma\backslash\{a\})} (v_m, \ldots, v_0)$$

we say that the syllable ordering has **status right**. $\diamond$

The total precedence used on an alphabet $\Sigma = \{a_i, a_i^{-1} \mid 1 \leq i \leq n\}$ in our setting is $a_1^{-1} \succ a_1 \succ \ldots a_i^{-1} \succ a_i \succ \ldots \succ a_n^{-1} \succ a_n$. Using the syllable ordering induced by this precedence we can give a characterization of the elements of our group as a subset of the set of **ordered group words** $\mathsf{ORD}(\Sigma) = \mathsf{ORD}(\Sigma_1)$, where we define $\mathsf{ORD}(\Sigma_i)$ recursively by $\mathsf{ORD}(\Sigma_{n+1}) = \{\lambda\}$, and $\mathsf{ORD}(\Sigma_i) = \{w \in \Sigma_i^* \mid w \equiv uv$ for some $u \in \{a_i\}^* \cup \{a_i^{-1}\}^*, v \in \mathsf{ORD}(\Sigma_{i+1})\}$. Further with respect to T we define some constants $\epsilon_T(i)$ for $1 \leq i \leq n$ by setting

$$\epsilon_T(i) = \begin{cases} \infty & \text{if } T \text{ contains no P-rules for } a_i \\ m & \text{if } T \text{ contains a P-rule } a_i^m \longrightarrow r \text{ for some unique } m > 0. \end{cases}$$

One can show that using the syllable ordering for orienting T we get

$$\mathrm{IRR}(T) = \{a_1^{i_1} \ldots a_n^{i_n} | i_1, \ldots, i_n \in \mathbf{Z}, \text{ and if } \epsilon_R(j) \neq \infty \text{ then } 0 \leq i_j \leq \epsilon_T(j)\}.$$

For example the semi-Thue system (Σ, T) where $T = C \cup I$ such that we have $C = \{a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta} \mid 1 \leq i < j \leq n, \delta, \delta' \in \{1, -1\}\}$ and $I = \{a_i a_i^{-1} \longrightarrow \lambda, a_i^{-1} a_i \longrightarrow \lambda \mid 1 \leq i \leq n\}$ is a presentation of the free commutative group generated by $\{a_1, \ldots, a_n\}$ and we have $\mathrm{IRR}(T) = \mathsf{ORD}(\Sigma)$.

In restricting the syllable ordering introduced in definition 2.4.13 to ordered group words this gives us $a_1^{i_1} \ldots a_n^{i_n} >_{\mathrm{syll}} a_1^{j_1} \ldots a_n^{j_n}$ if and only if for some $1 \leq d \leq n$ we have $i_l = j_l$ for all $1 \leq l \leq d-1$ and $i_d >_{\mathbf{Z}} j_d$ with

$$\alpha <_{\mathbf{Z}} \beta \text{ iff } \begin{cases} \alpha \geq 0 \text{ and } \beta < 0 \\ \alpha \geq 0, \beta > 0 \text{ and } \alpha < \beta \\ \alpha < 0, \beta < 0 \text{ and } \alpha > \beta \end{cases}$$

where $\leq$ is the usual ordering on $\mathbf{Z}$. We then call a_d the **distinguishing letter** between the two ordered group words.

Let us continue by giving some further information on nilpotent groups. The following lemma gives syntactical information on the results of multiplying a letter by special ordered group words.

Lemma 2.4.14
Let $\mathcal{G}$ be a nilpotent group with a convergent PCNI-presentation (Σ, T). Further for some $1 \leq j < i \leq n$ let $w_1 \in \mathsf{ORD}(\Sigma\backslash\Sigma_j)$, $w_2 \in \mathsf{ORD}(\Sigma_{i+1})$. Then we have $a_i \circ w_1 \equiv w_1 a_i z_1$ and $w_2 \circ a_i \equiv a_i z_2$ for some $z_1, z_2 \in \mathsf{ORD}(\Sigma_{i+1})$. $\square$

In section 2.1 it was stated that an arbitrary finitely generated nilpotent group $\mathcal{G}$ has a normal subgroup $\mathcal{N}$ such that $\mathcal{N}$ is torsion-free nilpotent and $\mathcal{G}/\mathcal{N}$ is finite. Furthermore, torsion-free nilpotent groups have a central series with infinite cyclic factors and, therefore, we can assume that $\mathcal{N}$ has a CNI-presentation, i.e., a presentation containing no power rules (compare [Wi89]). Now every element $g \in \mathcal{G}$ can be uniquely expressed in the form $g \equiv ew$ where $e \in \mathcal{G}/\mathcal{N}$ and w is an ordered group word in $\mathcal{N}$. We can apply the same technique used for context-free groups to give a presentation of $\mathcal{G}$ in terms of $\mathcal{N}$ and $\mathcal{G}/\mathcal{N}$. Let $(\Sigma, C \cup I)$ be a CNI-presentation of $\mathcal{N}$ and $\mathcal{E} \cong \mathcal{G}/\mathcal{N}$ such that $(\mathcal{E}\backslash\{\lambda\}) \cap \Sigma = \emptyset$. For all $e \in \mathcal{E}$ let $\phi_e : \Sigma \longrightarrow \mathcal{N}$ be a function such that ϕ_λ is the inclusion and for all $a \in \Sigma$, $\phi_e(a) = \mathsf{inv}(e) \circ_{\mathcal{G}} a \circ_{\mathcal{G}} e$. For all $e_1, e_2 \in \mathcal{E}$ let $z_{e_1,e_2} \in \mathcal{N}$ such that $z_{e_1,\lambda} \equiv z_{\lambda,e_1} \equiv \lambda$ and for all $e_1, e_2, e_3 \in \mathcal{E}$ with $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$, $e_1 \circ_{\mathcal{G}} e_2 \equiv e_3 z_{e_1,e_2}$. Let $\Gamma = (\mathcal{E}\backslash\{\lambda\}) \cup \Sigma$ and let T consist of the sets of rules C and I, and the additional rules:

$$
\begin{array}{lll}
e_1e_2 & \longrightarrow e_3 z_{e_1,e_2} & \text{for all } e_1, e_2 \in \mathcal{E}\backslash\{\lambda\}, e_3 \in \mathcal{E} \text{ such that } e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3, \\
ae & \longrightarrow e\phi_e(a) & \text{for all } e \in \mathcal{E}\backslash\{\lambda\}, a \in \Sigma.
\end{array}
$$

Then (Γ, T) is a convergent presentation of $\mathcal{G}$ as an extension of $\mathcal{N}$ by $\mathcal{E}$.

Note that finitely generated commutative groups can also be treated as a special case of nilpotent groups. But they can also be viewed as special commutative monoids. Therefore, let us close this section with a short remark on presentations of finitely presented commutative monoids. If $\mathcal{M}$ is finitely presented by a semi-Thue system $(\Sigma, T \cup C)$, where C is the commutator system for $\Sigma = \{a_1, \ldots, a_n\}$, in general we cannot expect this presentation to be convergent or to allow an equivalent finite convergent semi-Thue system[18]. But finitely generated commutative monoids always allow finite convergent presentations in terms of semi-Thue systems modulo commutativity. Let us start to specify such presentations by giving some basic definitions.

Definition 2.4.15
For an alphabet $\Sigma = \{a_1, \ldots, a_n\}$ let $\mathcal{T}_\Sigma = \{a_1^{i_1} \ldots a_n^{i_n} \mid i_j \in \mathbf{N}\}$ denote the set of **ordered words** over Σ. We can define a mapping $\circ_{\mathcal{T}_\Sigma} : \mathcal{T}_\Sigma \times \mathcal{T}_\Sigma \longrightarrow \mathcal{T}_\Sigma$ by setting $a_1^{i_1} \ldots a_n^{i_n} \circ_{\mathcal{T}_\Sigma} a_1^{j_1} \ldots a_n^{j_n} \equiv a_1^{i_1+j_1} \ldots a_n^{i_n+j_n}$. Then $\circ_{\mathcal{T}_\Sigma}$ is an associative binary operation on $\mathcal{T}_\Sigma$ with identity $\lambda = a_1^0 \ldots a_n^0$. Thus, $\mathcal{T}_\Sigma$ together with $\circ_{\mathcal{T}_\Sigma}$ and λ is a monoid, namely the **free commutative monoid generated by** Σ. $\diamond$

We will write $\mathcal{T}$ is case no confusion is likely to arise.

Definition 2.4.16
Let Σ be a finite alphabet and $\mathcal{T}$ as in definition 2.4.15.

1. A **semi-Thue system modulo commutativity** T_c is a subset of $\mathcal{T} \times \mathcal{T}$. The elements (l, r) of T_c are called **rules** and will often be written as $l \longrightarrow r$.

[18] For example take $\Sigma = \{a, b, c\}$ and $T = \{(abc, \lambda)\} \cup \{(ba, ab), (ca, ac), (cb, bc)\}$. Then no equivalent finite convergent semi-Thue system exists.

2. The **single-step reduction relation** on $\mathcal{T}$ induced by a semi-Thue system modulo commutativity T_c is defined as follows: For any u, v in $\mathcal{T}$, $u \longrightarrow_{T_c} v$ if and only if there exist x in $\mathcal{T}$ and (l, r) in T_c such that $u = l \circ_{\mathcal{T}} x$ and $v = r \circ_{\mathcal{T}} x$. The **reduction relation** on $\mathcal{T}$ induced by T_c is the reflexive transitive closure of $\longrightarrow_{T_c}$ and is denoted by $\stackrel{*}{\longrightarrow}_{T_c}$. The reflexive transitive symmetric closure is defined as usual and denoted by $\stackrel{*}{\longleftrightarrow}_{T_c}$. $\diamond$

Recall that for u, $v \in \mathcal{T}$, u is called a divisor of v if there exists an element $w \in \mathcal{T}$ such that $u \circ_{\mathcal{T}} w = v$. The least common multiple of two terms $u \equiv a_1^{i_1} \dots a_n^{i_n}$ and $v \equiv a_1^{j_1} \dots a_n^{j_n}$ is defined as $\mathsf{LCM}(u, v) = a_1^{\max\{i_1, j_1\}} \dots a_n^{\max\{i_n, j_n\}}$ and is the "shortest" term that has both u and v as divisors. Hence this term gives rise to a critical situation in case u and v are left hand sides of rules and $\mathsf{LCM}(u, v) \neq u \circ_{\mathcal{T}} v$.

Definition 2.4.17
A partial ordering $\preceq$ on $\mathcal{T}$ is called **admissible** (with respect to $\circ_{\mathcal{T}_\Sigma}$) if for all u, v, x in $\mathcal{T}$

1. $\lambda \preceq u$, and
2. $u \prec v$ implies $u \circ_{\mathcal{T}} x \prec v \circ_{\mathcal{T}} x$. $\diamond$

Then if $\preceq$ is an admissible total ordering on $\mathcal{T}$ (which is of course well-founded) and u is a proper divisor of v this implies $u \prec v$. Notice that given an admissible total ordering, a finite semi-Thue system modulo commutativity always has a finite equivalent convergent semi-Thue system modulo commutativity with respect to this ordering. Then in case a commutative monoid $\mathcal{M}$ is presented by a finite semi-Thue system modulo commutativity (Σ, T_c) which is convergent with respect to an admissible total ordering $\succeq_{T_c}$, for u, $v \in \mathcal{M}$ we have $u \circ_{\mathcal{T}} v \succeq_{T_c} u \circ_{\mathcal{M}} v$.

In the following chapters, if not stated otherwise, our monoids and groups are presented by finite convergent semi-Thue systems respectively finite convergent semi-Thue systems modulo commutativity which are convergent with respect to some admissible well-founded total ordering[19] in the respective setting, i.e., if $\succeq$ is the completion ordering, then for all rules (l, r) in the set T, $l \succ r$ holds.

[19] This ordering used for completion will sometimes be called the completion ordering of the system and we will only consider convergent systems having such an ordering in this thesis. Notice that in general there are convergent systems which allow no such completion ordering (see e.g. [Es86]).

Chapter 3

Non-Commutative Gröbner Bases

Was du tust, bedenke das Ende.

SIRACH 7:40

In this chapter we will now give a short outline on the results on ideals in non-commutative rings. Further we state some undecidability results which give a limit to what can be achieved in certain non-commutative structures.

Section 3.1: Mora generalized Buchberger's ideas to finitely generated free monoid rings. The notions of reduction, s-polynomials and Gröbner bases can be carried over and a characterization of Gröbner bases in a finitary manner is possible. Hence it is decidable, whether a finite set of polynomials is a Gröbner basis. But this characterization can no longer be used to give a terminating completion algorithm as none exists. Mora developed an enumerating procedure for two-sided ideals and in restricting the attention to finitely generated right ideals and prefix reduction, a terminating completion algorithm was provided.

Section 3.2: Kandri-Rody and Weispfenning have shown that the ideal membership problem for two-sided ideals in a free monoid ring with two generators is undecidable in general. We here show the equivalence of the word problem for semi-Thue systems to a restricted version of the ideal membership problem in a free monoid ring. Hence the existence of a semi-Thue system over two letters with undecidable word problem implies the undecidability of the ideal membership problem for a free monoid ring with two generators. The same equivalence can be shown for the word problem in groups and a restricted version of the ideal membership problem in a free group ring. Again the existence of a group system with four letters (two generators plus their inverses) with undecidable word problem implies the undecidability of the ideal membership problem for free group rings with more than one generator. Finally we show that it is undecidable whether a finite Gröbner basis with respect to an admissible ordering in a free monoid ring with more than one generator exists.

Section 3.3: A class of non-commutative rings where finitely generated left, right and two-sided ideals have finite Gröbner bases are the solvable polynomial rings and the skew polynomial rings. We sketch Weispfenning's approach to the latter structure as it can be viewed as a monoid ring.

For more information on Mora's or Weispfenning's approach the reader is referred to [Mo85] and [We92].

3.1 The Free Monoid Ring

Let Σ^* be a free monoid over a finite alphabet Σ. It has been shown by Mora that Buchberger's ideas generalize naturally to the free monoid ring over $\mathbf{K}$ and Σ^*. In this section we now sketch his approach which can be found more explicitly for example in [Mo85].

Because of non-commutativity it becomes important to distinguish one and two-sided ideals and the results gained differ from the commutative case. This is e.g. due to the fact that for more than one variable the corresponding free monoid ring is no longer Noetherian and that for the set Σ^* no equivalent to Dickson's lemma in $\mathcal{T}$ holds, i.e., we cannot prove termination with the methods used in the commutative case and it can be shown that finite Gröbner bases need not exist, even for finitely generated two-sided ideals.

Let $\succeq$ be a total admissible well-founded ordering on Σ^*. This ordering can be extended to $\mathbf{K}[\Sigma^*]$ and used to distinguish the head term, head coefficient, head monomial and the reduct of a polynomial. Two-sided reduction then can be defined naturally.

Definition 3.1.1 (Mora)
Let p, f be two non-zero polynomials in $\mathbf{K}[\Sigma^*]$. We say f **reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{m}}_{g} q$, if

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

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

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

When studying right ideals this reduction is restricted to prefix reduction[1].

Definition 3.1.2
Let p, f be two non-zero polynomials in $\mathbf{K}[\Sigma^*]$. We say f **prefix reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{p}}_{f} q$, if

[1] A similar approach is possible to study left ideals.

(a) $\mathsf{HT}(f)w \equiv t$ for some $w \in \mathcal{M}$, i.e., $\mathsf{HT}(f)$ is a prefix of t, and

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

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

Note that Mora's two-sided reduction and prefix reduction have all nice properties connected to reductions in structures with an admissible ordering and capture the ideal respectively right ideal congruence in the free monoid ring. Furthermore, the translation lemma holds and the respective reductions are preserved under two-sided respectively right-sided multiplication with terms. We can define Gröbner bases for two-sided ideals and prefix Gröbner bases for right ideals and characterize them in a natural way by corresponding s-polynomials.

Definition 3.1.3
A set $G \subseteq \mathbf{K}[\Sigma^*]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{m}}$, if

(i) $\xleftrightarrow{*}^{\mathrm{m}}_{G} \; = \; \equiv_{\mathsf{ideal}(G)}$, and

(ii) $\longrightarrow^{\mathrm{m}}_{G}$ is confluent. $\diamond$

Definition 3.1.4
A set $G \subseteq \mathbf{K}[\Sigma^*]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{p}}$ or a **prefix Gröbner basis**, if

(i) $\xleftrightarrow{*}^{\mathrm{p}}_{G} \; = \; \equiv_{\mathsf{ideal}_r(G)}$, and

(ii) $\longrightarrow^{\mathrm{p}}_{G}$ is confluent. $\diamond$

Definition 3.1.5
Given two non-zero polynomials $p_1, p_2 \in \mathbf{K}[\Sigma^*]$, if there are $u, v \in \Sigma^*$ such that either $\mathsf{HT}(p_1)u \equiv v\mathsf{HT}(p_2)$ and $|\mathsf{HT}(p_1)| < |v|$ or $u\mathsf{HT}(p_1)v \equiv \mathsf{HT}(p_2)$, the corresponding **s-polynomial** is defined either as

$$\mathsf{spol}_m(p_1, p_2, u, v) = \mathsf{HC}(p_1)^{-1} \cdot p_1 * u - \mathsf{HC}(p_2)^{-1} \cdot v * p_2 \text{ or as}$$

$$\mathsf{spol}_m(p_1, p_2, u, v) = \mathsf{HC}(p_1)^{-1} \cdot u * p_1 * v - \mathsf{HC}(p_2)^{-1} \cdot p_2.$$

Let $U_{p_1,p_2} \subseteq \Sigma^* \times \Sigma^*$ be the set containing *all* such pairs $u, v \in \Sigma^*$. $\diamond$

Notice that the sets U_{p_1,p_2} are always finite and that they correspond to the critical pairs for semi-Thue systems as mentioned in section 2.4.

Definition 3.1.6
Given two non-zero polynomials $p_1, p_2 \in \mathbf{K}[\Sigma^*]$, if there is $w \in \Sigma^*$ such that $\mathsf{HT}(p_1) \equiv \mathsf{HT}(p_2)w$ the **prefix s-polynomial** is defined as

$$\mathsf{spol}_p(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w.$$

$\diamond$

In analogy to theorem 2.3.8 we can give the following characterizations of Gröbner bases respectively prefix Gröbner bases, which can be used to decide whether a finite set of polynomials is a respective basis and to give procedures to enumerate such bases.

Theorem 3.1.7
For a set of polynomials $F \subseteq \mathbf{K}[\Sigma^*]$, the following statements are equivalent:

1. *F is a Gröbner basis.*
2. *For all $f_k, f_l \in F$, $(u, v) \in U_{f_k, f_l}$ we have $\mathsf{spol}_m(f_k, f_l, u, v) \overset{*}{\longrightarrow}{}^{\mathrm{m}}_{F} 0$.* $\square$

Procedure: Gröbner Bases in Free Monoid Rings [Mora]

Given: A finite set $F \subseteq \mathbf{K}[\Sigma^*]$.
Find: G, a Gröbner basis of $\mathsf{ideal}(F)$.

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

Theorem 3.1.8
For a set of polynomials $F \subseteq \mathbf{K}[\Sigma^*]$, the following statements are equivalent:

1. *F is a prefix Gröbner basis.*

2. *For all polynomials* $f_k, f_l \in F$ *we have* $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$. □

Procedure: PREFIX GRÖBNER BASES IN FREE MONOID RINGS [MORA]

Given: A finite set $F \subseteq \mathbf{K}[\Sigma^*]$.
Find: G, a prefix Gröbner basis of $\mathsf{ideal}_r(F)$.

$G := F$;
while there is $g \in G$ such that $\mathsf{HT}(g)$ is prefix reducible by $G\backslash\{g\}$ **do**
  $G := G\backslash\{g\}$;
  $f :=$ normalform$(g, \longrightarrow^{\mathrm{p}}_{G})$;
  % Compute a normal form using prefix reduction.
  if $f \neq 0$
    then $G := G \cup \{f\}$;
  endif
endwhile

While termination for procedure PREFIX GRÖBNER BASES IN FREE MONOID RINGS follows immediately from the fact that polynomials in G are replaced by "smaller" polynomials and no cycles can occur, procedure GRÖBNER BASES IN FREE MONOID RINGS need not terminate as the ideal membership problem for finitely generated two-sided ideals in $\mathbf{K}[\Sigma^*]$ is unsolvable in general. The following section will give some insight into undecidability results related to free monoid rings and free group rings.

3.2 Undecidability Results

Kandri-Rody and Weispfenning have shown in [KaWe90] that the ideal membership problem for finitely generated two-sided ideals is algorithmically unsolvable for the free monoid ring $\mathbf{Q}[\{X_1, X_2\}^*]$ by reducing the halting problem for Turing machines to this problem. Here we state a similar result by showing that the word problem for semi-Thue systems is equivalent to a restricted version of the ideal membership problem in free monoid rings.

Theorem 3.2.1
Let (Σ, T) *be a finite semi-Thue system and* $P_T = \{l - r \mid (l, r) \in T\}$. *Then for* $u, v \in \Sigma^*$ *the following statements are equivalent:*

1. $u \overset{*}{\longleftrightarrow}_T v$.
2. $u - v \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$.

Proof :
$1 \Longrightarrow 2$: Using induction on k we show that $u \overset{k}{\longleftrightarrow}_T v$ implies $u - v \in \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$.

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

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

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

where $p_k' = \alpha_k \cdot (w_l' - w_k')$, $w_k' \overset{*}{\longleftrightarrow}_T t \overset{*}{\longleftrightarrow}_T w_l'$ and $w_l' \neq w_k'$. Therefore, in case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p_k' does not contain t, i.e., K will be decreased in any case.

q.e.d.

The existence of a finite semi-Thue system over an alphabet with two elements having undecidable word problem yields that the ideal membership problem for free monoid rings with more than one generator is undecidable. In case the free monoid is generated by one element, we have decidable ideal membership problem. This is due to the fact that this corresponds to the ordinary polynomial ring in one variable and there e.g. the Euclidean algorithm can be applied to solve the ideal membership problem.

Perhaps less obvious is that the word problem for groups is similarly equivalent to a restricted version of the membership problem for ideals in a free group ring. Let the group be presented by a semi-Thue system $(\Sigma, T \cup T_I)$ such that there exists an involution $\imath : \Sigma \longrightarrow \Sigma$ such that for all $a \in \Sigma$ we have $\imath(a) \neq a$, $\imath(\imath(a)) = a$ and $(\imath(a)a, \lambda), (a\imath(a), \lambda) \in T_I$.

Theorem 3.2.2
Let $(\Sigma, T \cup T_I)$ be a finite group system with $T_I = \{(\imath(a)a, \lambda), (a\imath(a), \lambda) \mid a \in \Sigma\}$, i.e., (Σ, T_I) is a presentation of a free group $\mathcal{F}$. Further we can associate a system of polynomials $P_T = \{l - r \mid (l, r) \in T\}$ with T and without loss of generality we can assume that l and r are in normal form with respect to T_I. Then for $u, v \in \Sigma^*$ the following statements are equivalent:

1. $u \overset{*}{\longleftrightarrow}_{T \cup T_I} v$.
2. $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$.

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

1. $u_k \longleftrightarrow_T v$ with $(l, r) \in T$.
   Without loss of generality we can assume $u_k \equiv xly$ and $v \equiv xry$ for some words $x, y \in \Sigma^*$. Now this gives us
   $$u{\downarrow_{T_I}} - v{\downarrow_{T_I}} = u{\downarrow_{T_I}} - \underbrace{u_k{\downarrow_{T_I}} + xly{\downarrow_{T_I}}}_{=0} - xry{\downarrow_{T_I}}$$
   and $xly{\downarrow_{T_I}} - xry{\downarrow_{T_I}} = x * (l - r) * y$, where $*$ denotes multiplication in $\mathbf{K}[\mathcal{F}]$. By our induction hypothesis we know $u{\downarrow_{T_I}} - u_k{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$ and, hence, we get $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$.
2. $u_k \longleftrightarrow_{T_I} v$ with $(a\imath(a), \lambda) \in T_I$[2].
   Without loss of generality we can assume $u_k \equiv xa\imath(a)y$ for some $x, y \in \Sigma^*$ and $v \equiv xy$, i.e., $u_k{\downarrow_{T_I}} = v{\downarrow_{T_I}}$ and therefore $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$.

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

$2 \Longrightarrow 1$: It remains to show that $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} \in \mathsf{ideal}^{\mathbf{K}[\mathcal{F}]}(P_T)$ implies $u \overset{*}{\longleftrightarrow}_{T \cup T_I} v$. We know $u{\downarrow_{T_I}} - v{\downarrow_{T_I}} = \sum_{j=1}^{n} \beta_j \cdot x_j * (l_{i_j} - r_{i_j}) * y_j$, where $\beta_j \in \mathbf{K}^*$, $x_j, y_j \in \mathcal{F}$. Therefore, by showing the following stronger result we are done: A representation $u - v = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w_j')$, $\alpha_j \in \mathbf{K}^*$, $u, v, w_j, w_j' \in \mathcal{F}$ and $w_j \overset{+}{\longleftrightarrow}_T w_j'$ implies that $u \overset{*}{\longleftrightarrow}_T v$. Hence, let $u - v = \sum_{j=1}^{m} p_j$ be such a representation. Depending on this representation $\sum_{j=1}^{m} p_j$ and the ordering $\succeq$ on Σ^* we can define $t = \max\{w_j, w_j' \mid j = 1, \dots m\}$ and K is the number of polynomials p_j containing t as a term. We will show our claim by induction on (m, K), where $(m', K') < (m, K)$ if and only if $m' < m$ or ($m' = m$ and $K' < K$). In case $m = 0$, then $u - v = 0$ implies $u = v$ and hence $u \overset{0}{\longleftrightarrow}_T v$[3]. Now suppose $m > 0$.

In case $K = 1$, let p_k be the polynomial containing t. Since we either have $p_k = \alpha_k \cdot (t - w_k')$ or $p_k = \alpha_k \cdot (w_k - t)$, where $\alpha_k \in \{1, -1\}$, without loss of generality we can assume $u = t$ and $p_k = t - w_k'$. Using p_k we can decrease m by subtracting p_k from $u - v$ giving us $w_k' - v = \sum_{j=1, j \neq k}^{m} p_j$. Since $u = t \overset{*}{\longleftrightarrow}_T w_k'$ and our induction hypothesis yields $w_k' \overset{*}{\longleftrightarrow}_T v$ we get $u \overset{*}{\longleftrightarrow}_T v$.

In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation containing the term t and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w_k')$ and $p_l = \alpha_l \cdot (t - w_l')$, as the cases where $p_k = \alpha_k \cdot (w_k' - t)$ or $p_l = \alpha_l \cdot (w_l' - t)$ occur can be treated similarly by modifying the respective coefficient. If $w_k' = w_l'$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

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

where $p_k' = \alpha_k \cdot (w_l' - w_k')$, $w_k' \overset{*}{\longleftrightarrow}_T t \overset{*}{\longleftrightarrow}_T w_l'$ and $w_l' \neq w_k'$. Hence, in case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p_k' does not contain t, i.e., K will be decreased in any case.

q.e.d.

As before, the existence of a finite group presentation over four letters (resulting from two generators) with unsolvable word problem implies that the ideal membership problem for free group rings with more than one generator is undecidable. Groups with one generator are known to have decidable word problem as this case corresponds to the ring of Laurent polynomials[4] in the (commutative) free group with one generator.

By theorem 3.2.1 we know that finitely generated ideals in free monoid rings need not admit finite Gröbner bases. It even is possible for a finitely generated ideal to admit a finite Gröbner basis with respect to one admissible ordering and none with respect

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

[4] Notice that the Laurent polynomials can be treated as a quotient of an ordinary polynomial ring.

to another admissible ordering. On the other hand, Mora provided a procedure which given an admissible ordering enumerates a Gröbner basis with respect to this ordering. This procedure terminates in case a finite Gröbner basis with respect to the given ordering exists. Hence the question might arise, whether it is possible to decide for a given finite set of polynomials whether there exists an admissible ordering such that procedure GRÖBNER BASES IN FREE MONOID RINGS terminates, hence whether a finite Gröbner basis exists. This question turns out to be undecidable.

Theorem 3.2.3
It is undecidable, whether a finitely generated ideal has a finite Gröbner basis in the free monoid ring $\mathbf{K}[\{s,t\}^*]$ with respect to a fixed two-sided reduction as defined in definition 3.1.1.

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

Let $\succeq$ be a compatible well-founded partial ordering on $\{s,t\}^*$ such that $s \succ \lambda$ and $t \succ \lambda$ both hold.
Given a finite Thue system T on $\{s,t\}$. Is there a finite and confluent system T' on $\{s,t\}$ that is equivalent to T and based on $\succ$?

To prove our claim we show that the answer for T is "yes" if and only if the set of polynomials P_T associated to T has a finite Gröbner basis in $\mathbf{K}[\{s,t\}^*]$ with respect to $\succ$. If there is an equivalent, finite presentation $(\{s,t\},T')$ convergent with respect to $\succ$, then the set $P_{T'}$ is a finite Gröbner basis of P_T in $\mathbf{K}[\{s,t\}^*]$. This follows as the Thue reduction $\longleftrightarrow_{T'}$ can be simulated by the symmetric closure of the reduction $\longrightarrow^{\mathrm{m}}_{P_T}$ in $\mathbf{K}[\{s,t\}^*]$ (compare definition 3.1.1). Thus it remains to show that in case P_T has a finite Gröbner basis in $\mathbf{K}[\{s,t\}^*]$, there exists a finite Gröbner basis G such that for all $g \in G$ we have $g = u - v$, where $u, v \in \{s,t\}^*$, and $u \stackrel{*}{\longleftrightarrow}_T v$. Then $(\{s,t\},T)$ has an equivalent, convergent, finite presentation $(\{s,t\},T')$, namely $T' = \{(u,v) \mid u-v \in G\}$, since the reduction $\longrightarrow^{\mathrm{m}}$ in $\mathbf{K}[\{s,t\}^*]$ can be compared to a transformation step in a Thue system when restricted to polynomials of the form $u - v$. First we show that in case a finite set F has a finite Gröbner basis in $\mathbf{K}[\{s,t\}^*]$ the procedure GRÖBNER BASES IN FREE MONOID RINGS also computes a finite Gröbner basis of F. Let $\tilde{G}$ be a finite Gröbner basis of P_T with $\mathsf{HT}(\tilde{G}) = \{\mathsf{HT}(g) \mid g \in \tilde{G}\} = \{t_1,\ldots,t_k\}$. Let $H_{t_i} = \{xt_iy \mid x,y \in \Sigma^*\}$, then $\mathsf{HT}(\mathsf{ideal}(P_T)) = \bigcup_{i=1}^k H_{t_i}$, since all polynomials in $\mathsf{ideal}^{\mathbf{K}[\{s,t\}^*]}(P_T)$ reduce to zero by $\tilde{G}$. Further our procedure is correct and, therefore, for each t_i there has to be at least one g_i added to G such that $t_i \equiv x\mathsf{HT}(g_i)y$ for some $x,y \in \Sigma^*$, i.e., $\mathsf{HT}(g_i)$ "divides" t_i. Note that as soon as all such g_i are added to G, we have $\mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\{s,t\}^*]}(G)) \supseteq \bigcup_{i=1}^k H_{t_i}$ and all further computed s-polynomials must reduce to zero. Since the procedure is correct, G then is also a Gröbner basis of $\mathsf{ideal}(P_T)$. It remains to show that in case P_T has a finite Gröbner basis, the finite output G of our procedure has the desired property that for all $g \in G$, $g = u - v$ where

$u, v \in \{s,t\}^*$, and $u \overset{*}{\longleftrightarrow}_T v$. Since all polynomials in P_T have the desired property let us look at the polynomials added to G: Let us assume all polynomials in G have the desired structure and a new polynomial g is added. In case g is due to s–polynomial computation of two polynomials $u_1 - v_1, u_2 - v_2$ we do not lose our structure. The same is true for computing the normal form of a polynomial $u - v$ using a set of polynomials having the same structure. Further $u \overset{*}{\longleftrightarrow}_T v$ is inherited within these operations (compare also the proof of theorem 3.2.1).

q.e.d.

In this proof we used a result of Madlener and Otto in [MaOt94] - a strengthening of Ó'Dúnlaing's result in [OD83] to alphabets Σ_2 containing 2 letters. Let $\mathcal{P}$ be a property of semi-Thue systems over Σ_2 satisfying the following three conditions:

(P1) Whenever T_1 and T_2 are two finite semi-Thue systems on the same alphabet Σ_2 such that T_1 and T_2 are equivalent, then T_1 has property $\mathcal{P}$ if and only if T_2 has it.

(P2) Each semi-Thue system $T_{\Sigma_2} = \{a \longrightarrow \lambda \mid a \in \Sigma_2\}$ has property $\mathcal{P}$.

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

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

Given: A finite semi-Thue system T on Σ_2.
Question: Does the Thue congruence $\overset{*}{\longleftrightarrow}_T$ have $\mathcal{P}$?

Using this result we can easily show the following corollary.

Corollary 3.2.4
It is undecidable, whether for a finitely generated ideal in $\mathbf{K}[\{s,t\}^*]$ there exists a total, well-founded, admissible ordering on $\{s,t\}^*$ such that the ideal has a finite Gröbner basis with respect to reduction as defined in 3.1.1.

Proof :
This follows using the correspondance between Thue systems and ideal bases shown in theorem 3.2.3. Let us define a property $\mathcal{P}(T)$ for semi-Thue systems T on $\Sigma_2 = \{s,t\}$ as follows: $\mathcal{P}(T)$ if and only if there exists a total, well-founded, admissible ordering $\succeq$ on Σ_2^* such that there exists an equivalent finite semi-Thue system T' which is convergent with respect to $\succ$. Then $\mathcal{P}$ fulfills the conditions (P1), (P2) and (P3) mentioned above:

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

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

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

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

q.e.d.

Hence, for two-sided ideals the case of free monoids with two generators is already hard although free monoids allow simple presentations, namely empty sets of defining relations.

3.3 Skew Polynomial Rings

Other classes of non-commutative rings and the possibilities of introducing the theory of Gröbner bases to them have been studied extensively by authors as e.g., Apel and Lassner in [ApLa88], Gateva-Ivanova in [Ga88], Kandri-Rody and Weispfenning in [KaWe90, We92], and Kredel in [Kr93].

A structure where finite Gröbner bases for one- and two-sided ideals exist is the class of solvable polynomial rings which includes the commutative polynomial rings, enveloping algebras of finite dimensional Lie algebras and iterated skew polynomial rings. Solvable polynomial rings can be described by ordinary polynomial rings provided with a "new" multiplication which coincides with the ordinary multiplication except for the case that a variable X_j is multiplied with a variable X_i with lower index, i.e., $i < j$. Then multiplication can be defined by equations

$$X_j \star X_i = c_{ij} X_i X_j + p_{ij}$$

where $c_{ij} \in \mathbf{K}^*$ and p_{ij} is a polynomial "smaller" than $X_i X_j$ with respect to a fixed admissible term ordering on the polynomial ring. One-sided reduction relations and one-sided Gröbner bases are defined naturally but two-sided ideals are not defined by extending the one-sided reduction relations. Instead two-sided Gröbner bases are characterized by one-sided Göbner bases, i.e., a set is a two-sided Gröbner basis if it is both, a left and a right Gröbner basis. The proofs for this theory are more complicated than for commutative polynomial rings and an extensive study of the Gröbner basis approach to solvable polynomial rings can be found in Kredel's PhD thesis ([Kr93]). Note that since we require $c_{ij} \in \mathbf{K}^*$ and p_{ij} is a polynomial "smaller" than $X_i X_j$ with respect to a fixed admissible term ordering on the polynomial ring, we can use an admissible ordering on the solvable polynomial ring and reduction is preserved under multiplication. This is no longer true if we allow $c_{ij} = 0$ as then we find that the head term of a multiple $p * w$ need no longer be the usual commutative product of the two terms $\mathsf{HT}(p)$ and w. Kredel gives a short discussion on such general solvable polynomial rings, which include the Grassmann and Clifford algebras. It is suggested to introduce a concept called saturated reduction to remedy the problems arising for general reduction.

We close this chapter by giving some details on Weispfenning's approach to skew polynomial rings (compare [We92]), as they can be regarded as monoid rings, which will be the subject of the next chapter. Let $\mathbf{K}[X, Y]$ be the ordinary commutative polynomial ring over $\mathbf{K}$ in two variables. As in the case of solvable polynomial rings, a new multiplication $\star$ is introduced, such that for some arbitrary but fixed $1 < e \in \mathbf{N}$ the new structure satisfies the following axioms:

1. $\mathbf{K}[X, Y]$ together with $0, 1, +, -$ and $\star$ forms a $\mathbf{K}$-algebra,
2. for all $\alpha \in \mathbf{K}$, $m, n \in \mathbf{N}$ we have
   $X^m Y^n \star \alpha = \alpha \star X^m Y^n = \alpha \cdot X^m Y^n$,
   $X^m \star X^n = X^{m+n}$,
   $Y^m \star Y^n = Y^{m+n}$,
   $X^m \star Y^n = X^m Y^n$, and
3. $Y \star X = X^e Y$.

The skew polynomial ring corresponding to e is denote by R_e. Although two-sided ideals in this ring are finitely generated, this is no longer true for one-sided ideals. Nevertheless, Weispfenning shows that for finitely generated one-sided ideals finite Gröbner bases exist and how they can be characterized by s-polynomials. Let us proceed by giving some technical details. The next lemma gives some insight into computation in R_e that will be used later on. If for some terms s, t, u we have $s \star t = u$, then s left-divides u and t right-divides u, denoted by s ldiv u respectively t rdiv u. Similarly, in case for a further term s' we have $s \star t \star s' = u$, then t divides u, denoted by t div u.

Lemma 3.3.1
For two terms $s = X^m Y^n$ and $t = X^q Y^r$ the following statements hold:

1. *s rdiv t if and only if $n \leq r$ and $m \cdot e^{r-n} \leq q$. Then $X^{q-m \cdot e^{(r-n)}} Y^{(r-n)} \star s = t$.*
2. *s ldiv t if and only if $n \leq r$, $m \leq q$ and e^n divides $(q-m)$. Then $s \star X^{\frac{q-m}{e^n}} Y^{(r-n)} = t$.*
3. *s div t if and only if $m \leq q$ and $n \leq r$ if and only if there exist $h, k \in \mathbf{N}$ such that $X^h \star s \star Y^k = t$. Note that if furthermore $t = u \star s \star v$ for some terms u, v, then these terms need not be unique.* □

Weispfenning uses an inverse-lexicographical ordering on the terms and proves that this ordering is admissible with respect to the new multiplication $\star$. Hence in defining left, right and two-sided reduction, it turns out that for these reductions essential properties hold, e.g., the translation lemma, and the reduction steps are preserved under the corresponding multiplications.

Definition 3.3.2
Let p, f be two non-zero polynomials in R_e. We say f **left reduces** p at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{l}_{f} q$, if

(a) $w \star \mathsf{HT}(f) = t$ for some $w \in \mathcal{M}$, i.e., $\mathsf{HT}(f)$ rdiv t, and

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

We say f **right reduces** p at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{r}}_{f} q$, if

(a) $\mathsf{HT}(f) \star w = t$ for some $w \in \mathcal{M}$, i.e., $\mathsf{HT}(f)$ ldiv t, and

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

We say f **two-sided reduces** p at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{t}}_{f} q$, if

(a) $X^m \star \mathsf{HT}(f) \star Y^n = t$ for some $m, n \in \mathbf{N}$, and

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

Notice that the one-sided reductions correspond to the respective one-sided ideals. Since in defining two-sided reduction only special multiples are allowed, this correspondence to ideals no longer holds. The set connected to two-sided reduction using F is called the **restricted ideal** generated by F, which is the closure of F under addition and multiplication with powers of X from the left and powers of Y from the right. Closely related to these reductions are s-polynomials, which as usual arise from special multiples of head terms of polynomials. For two terms $t = X^m Y^n$, $t' = X^{m'} Y^{n'}$ with $n \geq n'$ such special multiples are defined as follows:

1. For $r = \max\{m, m' \cdot e^{(n-n')}\}$, the term $X^r Y^n$ is the least common left multiple of t and t' denoted by $\mathsf{llcm}(t, t')$.

2. Suppose t and t' have some common right multiple. Then put $r = m$ if $m \geq m'$ and else put $r = m' + \lceil \frac{m'-m}{e^n} \rceil \cdot e^n - m' + m$. Then $r \in \mathbf{N}$ and $X^r Y^n$ is the least right common multiple of t and t' denoted by $\mathsf{lrcm}(t, t')$.

Now such multiples allow to specify "overlaps" between "rules" corresponding to polynomials.

Definition 3.3.3
Let p_1, p_2 be two non-zero polynomials in R_e. Further let $\mathsf{HT}(p_i) = X^{m_i} Y^{n_i}$, $i \in \{1, 2\}$. For $u = \mathsf{llcm}(\mathsf{HT}(p_1), \mathsf{HT}(p_2))$ with $u_1 \star \mathsf{HT}(p_1) = u_2 \star \mathsf{HT}(p_2) = u$ we get the **left s-polynomial**

$$\mathsf{spol}_l(p_1, p_2) = \mathsf{HC}(p_2) \cdot u_1 * p_1 - \mathsf{HC}(p_1) \cdot u_2 * p_2.$$

In case $v = \mathsf{lrcm}(\mathsf{HT}(p_1), \mathsf{HT}(p_2))$ exists and $\mathsf{HT}(p_1) \star v_1 = \mathsf{HT}(p_2) \star v_2 = v$ we get the **right s-polynomial**

$$\mathsf{spol}_r(p_1, p_2) = \mathsf{HC}(p_2) \cdot p_1 * v_1 - \mathsf{HC}(p_1) \cdot p_2 * v_2.$$

For $m = \max\{m_1, m_2\}$ and $n = \max\{n_1, n_2\}$ we get the **two-sided s-polynomial**

$$\mathsf{spol}_t(p_1, p_2) = \mathsf{HC}(p_2) \cdot X^{m-m_1} * p_1 * Y^{n-n_1} - \mathsf{HC}(p_1) \cdot X^{m-m_2} * p_2 * Y^{n-n_2}.$$

$\diamond$

In analogy to Buchberger, a finite set $G \subseteq R_e$ is called a **left, right or restricted Gröbner basis** if left, right respectively two-sided reduction with respect to G is confluent. These bases can now be characterized as follows:

Theorem 3.3.4
A finite subset G of R_e is a left, right, respectively restricted Gröbner basis in R_e if and only if for all polynomials $f \neq g$ in G, $\mathsf{spol}_l(f, g) \xrightarrow{*}{}^{\mathrm{l}}_G 0$, $\mathsf{spol}_r(f, g) \xrightarrow{*}{}^{\mathrm{r}}_G 0$, $\mathsf{spol}_t(f, g) \xrightarrow{*}{}^{\mathrm{t}}_G 0$, respectively. $\square$

Weispfenning has further shown the existence of an algorithm to compute these bases for finite subsets of R_e. Hence, the ideal membership problem for finitely generated left and right ideals in R_e is solvable. Weispfenning further showed how restricted Gröbner bases can be used to solve the ideal membership problem for two-sided ideals by constructing two-sided Gröbner bases. Two-sided Gröbner basis are defined as sets $G \subseteq R_e$ such that G is a restricted Gröbner basis and additionally the ideal and the restricted ideal generated by G coincide. Such bases now can be characterized by the following lemma which allows an algorithm to compute them.

Lemma 3.3.5
Let $G \subseteq R_e$ be a restricted Gröbner basis with $d = \max\{\mathsf{deg}_Y(g) \mid g \in G\}$[5]. If for all $g \in G$ and all $0 \leq m \leq d$, $Y * g \xrightarrow{*}{}^{\mathrm{t}}_G 0$ and $g * X^{e^m} \xrightarrow{*}{}^{\mathrm{t}}_G 0$, then G is a two-sided Gröbner basis. $\square$

Interesting is that two-sided Gröbner bases, as in the case of solvable polynomial rings, are constructed using a closure of a specialized Gröbner basis, here a restricted Gröbner basis. Important for termination is that the polynomials considered by the completion to compute left, right and restricted Gröbner bases have a bound on the Y-degree of the head terms of the computed polynomials.

The idea of filling up a term that divides another term in order to do reduction will be used later on in the approaches to commutative monoids and nilpotent groups (compare chapter 4 and chapter 5). In contrary to Weispfenning's approach the structures there will not allow admissible orderings in general, but as here Dickson's lemma can be used to prove the existence of finite bases and to ensure termination of the algorithms.

[5]Here deg_Y denotes the number of occurrences of the variable Y in the head term of g.

Chapter 4

Reduction in Monoid and Group Rings

Docendo discimus.

Seneca

In defining reduction for monoid and group rings different approaches are possible and some will be studied here. Since we mainly deal with non-commutative structures, we restrict ourselves to right reductions.

Section 4.1: In order to use polynomials as rules a well-founded ordering on the rings is necessary and this section gives information on how such an ordering can be lifted from the ordering induced by the presentation of the respective monoid. It is shown why well-founded orderings on the monoid in general need not be additionally compatible with the monoid operation.

Section 4.2: A natural way to use a set of polynomials as rules is to use all term multiples of these polynomials as rules. This is what is done e.g. in Buchberger's approach. A polynomial f then reduces a polynomial p at a monomial $\alpha \cdot t$ of p in case there exists an element $w \in \mathcal{M}$ such that the head term of the polynomial $f * w$ equals t. Then $\alpha \cdot t$ can be removed from p by subtracting an appropriate multiple $\beta \cdot f * w$ with head term equal to $\alpha \cdot t$. This reduction is called strong reduction as it can be used to characterize the right ideal congruence generated by the polynomials used for reduction. In defining s-polynomials related to strong reduction in general it turns out to be impossible to give a localization to finitely many candidates for the critical situations induced by two polynomials. Nevertheless, although some of the properties of Buchberger's reduction no longer hold, we can characterize strong Gröbner bases by s-polynomials, but this cannot be done in a finitary manner. Thus this characterization does not yield a test to decide whether a finite set is a strong Gröbner basis.

Section 4.3: Weakening reduction can provide the means to give a finitary confluence test. The first idea studied is to restrict the right multiples of a polynomial by terms used for reduction to those where the head term is preserved by multiplication, i.e., the head term of the multiple results from the head term of the original polynomial. Defining reduction in this way, the right ideal congruence is no longer captured by reduction. This defect can be repaired by a concept called saturation, but saturating sets need not be finite. A characterization of right Gröbner bases with respect to right s-polynomials can be given for saturated sets, but still this characterization is not finitary, i.e., it can neither be used to decide whether a finite set is a Gröbner basis nor does it give rise to a completion procedure.

Section 4.4 and 4.5: The next stage is to study weakenings of reduction involving syntactical information on the representatives of the monoid respectively group elements. We introduce the concept of prefix reduction for arbitrary monoid rings and the concept of commutative reduction for Abelian monoid rings. In both cases we have to use a special saturation to regain the expressiveness of the right ideal congruence. Now for prefix respectively commutatively saturated sets characterizations of the respective Gröbner bases by special s-polynomials in a finitary manner are given. These characterizations can be used to decide whether a finite set is an appropriate Gröbner basis in case it is saturated in the appropriate way which again is decidable. A procedure to enumerate a prefix Gröbner basis is provided which halts in case a finite prefix Gröbner basis exists. In the commutative case finite Gröbner bases always can be computed. Interreduction is introduced to both settings and the existence of unique monic reduced Gröbner bases with respect to the respective reductions is shown.

4.1 Using Polynomials as Rules

In order to define an effective reduction in monoid and group rings we have to ensure that certain algebraic operations can be done effectively and certain algebraic questions can be solved in our structure. Therefore, we will have to restrict the presentations allowed for the monoids and groups in the approach developed here. First of all we assume that our monoids are presented by finite convergent reduction systems (compare section 2.4). This implies that our monoids have solvable word problem and hence we can decide whether two elements are equal which is essential in performing ring operations effectively. When introducing polynomial reduction and later on s-polynomials to our ring, we will find that it is important to solve the following two algebraic questions in the monoid $\mathcal{M}$:

1. Given $w_1, w_2 \in \mathcal{M}$, is there an element $m \in \mathcal{M}$ such that $w_1 = w_2 \circ m$?
2. Given $w_1, w_2 \in \mathcal{M}$, are there elements $m_1, m_2 \in \mathcal{M}$ such that $w_1 \circ m_1 = w_2 \circ m_2$?

Note that these questions in general are undecidable even for monoids with convergent presentations. However, for groups the answer of course is "yes" in both cases, as the element $m = \mathsf{inv}(w_2) \circ w_1$ is a unique solution to the first question and the set $\{(\mathsf{inv}(w_1) \circ w, \mathsf{inv}(w_2) \circ w) | w \in \mathcal{M}\}$ contains all solutions to the second question.

Since the objects of interest will be polynomials and we want to use them as rules in a reduction system, we have to introduce an ordering on the monoid elements. This ordering is required to be total and well-founded, but we will find that in general we cannot expect it to be admissible as in Buchberger's approach and most of the extensions of his ideas to other structures. Because we will assume that the monoids are presented by reduction systems, monoid elements can be viewed as syntactical objects over an alphabet. Let us be more specific now for the case that our presentations are finite convergent semi-Thue systems having a total admissible well-founded completion ordering, where the above questions 1. and 2. are solvable and the solutions computable. If not stated otherwise we will assume our monoids to be presented in this manner. Further we will assume that $\succeq_T$ is a total well-founded admissible ordering on Σ^* such that the presentation (Σ, T) is convergent with respect to $\succeq_T$. Then we will always assume that the well-founded total ordering $\succeq$ on the monoid $\mathcal{M}$ is the restriction of the ordering $\succeq_T$ to the irreducible representatives of the monoid elements. In particular this gives us $m \succ \lambda$ for all $m \in \mathcal{M}\backslash\{\lambda\}$. Moreover, since we identify the elements of $\mathcal{M}$ with the words in $\mathrm{IRR}(T)$ an essential conclusion used throughout will be that for $u, v \in \mathcal{M}$, $uv \succeq u \circ v$ holds, where uv stands for the concatenation of u and v. This follows immediately as $\succeq_T$ is admissible on Σ^*. Similar properties hold if we use convergent semi-Thue systems modulo commutativity to present commutative monoids.

In order to define reduction in $\mathbf{K}[\mathcal{M}]$ we want to use polynomials as rules. This can be done by using the well-founded ordering on the monoid to give us an ordering on the monomials of a polynomial.

Definition 4.1.1
Let $\succeq$ denote a well-founded total ordering on $\mathcal{M}$.

1. Let $p \in \mathbf{K}[\mathcal{M}]\backslash\{0\}$ be denoted by the polynomial $p = \sum_{i=1}^{n} \alpha_i \cdot w_i$, where $\alpha_i \in \mathbf{K}^*$, $w_i \in \mathcal{M}$ and $w_i \neq w_j$ for $i \neq j$. Furthermore, we assume that according to our ordering $\succeq$ we have $w_1 \succ \ldots \succ w_n$. Then we let $\mathsf{HM}(p) = \alpha_1 \cdot w_1$ denote the **head monomial**, $\mathsf{HT}(p) = w_1$ the **head term** and $\mathsf{HC}(p) = \alpha_1$ the **head coefficient** of p. $\mathsf{RED}(p) = p - \mathsf{HM}(p)$ stands for the **reduct** of p. $\mathsf{T}(p) = \{w_1, \ldots, w_n\}$ is the set of **terms** occurring in p. The polynomial p is called **monic** in case $\mathsf{HC}(p) = 1$.

2. For a set of polynomials F in $\mathbf{K}[\mathcal{M}]$ we define $\mathsf{HT}(F) = \{\mathsf{HT}(f) | f \in F\}$. $\diamond$

Moreover, we can extend the well-founded total ordering on $\mathcal{M}$ to an ordering on the elements of $\mathbf{K}[\mathcal{M}]$, which is again well-founded.

Definition 4.1.2
Let p, q be two polynomials in $\mathbf{K}[\mathcal{M}]$. Then we say p is **greater** than q with respect to an ordering $\succeq$ on $\mathcal{M}$, i.e., $p > q$, if

(i) $\mathsf{HT}(p) \succ \mathsf{HT}(q)$ or

(ii) $\mathsf{HM}(p) = \mathsf{HM}(q)$ and $\mathsf{RED}(p) > \mathsf{RED}(q)$. ◇

Note that this ordering is not total on $\mathbf{K}[\mathcal{M}]$, e.g. $5 \cdot w$ and $3 \cdot w$ are incomparable.

Lemma 4.1.3
The ordering $\geq$ on $\mathbf{K}[\mathcal{M}]$ as given in definition 4.1.2 is well-founded.

Proof :
The proof of this lemma will use a method that is known as Cantor's second diagonal argument (compare e.g. [BeWe92] chapter 4). Let us assume that $\geq$ is not well-founded on $\mathbf{K}[\mathcal{M}]$. We will show that this gives us a contradiction to the fact that the ordering $\succeq$ on $\mathcal{M}$ inducing $\geq$ is well-founded. Hence, let us suppose $f_0 > f_1 > \ldots > f_k > \ldots$, $k \in \mathbf{N}$ is a strictly descending chain in $\mathbf{K}[\mathcal{M}]$. Then we can construct a sequence of sets of pairs $\{\{(t_k, g_{kn}) | n \in \mathbf{N}\} | k \in \mathbf{N}\}$ recursively as follows: For $k = 0$ let $t_0 = \min\{\mathsf{HT}(f_i) | i \in \mathbf{N}\}$[1]. Now let $j \in \mathbf{N}$ be the least index such that we have $t_0 = \mathsf{HT}(f_j)$. Then $t_0 = \mathsf{HT}(f_{j+n})$ holds for all $n \in \mathbf{N}$ and we can set $g_{0n} = f_{j+n} - \mathsf{HM}(f_{j+n})$, i.e., $\mathsf{HT}(g_{0n}) \prec t_0$ for all $n \in \mathbf{N}$. For $k+1$ we let $t_{k+1} = \min\{\mathsf{HT}(g_{ki}) | i \in \mathbf{N}\}$ and again let $j \in \mathbf{N}$ be the least index such that $t_{k+1} = \mathsf{HT}(g_{kj})$ holds, i.e., $t_{k+1} = \mathsf{HT}(g_{k(j+n)})$ for all $n \in \mathbf{N}$. Again we set $g_{(k+1)n} = g_{k(n+j)} - \mathsf{HM}(g_{k(n+j)})$.
Then the following statements hold:

1. For all $s \in \mathsf{T}(g_{kn})$ we have $s \prec t_k$.

2. For every $k \in \mathbf{N}$, $g_{k0} > g_{k1} > \ldots$ is a strictly descending chain in $\mathbf{K}[\mathcal{M}]$.

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

q.e.d.

The choice of the well-founded ordering on the reduction ring is of great importance for the characteristics of reduction in a structure. As we have seen in the survey on Buchberger's approach, in the case of polynomial rings (which correspond to free commutative monoid rings) a special class of orderings, namely term orderings, can be used. These orderings have the following useful property which is closely related to the fact that reduction is preserved under multiplication.

Definition 4.1.4
An ordering $\succeq$ on a monoid $\mathcal{M}$ is called **monotone** (**compatible with multiplication** $\circ$) if $u \succeq v$ implies $u \circ w \succeq v \circ w$ for all $u, v, w \in \mathcal{M}$. It is called **admissible** in case we additionally have $w \succeq \lambda$ for all $w \in \mathcal{M}$. ◇

This property is essential in Buchberger's approach, since it ensures that $p \xrightarrow{*}_F 0$ implies $\alpha \cdot p * w \xrightarrow{*}_F 0$ for all $p \in \mathbf{K}[X_1, \ldots, X_n]$, $\alpha \in \mathbf{K}$ and $w \in \mathcal{T}$. Unfortunately

[1] Note that this minimum exists as we have a subset of $\mathcal{M}$ and $\succeq$ is well-founded on $\mathcal{M}$.

in general a monotone total ordering $\succeq$ on a monoid $\mathcal{M}$ cannot be expected to be well-founded, as the following remark shows.

Remark 4.1.5
Let $\mathcal{M} \neq \{\lambda\}$ be a monoid with a monotone total ordering $\succeq$.

1. Then $\mathcal{M}$ cannot contain a nontrivial element of finite order.
   To see this, suppose $w \in \mathcal{M}\backslash\{\lambda\}$ is of finite order, i.e., there are $n, m \in \mathbf{N}$, $n > m$ such that $w^n = w^m$. Without loss of generality let us assume $w \succ \lambda$. In case $n = m + 1$, then (as $\succeq$ is monotone and transitive) we get $w^m \succ w^{m-1}$ giving us $w^m = w^n = w^{m+1} \succ w^m$, contradicting our assumption. Otherwise we get $w^{n-1} \succ \ldots \succ w^{m+1} \succ w^m$ likewise giving us $w^m = w^n \succ w^m$ which is again a contradiction.

2. The ordering $\succeq$ cannot be well-founded, in case there are two elements of infinite order $u, v \in \mathcal{M}\backslash\{\lambda\}$ satisfying $u \circ v = \lambda$.
   Without loss of generality let us assume $u \succ \lambda$. Then (as $\succeq$ is monotone) we have $\lambda \succ v$, and (as $\succeq$ is transitive) $u \succ \lambda \succ v \succ \ldots \succ v^n$ for all $n \in \mathbf{N}$ gives us an infinite descending chain of elements in $\mathcal{M}$. $\diamond$

Especially non-trivial groups do not allow monotone well-founded total orderings.

Now we can move on to discuss reduction in monoid rings. We will see that in defining appropriate reductions we have to be more cautious than in defining reductions in the polynomial ring (compare section 2.3) where simply the head of a polynomial is modified in order to use the polynomial for reduction. Let us start by examining a rather natural approach to reduction. Since we are mainly interested in non-commutative structures, we will restrict ourselves to one-sided ideals and investigate right ideals and concepts for reduction using right multiplication by monomials only.

4.2 The Concept of Strong Reduction

In order to study right ideals generated by a set of polynomials it is often useful to take a look at special representations of the elements in this set. We will start with a first description here and refine this approach within the following sections. Such representations of right ideal elements can then be connected to different definitions of reduction in a monoid ring. Henceforth, let $\succeq$ denote a well-founded total ordering on $\mathcal{M}$.

Definition 4.2.1
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$. A representation

$$p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i, \text{ with } \alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$$

is called a **standard representation** of p with respect to F, if for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i * w_i)$. $\diamond$

For the reader familiar with the framework of standard and Gröbner bases, we mention that this is a natural adaption of the term "standard representation", as e.g. defined in [BeWe92] for the polynomial ring, to the case of right ideals in monoid rings. A standard representation of a polynomial p with respect to a set of polynomials F is thus a representation where all occurring terms involved are bounded by the head term of p. Note that for at least one index $1 \leq i \leq n$ we must have $\mathsf{HT}(p) = \mathsf{HT}(f_i * w_i)$ and $\mathsf{HC}(p) = \sum_{i, \mathsf{HT}(p)=\mathsf{HT}(f_i*w_i)} \alpha_i \cdot \mathsf{HC}(f_i * w_i)$. Standard representations can be used to characterize special bases of right ideals.

Definition 4.2.2
A set $F \subseteq \mathbf{K}[\mathcal{M}]$ is called a **(right) standard basis**, if every non-zero polynomial in $\mathsf{ideal}_r(F)$ has a standard representation with respect to F. $\diamond$

One way to characterize such bases arises from introducing reduction to $\mathbf{K}[\mathcal{M}]$ and a rather natural approach is to use a right multiple of a polynomial as a rule.

Definition 4.2.3
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{M}]$. We say f **strongly right reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathsf{s}}_f q$, if

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

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

We write $p \longrightarrow^{\mathsf{s}}_f$ if there is a polynomial q as defined above and p is then called strongly right reducible by f. Further, we can define $\xrightarrow{*}^{\mathsf{s}}$, $\xrightarrow{+}^{\mathsf{s}}$ and $\xrightarrow{n}^{\mathsf{s}}$ as usual. Strong right reduction by a set $F \subseteq \mathbf{K}[\mathcal{M}]$ is denoted by $p \longrightarrow^{\mathsf{s}}_F q$ and abbreviates $p \longrightarrow^{\mathsf{s}}_f q$ for some $f \in F$, which is also written as $p \longrightarrow^{\mathsf{s}}_{f \in F} q$. $\diamond$

Note that in order to strongly right reduce p, the polynomial f need not be smaller than p. The condition $\mathsf{HT}(f * w) = t$ prevents reduction with a polynomial in case $f * w = 0$, i.e., if the monomials of f eliminate each other by multiplying f with w. This might happen in case the monoid ring contains zero-divisors (compare remark 2.1.26). Further, in case we have $p \longrightarrow^{\mathsf{s}}_f q$ at the monomial $\alpha \cdot t$, then $t \notin \mathsf{T}(q)$.

Definition 4.2.4
A set of polynomials F is called **interreduced** or **reduced** with respect to $\longrightarrow^{\mathsf{s}}$ if for all $f \in F$,$f \longrightarrow^{\mathsf{s}}_F f'$ implies $f' = 0$. $\diamond$

Notice that in literature an interreduced set is often characterized by requiring that none of its elements is reducible by the other elements in the set. In our setting this no longer holds, since strongly right reducing a polynomial with *itself* need not result in zero as the following example shows.

Example 4.2.5
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a

presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b \succ c$.
Then the polynomial $a + b + c$ is strongly reducible by itself at a as follows: $a + b + c \longrightarrow^{s}_{a+b+c} a + b + c - (a + b + c) * b = a + b + c - (c + \lambda + \underline{a}) = b - \lambda$.
Moreover, since $\mathsf{ideal}_r(a + b + c) \neq \mathsf{ideal}_r(b - \lambda)$, this shows that while $f \longrightarrow^{s}_{f} f'$ implies $f' \in \mathsf{ideal}_r(f)$ the case $f \notin \mathsf{ideal}_r(f')$ is possible. ◇

This example also reveals that interreduced bases of right ideals in general need not exist: neither $\{a + b + c\}$ nor $\{a + b + c, b - \lambda\}$ are interreduced, and while $\{b - \lambda\}$ is interreduced it no longer generates $\mathsf{ideal}_r(a + b + c)$.

In order to decide, whether a polynomial f strongly right reduces a polynomial p at a monomial $\alpha \cdot t$ one has to decide whether there exist elements $s \in \mathsf{T}(p)$ and $w \in \mathcal{M}$ such that $s \circ w = \mathsf{HT}(f * w) = t$. Since this problem reduces to solving equations $s \circ \mathrm{x} = t$ in one variable x in the monoid $\mathcal{M}$ presented by (Σ, T), this problem is undecidable in general, even if $\mathcal{M}$ is presented by a convergent semi-Thue-system. Note that there can be no, one or even (infinitely) many solutions depending on $\mathcal{M}$.

Example 4.2.6
Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b$.
Then the equation $b \circ \mathrm{x} = a$ has no solution in $\mathcal{M}$, the equation $b \circ \mathrm{x} = b$ has one solution in $\mathcal{M}$, namely $\mathrm{x} = \lambda$, and the equation $a \circ \mathrm{x} = a$ has infinitely many solutions in $\mathcal{M}$, namely the set $\{b^n | n \in \mathbf{N}\}$. ◇

The following example illustrates how different monomials can become equal when modifying a polynomial in order to use it for strong right reduction.

Remark 4.2.7
Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow b\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b$. Furthermore, let f_1, f_2, p be polynomials in $\mathbf{Q}[\mathcal{M}]$ such that $f_1 = a^2 + a$, $f_2 = a^2 - a$ and $p = b + \lambda$.
Then p is strongly right reducible by f_1 at b, as $\mathsf{HT}(f_1 * b) = \mathsf{HT}(2 \cdot b) = b$ and $p \longrightarrow^{s}_{f_1} p - \frac{1}{2} \cdot f_1 * b = b + \lambda - \frac{1}{2} \cdot 2 \cdot b = \lambda$. On the other hand, although both equations $a^2 \circ \mathrm{x} = b$ and $a \circ \mathrm{x} = b$ have a solution b, we get that p is not strongly right reducible by f_2, as $f_2 * b = b - b = 0$. ◇

In case $\mathcal{M}$ is a right cancellative monoid or a group the phenomenon described in this remark can no longer occur, since then $u \circ m = v \circ m$ implies $u = v$ for all $u, w, m \in \mathcal{M}$.
Let us continue to state some of the properties strong right reduction satisfies.

Lemma 4.2.8
Let F be a set of polynomials and p, q, q_1, q_2 some polynomials in $\mathbf{K}[\mathcal{M}]$.

1. $p \longrightarrow^{s}_{F} q$ *implies* $p > q$, *in particular* $\mathsf{HT}(p) \succeq \mathsf{HT}(q)$.
2. $\longrightarrow^{s}_{F}$ *is Noetherian.*

3. $p \longrightarrow^{\mathrm{s}}_{q_1} 0$ *and* $q_1 \longrightarrow^{\mathrm{s}}_{q_2} 0$ *imply* $p \longrightarrow^{\mathrm{s}}_{q_2} 0$.

4. $\alpha \cdot p * w \stackrel{\leq 1}{\longrightarrow}^{\mathrm{s}}_{p} 0$ *for all* $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$.

Proof :

1. This follows from the fact that using a polynomial f together with $\alpha \in \mathbf{K}^*$ and $w \in \mathcal{M}$ for reduction we use $\alpha \cdot \mathsf{HM}(f * w) \longrightarrow -\alpha \cdot \mathsf{RED}(f * w)$ as a rule and we know $\mathsf{HM}(f * w) > -\mathsf{RED}(f * w)$.

2. This follows from (1), as the ordering $\geq$ on $\mathbf{K}[\mathcal{M}]$ is well-founded.

3. $p \longrightarrow^{\mathrm{s}}_{q_1} 0$ implies $p = \alpha_1 \cdot q_1 * w_1$ for some $\alpha_1 \in \mathbf{K}^*, w_1 \in \mathcal{M}$, and $q_1 \longrightarrow^{\mathrm{s}}_{q_2} 0$ implies $q_1 = \alpha_2 \cdot q_2 * w_2$ for some $\alpha_2 \in \mathbf{K}^*, w_2 \in \mathcal{M}$. Combining this information we immediately get $p \longrightarrow^{\mathrm{s}}_{q_2} 0$, as $p = \alpha_1 \cdot q_1 * w_1 = \alpha_1 \cdot (\alpha_2 \cdot q_2 * w_2) * w_1 = (\alpha_1 \cdot \alpha_2) \cdot q_2 * (w_2 \circ w_1)$ and thus $\mathsf{HT}(q_2 * (w_2 \circ w_1)) = \mathsf{HT}(p)$.

4. This follows immediately from definition 4.2.3.

q.e.d.

However, a closer inspection of strong right reduction reveals some dependencies on the monoid and some restrictions in general.

Remark 4.2.9
Let p, q, q_1 and q_2 be some polynomials in $\mathbf{K}[\mathcal{M}]$.

1. $p \longrightarrow^{\mathrm{s}}_{q_1} 0$ and $p \longrightarrow^{\mathrm{s}}_{q_2} 0$ need not imply $q_1 \longrightarrow^{\mathrm{s}}_{q_2}$ or $q_2 \longrightarrow^{\mathrm{s}}_{q_1}$.
Let us recall that $p \longrightarrow^{\mathrm{s}}_{q_1} 0$ and $p \longrightarrow^{\mathrm{s}}_{q_2} 0$ imply $p = \alpha_1 \cdot q_1 * w_1 = \alpha_2 \cdot q_2 * w_2$ for some $\alpha_1, \alpha_2 \in \mathbf{K}^*$ and $w_1, w_2 \in \mathcal{M}$. Obviously, if $\mathcal{M}$ is a group we get $q_1 = (\alpha_1^{-1} \cdot \alpha_2) \cdot q_2 * (w_2 \circ \mathsf{inv}(w_1))$ and $q_2 = (\alpha_2^{-1} \cdot \alpha_1) \cdot q_1 * (w_1 \circ \mathsf{inv}(w_2))$, i.e., $q_1 \longrightarrow^{\mathrm{s}}_{q_2} 0$ and $q_2 \longrightarrow^{\mathrm{s}}_{q_1} 0$. But for arbitrary monoids this does not hold, as it is already wrong for Buchberger's reduction in the usual polynomial ring[2].

2. $p \longrightarrow^{\mathrm{s}}_{q}$ and $q \longrightarrow^{\mathrm{s}}_{q_1} q_2$ need not imply $p \longrightarrow^{\mathrm{s}}_{\{q_1, q_2\}}$.
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, c^2 \longrightarrow \lambda\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group), with with a length-lexicographical ordering induced by $a \succ b \succ c$.
Looking at the polynomials $p = ba + b, q = bc + \lambda$ and $q_1 = ac + b$ we find $p \longrightarrow^{\mathrm{s}}_{q} p - q * ca = ba + b - (bc + \lambda) * ca = ba + b - ba - ca = -ca + b$ and $q \longrightarrow^{\mathrm{s}}_{q_1} q - q_1 * c = bc + \lambda - (ac + b) * c = bc + \lambda - a - bc = -a + \lambda =: q_2$, but $p \not\longrightarrow^{\mathrm{s}}_{\{q_1, q_2\}}$, as trying to reduce ba by q_1 or q_2 we get $q_1 * a = \underline{aca} + ba, q_1 * caba = ba + \underline{bcaba}$ and $q_2 * aba = -ba + \underline{aba}, q_2 * ba = -\underline{aba} + ba$ all violating[3] condition (a) of definition 4.2.3, i.e., there exists no $w \in \mathcal{M}$ such that $\mathsf{HT}(q_1 * w) = ba$ or $\mathsf{HT}(q_2 * w) = ba$.

[2] Take e.g. the polynomials $p = X_1 X_2$, $q_1 = X_1$ and $q_2 = X_2$.
[3] The underlined terms in the polynomial multiples are the respective head terms.

Trying to reduce b we get the same problem with $q_1 * cab = b + \underline{bcab}$, $q_2 * ab = -b + \underline{ab}$ and $q_2 * b = -\underline{ab} + b$. $\diamond$

Note that the latter property is connected to interreduction and this example states that in case a polynomial p is strongly right reducible by a polynomial q and the latter polynomial is reduced to a new polynomial q_2 by a polynomial q_1, then p need no longer be strongly right reducible by the set $\{q_1, q_2\}$. Hence, interreducing a set of polynomials might affect the set of polynomials which have been strongly right reducible by the not interreduced set. Nevertheless, strong right reduction has the essential properties which allow us to characterize a right ideal by reduction with respect to a a set of generators, e.g. the translation lemma holds and the right ideal congruence can be described by reduction.

Lemma 4.2.10
Let F be a set of polynomials and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$.

1. *Let $p - q \longrightarrow^{\mathrm{s}}_F h$. Then there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that we have $p \xrightarrow{*}^{\mathrm{s}}_F p', q \xrightarrow{*}^{\mathrm{s}}_F q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{s}}_F$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}^{\mathrm{s}}_F g$ and $q \xrightarrow{*}^{\mathrm{s}}_F g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{s}}_F h = p - q - \alpha \cdot f * w$ with $\alpha \in \mathbf{K}^*, f \in F, w \in \mathcal{M}$ and let $\mathsf{HT}(f * w) = t$, i.e., $\alpha \cdot \mathsf{HC}(f * w)$ is the coefficient of t in $p - q$. We have to distinguish three cases:
   (a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$: Then we can eliminate the term t in the polynomials p respectively q by reduction and get $p \longrightarrow^{\mathrm{s}}_f p - \alpha_1 \cdot f * w = p'$, $q \longrightarrow^{\mathrm{s}}_f q - \alpha_2 \cdot f * w = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f * w)$ and $\alpha_2 \cdot \mathsf{HC}(f * w)$ are the coefficients of t in p respectively q.
   (b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$: Then we can eliminate the term t in the polynomial p by reduction and get $p \longrightarrow^{\mathrm{s}}_f p - \alpha \cdot f * w = p'$ and $q = q'$.
   (c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$: Then we can eliminate the term t in the polynomial q by reduction and get $q \longrightarrow^{\mathrm{s}}_f q + \alpha \cdot f * w = q'$ and $p = p'$.

   In all three cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.
2. We show our claim by induction on k, where $p - q \xrightarrow{k}^{\mathrm{s}}_F 0$. In the base case $k = 0$ there is nothing to show. Hence, let $p - q \longrightarrow^{\mathrm{s}}_F h \xrightarrow{k}^{\mathrm{s}}_F 0$. Then by (1) there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}^{\mathrm{s}}_F p', q \xrightarrow{*}^{\mathrm{s}}_F q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \xrightarrow{k}^{\mathrm{s}}_F 0$ yields the existence of a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}^{\mathrm{s}}_F p' \xrightarrow{*}^{\mathrm{s}}_F g$ and $q \xrightarrow{*}^{\mathrm{s}}_F q' \xrightarrow{*}^{\mathrm{s}}_F g$.

q.e.d.

Lemma 4.2.11
Let F be a set of polynomials and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$. Then

$$p \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_{F} q \text{ if and only if } p - q \in \mathsf{ideal}_r(F).$$

Proof :

1. Using induction on k we show that $p \overset{k}{\longleftrightarrow}{}^{\mathrm{s}}_{F} q$ implies $p - q \in \mathsf{ideal}_r(F)$. In the base case $k = 0$ there is nothing to show, since $p - p = 0 \in \mathsf{ideal}_r(F)$. Thus let us assume that $\tilde{p} \overset{k}{\longleftrightarrow}{}^{\mathrm{s}}_{F} \tilde{q}$ implies $\tilde{p} - \tilde{q} \in \mathsf{ideal}_r(F)$. Then looking at $p \overset{k}{\longleftrightarrow}{}^{\mathrm{s}}_{F} p_k \longleftrightarrow^{\mathrm{s}}_{F} q$ we can distinguish two cases:

   (a) $p_k \longrightarrow^{\mathrm{s}}_{f} q$ using a polynomial $f \in F$.
   This gives us $q = p_k - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*, w \in \mathcal{M}$, and since $p - q = p - p_k + \alpha \cdot f * w$ and $p - p_k \in \mathsf{ideal}_r(F)$, we get $p - q \in \mathsf{ideal}_r(F)$.

   (b) $q \longrightarrow^{\mathrm{s}}_{f} p_k$ using a polynomial $f \in F$ can be treated similarly.

2. It remains to show that $p - q \in \mathsf{ideal}_r(F)$ implies $p \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_{F} q$. Remember that $p - q \in \mathsf{ideal}_r(F)$ gives us a representation $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ such that $\alpha_j \in \mathbf{K}^*$, $f_j \in F$, and $w_j \in \mathcal{M}$. We will show $p \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_{F} q$ by induction on m. In the base case $m = 0$ there is nothing to show. Hence, let $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$ and by our induction hypothesis $p \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_{F} q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$. Further, let $t = \mathsf{HT}(f_{m+1} * w_{m+1})$. In case $t \notin \mathsf{T}(q)$ we get $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \longrightarrow^{\mathrm{s}}_{f_{m+1}} q$ and are done. In case $t \notin \mathsf{T}(p)$ we get $p - \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \longrightarrow^{\mathrm{s}}_{f_{m+1}} p$. Thus, as $p - \alpha_{m+1} \cdot f_{m+1} * w_{m+1} = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ the induction hypothesis yields $p - \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \overset{*}{\longleftrightarrow}{}^{\mathrm{s}}_{F} q$ and hence we are done. Otherwise let $\beta_1 \neq 0$ be the coefficient of t in $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$ and $\beta_2 \neq 0$ the coefficient of t in q. This gives us a reduction step

$$\begin{aligned}
& q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1} \longrightarrow^{\mathrm{s}}_{f_{m+1}} \\
& q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1} - \beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} \cdot f_{m+1} * w_{m+1} = \\
& q - (\beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} - a_{m+1}) \cdot f_{m+1} * w_{m+1}
\end{aligned}$$

   eliminating the occurrence of the term t in $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$. Then obviously $\beta_2 = (\beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} - \alpha_{m+1}) \cdot \mathsf{HC}(f_{m+1} * w_{m+1})$ and, therefore, $q \longrightarrow^{\mathrm{s}}_{f_{m+1}} q - (\beta_1 \cdot \mathsf{HC}(f_{m+1} * w_{m+1})^{-1} - \alpha_{m+1}) \cdot f_{m+1} * w_{m+1}$, i.e., q and $q + \alpha_{m+1} \cdot f_{m+1} * w_{m+1}$ are joinable.

q.e.d.

In analogy to Buchberger's definition of Gröbner bases in commutative polynomial rings, we can now specify special bases of right ideals in monoid rings.

Definition 4.2.12
A set $G \subseteq \mathbf{K}[\mathcal{M}]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{s}}$ or a **strong Gröbner basis**, if

(i) $\stackrel{*}{\longleftrightarrow}^{\mathrm{s}}_{G} \; = \; \equiv_{\mathsf{ideal}_r(G)}$, and

(ii) $\longrightarrow^{\mathrm{s}}_{G}$ is confluent. $\diamond$

Note that unlike in Buchberger's case a polynomial itself need not be a Gröbner basis of the right ideal it generates.

Example 4.2.13
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact is a group) with with a length-lexicographical ordering induced by $a \succ b \succ c$. Further, let us consider the polynomial $p = a + b + c \in \mathbf{Q}[\mathcal{M}]$.
Then $\longrightarrow^{\mathrm{s}}_{p}$ is not confluent on $\mathsf{ideal}_r(p)$, as we can reduce $a + b + c \longrightarrow^{\mathrm{s}}_{p} b - \lambda$ using $p * b = c + \lambda + \underline{a}$ and $a + b + c \longrightarrow^{\mathrm{s}}_{p} 0$, but although $b - \lambda \in \mathsf{ideal}_r(p)$, $b - \lambda \stackrel{*}{\not\longrightarrow}^{\mathrm{s}}_{p} 0$, as for all $w \in \mathcal{M}$, $\mathsf{HT}(p * w) \neq b$. $\diamond$

The following lemma collects some natural relations between strong right reduction and standard representations.

Lemma 4.2.14
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$.

1. *Then $p \stackrel{*}{\longrightarrow}^{\mathrm{s}}_{F} 0$ implies the existence of a standard representation for p.*

2. *In case the polynomial p has a standard representation with respect to F, then p is strongly right reducible at its head monomial by F, i.e., p is top-reducible by F.*

3. *In case F is a standard basis, every non-zero polynomial p in $\mathsf{ideal}_r(F)$ is top-reducible to zero by F.*

Proof :

1. This follows directly by adding up the polynomials used in the strong right reduction steps occurring in $p \stackrel{*}{\longrightarrow}^{\mathrm{s}}_{F} 0$.

2. This is an immediate consequence of the definition of standard representations in 4.2.1 as the existence of a polynomial f in F and an element $w \in \mathcal{M}$ with $\mathsf{HT}(f * w) = \mathsf{HT}(p)$ is guaranteed.

3. We show that every non-zero polynomial $p \in \mathsf{ideal}_r(F)\backslash\{0\}$ is top-reducible to zero using F by induction on $\mathsf{HT}(p)$. Let $\mathsf{HT}(p) = \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}_r(F)\backslash\{0\}\}$. Then, as $p \in \mathsf{ideal}_r(F)$ and F is a standard basis, we have $p = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ and $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i * w_i)$ for all $1 \leq i \leq k$. Without loss of generality, let $\mathsf{HT}(p) = \mathsf{HT}(f_1 * w_1)$. Hence, p is strongly right reducible

by f_1. Let $p \longrightarrow^{\mathsf{s}}_{f_1} q$, i.e., $q = p - \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$, and by the definition of strong right reduction the term $\mathsf{HT}(p)$ is eliminated from p implying that $\mathsf{HT}(q) \prec \mathsf{HT}(p)$ as $q < p$. Hence, as $q \in \mathsf{ideal}_r(F)$ and as $\mathsf{HT}(p)$ was minimal among the head terms of the non-zero elements in the right ideal generated by F, this implies $q = 0$, and, therefore, p is strongly right top-reducible to zero by f_1 in one step. On the other hand, in case $\mathsf{HT}(p) \succ \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}_r(F) \backslash \{0\}\}$, by the same arguments used before we can reduce p to a polynomial q with $\mathsf{HT}(q) \prec \mathsf{HT}(p)$, and, thus, by our induction hypothesis we know that q is top-reducible to zero. Therefore, as the reduction step $p \longrightarrow^{\mathsf{s}}_{f_1} q$ takes place at the head term of p, p is also top-reducible to zero.

q.e.d.

Now we can prove how standard representations can be used to characterize strong Gröbner bases, and that in fact standard bases are strong Gröbner bases.

Theorem 4.2.15
For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *F is a strong Gröbner basis.*
2. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \stackrel{*}{\longrightarrow}^{\mathsf{s}}_F 0$.*
3. *F is a standard basis.*

Proof :
$1 \Longrightarrow 2$: By the definition of strong Gröbner bases in 4.2.12 we know that $g \in \mathsf{ideal}_r(F)$ implies $g \stackrel{*}{\longleftrightarrow}^{\mathsf{s}}_F 0$, and since $\longrightarrow^{\mathsf{s}}_F$ is confluent and 0 irreducible, $g \stackrel{*}{\longrightarrow}^{\mathsf{s}}_F 0$ follows immediately.

$2 \Longrightarrow 3$: This follows directly from lemma 4.2.14.

$3 \Longrightarrow 1$: In order to show that F is a strong Gröbner basis, we have to prove two subgoals: $\stackrel{*}{\longleftrightarrow}^{\mathsf{s}}_F = \equiv_{\mathsf{ideal}_r(F)}$ follows immediately from lemma 4.2.11. It remains to show that $\longrightarrow^{\mathsf{s}}_F$ is confluent. Since $\longrightarrow^{\mathsf{s}}_F$ is Noetherian, we only have to prove local confluence. Let us suppose there exist polynomials $g, g_1, g_2 \in \mathbf{K}[\mathcal{M}]$ such that we have $g \longrightarrow^{\mathsf{s}}_F g_1$, $g \longrightarrow^{\mathsf{s}}_F g_2$ and $g_1 \neq g_2$. Then $g_1 - g_2 \in \mathsf{ideal}_r(F)$ and, therefore, is top-reducible to zero by F as a result of lemma 4.2.14. Thus lemma 4.2.10 provides the existence of a polynomial $h \in \mathbf{K}[\mathcal{M}]$ such that $g_1 \stackrel{*}{\longrightarrow}^{\mathsf{s}}_F h$ and $g_2 \stackrel{*}{\longrightarrow}^{\mathsf{s}}_F h$, i.e., $\longrightarrow^{\mathsf{s}}_F$ is confluent.

q.e.d.

In accordance with the terminology used in Buchberger's approach to describe Gröbner bases we define critical pairs of polynomials with respect to strong right reduction.

Definition 4.2.16
Given two non-zero polynomials $p_1, p_2 \in \mathbf{K}[\mathcal{M}]$[4], every pair $w_1, w_2 \in \mathcal{M}$ such that $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_2 * w_2)$, defines a **strong s-polynomial**

$$\mathsf{spol}_s(p_1, p_2, w_1, w_2) = \mathsf{HC}(p_1 * w_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2 * w_2)^{-1} \cdot p_2 * w_2.$$

Let $U_{p_1,p_2} \subseteq \mathcal{M} \times \mathcal{M}$ be the set containing *all* such pairs $w_1, w_2 \in \mathcal{M}$. $\diamond$

A strong s-polynomial will be called non-trivial in case it is non-zero and notice that for non-trivial s-polynomials we always have $\mathsf{HT}(\mathsf{spol}(p_1, p_2, w_1, w_2)) \prec \mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_2 * w_2)$. The set U_{p_1,p_2} is contained in the set of all solutions to the equations in two variables of the form $u \circ \mathrm{x} = v \circ \mathrm{y}$ where $u \in \mathsf{T}(p_1)$ and $v \in \mathsf{T}(p_2)$. It can be empty, finite or even infinite. As might be expected, we can give a criterion that implies confluence for strong right reduction in terms of strong s-polynomials.

Theorem 4.2.17
For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}^{\mathrm{s}}_F 0$.*
2. *For all not necessarily different polynomials $f_k, f_l \in F$ and every corresponding pair $(w_k, w_l) \in U_{f_k,f_l}$ we have $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{s}}_F 0$.*

Proof :
$1 \Longrightarrow 2$: Let $(w_k, w_l) \in U_{f_k,f_l}$ give us a strong s-polynomial belonging to the polynomials f_k, f_l. Then by definition 4.2.16 we get

$$\mathsf{spol}_s(f_k, f_l, w_k, w_l) = \mathsf{HC}(f_k * w_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l * w_l)^{-1} \cdot f_l * w_l \in \mathsf{ideal}_r(F)$$

and, thus, $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{s}}_F 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero polynomial $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{s}}_F$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{s}}_F h'$ implies $h' \in \mathsf{ideal}_r(F)$. Hence, as $\longrightarrow^{\mathrm{s}}_F$ is Noetherian, it suffices to show that every $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{s}}_F$-reducible. Now, let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*$, $f_j \in F$, and $w_j \in \mathcal{M}$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{M}$ we define $t = \max\{\mathsf{HT}(f_j * w_j) \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{s}}_F$-reducible. So by lemma 4.2.14 it is sufficient to show that g has a standard representation, as this implies that g is top-reducible using F. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[5]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[6] such

[4] Notice that $p_1 = p_2$ is possible.

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

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

that $\mathsf{HT}(f_k * w_k) = \mathsf{HT}(f_l * w_l)$. By definition 4.2.16 we have a strong s-polynomial $\mathsf{spol}_s(f_k, f_l, w_k, w_l) = \mathsf{HC}(f_k * w_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l * w_l)^{-1} \cdot f_l * w_l$ corresponding to this overlap. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \neq 0$[7]. Hence, the reduction sequence $\mathsf{spol}_s(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{s}_{F} 0$ results in a standard representation $\mathsf{spol}_s(f_k, f_l, w_k, w_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbf{K}^*, h_i \in F$, and $v_i \in \mathcal{M}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_s(f_k, f_l, w_k, w_l)) \prec t$. This gives us:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \;& \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}_s(f_k, f_l, w_k, w_l)} \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i) \qquad (4.1)
\end{aligned}$$

where $\beta_k = \mathsf{HC}(f_k * w_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l * w_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (4.1) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

q.e.d.

Note that this theorem, although characterizing a strong Gröbner basis by strong s-polynomials, does not give a finite test to check whether a set is a strong Gröbner basis, since in general infinitely many strong s-polynomials have to be considered. The following example shows how already two polynomials p_1, p_2 can cause infinitely many critical situations.

Example 4.2.18
Let $\Sigma = \{a, b, c, d, e, f\}$ and $T = \{abc \longrightarrow ba, fbc \longrightarrow bf, bad \longrightarrow e\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c \succ d \succ e \succ f$. Further consider two polynomials $p_1 = a + f, p_2 = bf + a \in \mathbf{Q}[\mathcal{M}]$.
Then we get infinitely many critical situations $\mathsf{HT}(p_1 * (bc)^i dw) = f \circ (bc)^i dw = bf \circ (bc)^{i-1} dw = \mathsf{HT}(p_2 * (bc)^{i-1} dw)$, where $i \in \mathbf{N}^+, w \in \mathcal{M}$, resulting in infinitely many strong s-polynomials

$$\mathsf{spol}_s(p_1, p_2, (bc)^i dw, (bc)^{i-1} dw) = (a + f) * (bc)^i dw - (bf + a) * (bc)^{i-1} dw$$

and $U_{p_1,p_2} = \{((bc)^i dw, (bc)^{i-1} dw) | i \in \mathbf{N}^+, w \in \mathcal{M}\}$. $\diamond$

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

Localization of critical situations might be very hard. As the previous example shows, the set U_{p_1,p_2} need not have a "suitable" finite basis, i.e., there need not exist a finite set $B \subseteq U_{p_1,p_2}$ such that for every pair $(w_1, w_2) \in U_{p_1,p_2}$ there exists a pair $(u_1, u_2) \in B$ and an element $w \in \mathcal{M}$ with $u_1 \circ w = w_1$ and $u_2 \circ w = w_2$.

One way to reduce the set of critical situations that have to be considered is to weaken reduction. The key idea is that for two reduction relations $\longrightarrow^1$ and $\longrightarrow^2$ on a set $\mathcal{E}$ such that $\longrightarrow^1 \subseteq \longrightarrow^2$ and $\stackrel{*}{\longleftrightarrow}^1 = \stackrel{*}{\longleftrightarrow}^2$, the confluence of $\longrightarrow^1$ on $\mathcal{E}$ implies the confluence of $\longrightarrow^2$ on $\mathcal{E}$. The next section will introduce a way to weaken strong right reduction.

4.3 The Concept of Right Reduction

In the previous section we have introduced standard representations to monoid rings and it was shown how they are related to a special reduction. We will now slightly extend this definition in order to reflect a possible weakening of strong right reduction and study what can be gained by this approach.

Definition 4.3.1
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$. A representation

$$p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i, \text{ with } \alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$$

is called a **stable standard representation** of p with respect to F, if for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ w_i \succeq \mathsf{HT}(f_i * w_i)$. A set $F \subseteq \mathbf{K}[\mathcal{M}]$ is called a **stable standard basis**, if every non-zero polynomial in $\mathsf{ideal}_r(F)$ has a stable standard representation with respect to F. $\diamond$

Notice that in this definition $\mathsf{HT}(f_i) \circ w_i \succeq \mathsf{HT}(f_i * w_i)$ need not imply $\mathsf{HT}(f_i) \circ w_i = \mathsf{HT}(f_i * w_i)$ as $\mathsf{HT}(f_i) \circ w_i \notin \mathsf{T}(f_i * w_i)$ is possible, e.g. if $\mathcal{M}$ is not cancellative. Nevertheless, in case $\mathsf{HT}(p) = \mathsf{HT}(f_i * w_i)$ we have $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ w_i$ and this situation occurs for at least one polynomial in the representation. In stable standard bases we can refine the concept of stable standard representations and gain more information on the head terms of the multiples of the polynomials involved in the respective representation. This is due to the fact that if we have $\mathsf{HT}(f_i) \circ w_i \succeq \mathsf{HT}(f_i * w_i)$, but $\mathsf{HT}(f_i) \circ w_i \neq \mathsf{HT}(f_i * w_i)$, i.e., $\mathsf{HT}(f_i) \circ w_i \notin \mathsf{T}(f_i * w_i)$, then we again have a stable standard representation for this multiple as it belongs to the right ideal generated by F. This is reflected in the proof of the following lemma.

Lemma 4.3.2
Let F be a stable standard basis in $\mathbf{K}[\mathcal{M}]$. Then every non-zero polynomial p in $\mathsf{ideal}_r(F)$ has a stable standard representation $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F$, and $w_i \in \mathcal{M}$ such that for all $1 \leq i \leq n$ we even have

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ w_i = \mathsf{HT}(f_i * w_i).$$

Proof :
Let p be a non-zero polynomial in $\mathsf{ideal}_r(F)$. We show our claim by induction on $\mathsf{HT}(p)$. In the base case we can assume $\mathsf{HT}(p) = \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}_r(F)\backslash\{0\}\}$. Since F is a stable standard basis, we know that the polynomial p has a stable standard representation $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ such that for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ w_i \succeq \mathsf{HT}(f_i * w_i)$. It remains to show that we can even achieve a representation where $\mathsf{HT}(f_i) \circ w_i = \mathsf{HT}(f_i * w_i)$. Without loss of generality we can assume that $\mathsf{HT}(p) = \mathsf{HT}(f_1) \circ w_1 = \mathsf{HT}(f_1 * w_1)$. Then the head term of p can be eliminated by subtracting an appropriate right multiple of f_1. Looking at the polynomial $h = p - \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$ we find that h lies in the right ideal generated by F and, since $\mathsf{HT}(p)$ is minimal and we find $\mathsf{HT}(h) \prec \mathsf{HT}(g)$, we can conclude that $h = 0$. Thus p has a stable standard representation $p = \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$ of the desired form. Now let us suppose $\mathsf{HT}(p) \succ \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}_r(F)\backslash\{0\}\}$. Then again resulting from the existence of a stable standard representation for p, there exists a polynomial $f_1 \in F$ such that $\mathsf{HT}(p) = \mathsf{HT}(f_1) \circ w_1 = \mathsf{HT}(f_1 * w_1)$ for some $w_1 \in \mathcal{M}$. Hence looking at the polynomial $h = p - \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$ we know that h lies in the right ideal generated by F and since $\mathsf{HT}(h) \prec \mathsf{HT}(p)$ either $h = 0$, giving us $p = \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$ or our induction hypothesis yields the existence of a stable standard representation of the desired form for h, say $h = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j$, with $\beta_j \in \mathbf{K}^*, g_j \in F$, $v_j \in \mathcal{M}$. Thus we have a stable standard representation of the polynomial p, namely $p = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j + \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$, which satisfies our requests.

q.e.d.

Similar as standard representations correspond to strong right reduction, stable standard representations correspond to a weakening of strong right reduction. Instead of using all right multiples of a polynomial by monomials as rules we restrict ourselves to those right multiples of a polynomial which allow the head term of the polynomial to keep its head position. Hence, reduction defined in this way can be called "stable".

Definition 4.3.3
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{M}]$. We say f **right reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{r}}_{f} q$, if

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

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

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

In case f right reduces p to q at the monomial $\alpha \cdot t$, then $t \notin \mathsf{T}(q)$. Furthermore, as in lemma 4.2.8, we have $p > q$, right reduction is Noetherian, and $p \longrightarrow^{\mathrm{r}}_{q_1} 0$ and $q_1 \longrightarrow^{\mathrm{r}}_{q_2} 0$ imply $p \longrightarrow^{\mathrm{r}}_{q_2} 0$.

Defining interreduced sets with respect to right reduction we have to be careful as in the case of strong right reduction.

Definition 4.3.4
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ **interreduced** or **reduced** with respect to $\longrightarrow^{\mathrm{r}}$, if for all $f \in F$, $f \longrightarrow^{\mathrm{r}}_{F} f'$ implies $f' = 0$. $\diamond$

Again right reducing a polynomial with itself need not result in zero and interreduced bases for right ideals need not exist.

Example 4.3.5
Let $\Sigma = \{a, b, c, d\}$ and $T = \{ab \longrightarrow c, b^2 \longrightarrow \lambda, cb \longrightarrow d\}$ be a presentation of a cancellative monoid with a length-lexicographical ordering induced by $a \succ b \succ c \succ d$. Then the polynomial $a+b+c$ is right reducible by itself as follows: $a+b+c \longrightarrow^{\mathrm{r}}_{a+b+c} a+b+c-(a+b+c)*b = a+b+c-(\underline{c}+\lambda+d) = a+b-d-\lambda$. $\diamond$

Note that we only use $\mathsf{HM}(f) \longrightarrow -\mathsf{RED}(f)$ as a rule in case we have $\mathsf{HT}(f*w) = \mathsf{HT}(f) \circ w$. We cannot always use $\mathsf{HM}(f) \longrightarrow -\mathsf{RED}(f)$, since then reduction would no longer be Noetherian, i.e., infinite reduction sequences could arise. This is due to the fact that multiplying f by an element $w \in \mathcal{M}$ can cause $\mathsf{HM}(f) \circ w < \mathsf{RED}(f) * w$. The following example illustrates this phenomenon.

Example 4.3.6
Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow \lambda, ba \longrightarrow \lambda\}$ be a presentation of a group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b$.
Suppose we use a polynomial f itself as a rule $\mathsf{HM}(f) \longrightarrow -\mathsf{RED}(f)$, i.e., in order to reduce a monomial $\alpha \cdot t$ we just require the existence of $w \in \mathcal{M}$ such that $t = \mathsf{HT}(f) \circ w$ similar to Buchberger's reduction in definition 2.3.4. Then we could right reduce the polynomial $b^2 + 1 \in \mathbf{Q}[\mathcal{M}]$ at the monomial b^2 by the polynomial $a + b$ as $b^2 = a \circ b^3$. This would give us:

$$b^2 + 1 \longrightarrow_{a+b} b^2 + 1 - (a + b) * b^3 = -b^4 + 1$$

and the polynomial $-b^4 + 1$ likewise would be reducible by $a + b$ at the monomial b^4 causing an infinite reduction sequence. $\diamond$

Hence right reduction using a polynomial p corresponds to the following set of rules $\{\alpha \cdot \mathsf{HM}(p*w) \longrightarrow (-\alpha) \cdot \mathsf{RED}(p*w) \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}, \mathsf{HT}(p*w) = \mathsf{HT}(p) \circ w\}$, while strong reduction corresponds to the set $\{\alpha \cdot \mathsf{HM}(p*w) \longrightarrow (-\alpha) \cdot \mathsf{RED}(p*w) \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}, p*w \neq 0\}$. Looking at the expressiveness of right reduction we find that while item 3 of lemma 4.2.8 holds for our weaker form of reduction, i.e., $p \longrightarrow^{\mathrm{r}}_{q_1} 0$ together with $q_1 \longrightarrow^{\mathrm{r}}_{q_2} 0$ yields $p \longrightarrow^{\mathrm{r}}_{q_2} 0$, we no longer have $\alpha \cdot p * w \xrightarrow{\leq 1}{}^{\mathrm{r}}_{p} 0$ for

$\alpha \in \mathbf{K}^*, p \in \mathbf{K}[\mathcal{M}]$ and $w \in \mathcal{M}$. Reviewing example 4.3.6 we find that $(a+b)*b = b^2+1$ is not right reducible by $a+b$. Similar to the case of strong right reduction, $p \longrightarrow^{\mathrm{r}}_{q}$ and $q \longrightarrow^{\mathrm{r}}_{q_1} q_2$ need not imply $p \longrightarrow^{\mathrm{r}}_{\{q_1,q_2\}}$ as the following example shows.

Example 4.3.7
Let $\Sigma = \{a,b,c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b \succ c$.
Looking at the polynomials $p = ba + b, q = a + \lambda$ and $q_1 = c^2 + b \in \mathbf{Q}[\mathcal{M}]$ we get $p \longrightarrow^{\mathrm{r}}_{q} p - q * ca = ba + b - (a+\lambda) * ca = ba + b - ba - ca = -ca + b$ and $q \longrightarrow^{\mathrm{r}}_{q_1} q - q_1 * bc = a + \lambda - (c^2+b) * bc = a + \lambda - a - c = -c + \lambda = q_2$, but $p \not\longrightarrow^{\mathrm{r}}_{\{q_1,q_2\}}$.
Trying to reduce ba by q_1 or q_2 we get $q_1 * bc^2a = ba + \underline{c^2a}$ and $q_2 * bca = -ba + \underline{bca}$ both violating condition (a) of definition 4.3.3. The same happens trying to reduce b, as $q_1 * bc^2 = b + \underline{c^2}$ and $q_2 * bc = -b + \underline{bc}$. $\diamond$

Nevertheless, an essential property for reduction to allow a characterization of Gröbner bases by s-polynomials is still true, as an analogon to lemma 4.2.10 holds for right reduction.

Lemma 4.3.8
Let F be a set of polynomials and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$.

1. *Let $p - q \longrightarrow^{\mathrm{r}}_{F} h$. Then there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that we have $p \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} p', q \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{r}}_{F}$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} g$ and $q \overset{*}{\longrightarrow}^{\mathrm{r}}_{F} g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{r}}_{F} h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*, f \in F, w \in \mathcal{M}$ and $\mathsf{HT}(f * w) = \mathsf{HT}(f) \circ w = t$, i.e., $\alpha \cdot \mathsf{HC}(f * w)$ is the coefficient of t in $p - q$. We have to distinguish three cases:
   (a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$: Then we can eliminate the term t in the polynomials p respectively q by right reduction and get $p \longrightarrow^{\mathrm{r}}_{f} p - \alpha_1 \cdot f * w = p'$, $q \longrightarrow^{\mathrm{r}}_{f} q - \alpha_2 \cdot f * w = q'$, and $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f * w)$ and $\alpha_2 \cdot \mathsf{HC}(f * w)$ are the coefficients of t in p respectively q.
   (b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$: Then we can eliminate the term t in the polynomial p by right reduction and get $p \longrightarrow^{\mathrm{r}}_{f} p - \alpha \cdot f * w = p'$ and $q = q'$.
   (c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$: Then we can eliminate the term t in the polynomial q by right reduction and get $q \longrightarrow^{\mathrm{r}}_{f} q + \alpha \cdot f * w = q'$ and $p = p'$.

   In all three cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

2. We show our claim by induction on k, where $p - q \xrightarrow{k}{}^{\mathrm{r}}_F 0$. In the base case $k = 0$ there is nothing to show. Thus let $p - q \longrightarrow^{\mathrm{r}}_F h \xrightarrow{k}{}^{\mathrm{r}}_F 0$. Then by (1) there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_F p', q \xrightarrow{*}{}^{\mathrm{r}}_F q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \xrightarrow{k}{}^{\mathrm{s}}_F 0$ yields the existence of a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{r}}_F p' \xrightarrow{*}{}^{\mathrm{r}}_F g$ and $q \xrightarrow{*}{}^{\mathrm{r}}_F q' \xrightarrow{*}{}^{\mathrm{r}}_F g$.

q.e.d.

But, unlike strong right reduction, right reduction no longer captures the right ideal congruence.

Lemma 4.3.9
Let F be a set of polynomials and p, q some polynomials in $\mathbf{K}[\mathcal{M}]$. Then $p \xleftrightarrow{*}{}^{\mathrm{r}}_F q$ implies $p - q \in \mathsf{ideal}_r(F)$ but not vice versa. $\square$

Example 4.3.10
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b \succ c$.
Inspecting the polynomials $p = a+b+c, q = b-\lambda \in \mathbf{Q}[\mathcal{M}]$ and the set $F = \{a+b+c\} \subseteq \mathbf{Q}[\mathcal{M}]$ we get $p - q = a + c + \lambda = (a + b + c) * b \in \mathsf{ideal}_r(F)$, but $a + b + c \not\xleftrightarrow{*}{}^{\mathrm{r}}_F b - \lambda$. To prove this claim, let us assume $a + b + c \xleftrightarrow{*}{}^{\mathrm{r}}_F b - \lambda$. Then, since $a + b + c \longrightarrow^{\mathrm{r}}_F 0$, we get $b - \lambda \xleftrightarrow{*}{}^{\mathrm{r}}_F 0$. Let $n \in \mathbf{N}^+$ be minimal such that $b - \lambda \xleftrightarrow{n}{}^{\mathrm{r}}_F 0$. As $b - \lambda \not\longrightarrow^{\mathrm{r}}_F 0$ we know $n > 1$. Thus, let us look at the sequence

$$b - \lambda =: p_0 \longleftrightarrow^{\mathrm{r}}_F p_1 \longleftrightarrow^{\mathrm{r}}_F \ldots \longleftrightarrow^{\mathrm{r}}_F p_{n-1} \longleftrightarrow^{\mathrm{r}}_F 0,$$

where for all $1 \leq i \leq n-1$, $p_i = p_{i-1} + \alpha_i \cdot (a + b + c) * w_i$, $\alpha_i \in \mathbf{K}^*, w_i \in \mathcal{M}$ and $\mathsf{HT}((a+b+c)*w_i) = a \circ w_i$. Further let $t = \max\{\mathsf{HT}(p_i) \mid 1 \leq i \leq n-1\}$. Then $t \succ b$, as $\mathsf{HT}((a+b+c)*w) \succ b$ for all $w \in \mathcal{M}$. Let p_l be the first polynomial with $\mathsf{HT}(p_l) = t$, i.e., $\mathsf{HT}(p_j) \prec t$ for all $j < l$, and let p_{l+k} be the next polynomial, where the occurrence of t is changed. Since $\mathsf{HT}((a+b+c)*w_{l+k}) = a \circ w_{l+k} = t = a \circ w_l = \mathsf{HT}((a+b+c)*w_l)$ and (Σ, T) presents a group, we can conclude $w_{l+k} = w_l$. Further our transformation sequence is supposed to be minimal, i.e., t is not changed by the reductions taking place in the sequence $p_l \xleftrightarrow{k-1}{}^{\mathrm{r}}_F p_{l+k-1}$. But then, eliminating p_l and substituting p_{l+j} by $p'_{l+j} = p_{l+j} - \alpha_l \cdot (a+b+c)*w_l$ for all $1 \leq j < k$ gives us a shorter sequence $b - \lambda \xleftrightarrow{n-1}{}^{\mathrm{r}}_F 0$ contradicting our assumption. $\diamond$

Obviously for a set of polynomials F we have $\longrightarrow^{\mathrm{r}}_F \subseteq \longrightarrow^{\mathrm{s}}_F$, but as seen in example 4.3.10 in general we cannot expect $\xleftrightarrow{*}{}^{\mathrm{r}}_F = \xleftrightarrow{*}{}^{\mathrm{s}}_F$ to hold and right reduction does not capture the right ideal congruence in general. To overcome this problem we will use special sets of polynomials for reduction. The following lemma shows that for special bases of right ideals right reduction corresponds to the right ideal congruence.

Lemma 4.3.11
Let F be a stable standard basis and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$. Then

$$p \xleftrightarrow{*}^{\mathrm{r}}_{F} q \text{ if and only if } p - q \in \mathsf{ideal}_r(F).$$

Proof :
In order to prove our claim we have to show two subgoals. The inclusion $\xleftrightarrow{*}^{\mathrm{r}}_{F} \subseteq \equiv_{\mathsf{ideal}_r(F)}$ is an immediate consequence of the definition of right reduction and can be shown by induction as in lemma 4.2.11. To prove the converse inclusion $\equiv_{\mathsf{ideal}_r(F)} \subseteq \xleftrightarrow{*}^{\mathrm{r}}_{F}$ we have to use some additional information. Remember that $p \equiv_{\mathsf{ideal}_r(F)} q$ implies $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$, where $\alpha_j \in \mathbf{K}^*, f_j \in F$, and $w_j \in \mathcal{M}$. As every multiple $f_j * w_j$ lies in $\mathsf{ideal}_r(F)$ and F is a stable standard basis, by lemma 4.3.2, we can assume $\mathsf{HT}(f_j * w_j) = \mathsf{HT}(f_j) \circ w_j$ for all polynomials occurring in the sum. Using these assumptions the proof of our claim can now be accomplished by induction on m as in lemma 4.2.11.

q.e.d.

Given an arbitrary set of polynomials, we now intend to enrich the set of polynomials used for reduction in order to describe the right ideal congruence by right reduction. This process will be called **saturation**.

Definition 4.3.12
A set of polynomials $F \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}\}$ is called a **saturating set** for a polynomial $p \in \mathbf{K}[\mathcal{M}]$, if for all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$, in case $\alpha \cdot p * w \neq 0$ then $\alpha \cdot p * w \longrightarrow^{\mathrm{r}}_{F} 0$ holds. Let $\mathcal{SAT}(p)$ denote the family of all saturating sets for p. ⋄

Note that in defining saturating sets we demand right reducibility to zero in *one* step in case the multiple is non-zero. This is done to have some equivalent for the situation $\alpha \cdot p * w \xrightarrow{\leq 1}^{\mathrm{s}}_{p} 0$ (compare lemma 4.2.8) respectively $\alpha \cdot p * w \longrightarrow^{\mathrm{b}}_{p} 0$ in Buchberger's approach. Furthermore, since $\mathbf{K}$ is a field it is sufficient to demand $p * w \xrightarrow{\leq 1}^{\mathrm{r}}_{F} 0$ for all $w \in \mathcal{M}$.

Let us now proceed by inspecting how saturating a polynomial reveals a natural connection between strong right reduction and right reduction.

Lemma 4.3.13
Let f, g, p be some polynomials in $\mathbf{K}[\mathcal{M}]$ and $S \in \mathcal{SAT}(p)$ a saturating set for p. Then

$$f \longrightarrow^{\mathrm{s}}_{p} g \text{ if and only if } f \longrightarrow^{\mathrm{r}}_{S} g.$$

Proof :

1. Suppose we have $f \longrightarrow^{\mathrm{s}}_{p} g$ at a monomial $\alpha \cdot t$, i.e., $g = f - \alpha \cdot \mathsf{HC}(p * w)^{-1} \cdot p * w$ for some $w \in \mathcal{M}$ and $\mathsf{HT}(p * w) = t$. Since $p * w \longrightarrow^{\mathrm{r}}_{S} 0$ there exists a polynomial $p_1 \in S$ such that $p * w = \beta \cdot p_1 * w_1$ for some $\beta \in \mathbf{K}^*$, $w_1 \in \mathcal{M}$. Further $t = \mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_1) \circ w_1$ implies $f \longrightarrow^{\mathrm{r}}_{p_1 \in S} g$.

2. Suppose $f \longrightarrow^{\mathrm{r}}_{p_1 \in S} g$, i.e., $g = f - \alpha \cdot p_1 * w_1$ for some $\alpha \in \mathbf{K}^*, w_1 \in \mathcal{M}$. Since $p_1 \in S$ we have $\beta \in \mathbf{K}^*$, $w_2 \in \mathcal{M}$ such that $p_1 = \beta \cdot p * w_2$. Further $\mathsf{HT}(p_1) \circ w_1 = \mathsf{HT}(p_1 * w_1) = \mathsf{HT}((p * w_2) * w_1) = \mathsf{HT}(p * (w_2 \circ w_1))$ implies $f \longrightarrow^{\mathrm{s}}_{p} g$.

q.e.d.

The following lemmata establish that saturation indeed is a well-defined concept to repair some defects of right reduction, i.e., the right ideal generated by p is the same as the right ideal generated by a saturating set of p and right reduction using a saturating set for a polynomial captures the right ideal generated by this polynomial.

Lemma 4.3.14
Let p be a polynomial in $\mathbf{K}[\mathcal{M}]$ and $S_1, S_2 \in \mathcal{SAT}(p)$ two saturating sets for p. Then

$$\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_1} \; = \; \stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_2} .$$

Proof :
We restrict ourselves to proving $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_1} \subseteq \stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_2}$ by induction on k for $\stackrel{k}{\longleftrightarrow}^{\mathrm{r}}_{S_1}$ since the case $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_2} \subseteq \stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_1}$ is symmetric. In the base case $k = 0$ there is nothing to show. Thue let us assume $\stackrel{k}{\longleftrightarrow}^{\mathrm{r}}_{S_1} \subseteq \stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_2}$ and $p_0 \stackrel{k}{\longleftrightarrow}^{\mathrm{r}}_{S_1} p_k \longleftrightarrow^{\mathrm{r}}_{S_1} p_{k+1}$. Without loss of generality we further suppose $p_k \longrightarrow^{\mathrm{r}}_{q} p_{k+1}$ with $q \in S_1$ (the other case is similar). Then $p_{k+1} = p_k - \alpha \cdot q * w$ for $\alpha \in \mathbf{K}^*, w \in \mathcal{M}$, and since S_2 is a saturating set for p we have a polynomial $q_1 \in S_2$ with $q * w \longrightarrow^{\mathrm{r}}_{q_1 \in S_2} 0$, i.e., $q * w = \beta \cdot q_1 * w_1$, where $\beta \in \mathbf{K}^*$, $w_1 \in \mathcal{M}$ and $p_{k+1} = p_k - (\alpha \cdot \beta) \cdot q_1 * w_1$. Therefore we get $p_k \longrightarrow^{\mathrm{r}}_{q_1 \in S_2} p_{k+1}$ and our induction hypothesis yields $p_0 \stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S_2} p_k \longleftrightarrow^{\mathrm{r}}_{S_2} p_{k+1}$.

q.e.d.

Lemma 4.3.15
Let $S \in \mathcal{SAT}(p)$ be a saturating set for a polynomial $p \in \mathbf{K}[\mathcal{M}]$. Then

$$\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S} \; = \; \equiv_{\mathsf{ideal}_r(p)} .$$

Proof :
This is a consequence of lemma 4.3.13, as we have $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{S} \; = \; \stackrel{*}{\longleftrightarrow}^{\mathrm{s}}_{p} \; = \; \equiv_{\mathsf{ideal}_r(p)}$. q.e.d.

The next lemma states that we can in some sense "simplify" saturating sets to "minimal" saturating sets such that no polynomial in the set is right reducible to zero in one step by the remaining polynomials.

Lemma 4.3.16
Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$ and $S \in \mathcal{SAT}(p)$ a saturating set for p.
If there is a polynomial $q \in S$ such that $q \longrightarrow^{\mathrm{r}}_{S \backslash \{q\}} 0$, then $S \backslash \{q\}$ is again a saturating set for p.

Proof :
This is an immediate consequence of the fact that $p \longrightarrow^{\mathrm{r}}_{q_1} 0$ and $q_1 \longrightarrow^{\mathrm{r}}_{q_2} 0$ imply $p \longrightarrow^{\mathrm{r}}_{q_2} 0$ (compare statement 3 of lemma 4.2.8 which also holds for right reduction).

q.e.d.

On the contrary, the property of being a saturating set for a polynomial is in general destroyed when interreducing it with respect to right reduction.

Example 4.3.17
Let $\Sigma = \{a\}$ and $T = \{a^3 \longrightarrow \lambda\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group).
Looking at the polynomial $p = a^2 + \lambda$ we find that the set $S = \{a^2 + \lambda, a + \lambda\}$ is a saturating set for p. Furthermore, we have $p \longrightarrow^{\mathrm{r}}_{a+\lambda} a^2 + \lambda - (a+\lambda) * a = a^2 + \lambda - a^2 - a = -a + \lambda \longrightarrow^{\mathrm{r}}_{a+\lambda} -a + \lambda - (-1) \cdot (a + \lambda) = 2 \cdot \lambda$, but the set $S' = \{a + \lambda, 2 \cdot \lambda\}$ is no longer a saturating set for p. $\diamond$

We move on now to examine how saturating sets can be constructed. Obviously the set $\{p * w \mid w \in \mathcal{M}\}$ itself is a trivial saturating set for the polynomial p. Since it is recursively enumerable, it can be used to specify enumerating procedures for saturating sets. Because in general such enumerations will not terminate we have to try to find criteria to decide whether a set is a saturating set for a polynomial without having to check all right multiples. We are interested in a systematic way to distinguish what terms can be brought to head position. Since in order to bring another term to head position in multiplying the head term a cancellation (in computing the product using the presenting semi-Thue system) has to take part, one first idea is to overlap with rules in the presentation of the monoid instead of multiplying with all monoid elements.

Procedure: SATURATION 1

Given: A polynomial $p \in \mathbf{K}[\mathcal{M}]$ and (Σ, T) a convergent presentation of $\mathcal{M}$.
Find: A (generally infinite) set $S \in \mathcal{SAT}(p)$.

$S := \{p\}$;
$H_0 := \{p\}$;
$i := 0$;
while $H_i \neq \emptyset$ **do**
  $q :=$ remove(H_i);
  % Remove an element using a fair strategy
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda$ for some $(l, r) \in T\}$ **do**
    % $C(t)$ contains special overlaps between t and left hand sides of rules in T
    $q' := q * w$;
    if $q' \notin S$;
      then **if** $q' \not\longrightarrow^{\mathrm{r}}_{S} 0$
        then $S := S \cup \{q'\}$;
          $H_i := H_i \cup \{q'\}$;

```
                else    H_i := H_i ∪ {q'};
            endif
        endif
    H_{i+1} := H_i;
    i := i + 1;
    endfor
endwhile
```

This procedure gives us an enumeration of a saturating set for a polynomial. This enumeration terminates in case for some index i the set H_i becomes empty. This can only arise if for any polynomial $q \in H_i$ either the set $C(\mathsf{HT}(q))$ is empty or for all $w \in C(\mathsf{HT}(q))$, $q{*}w \in S$ holds. Since these requirements are strong, it will be important to find additional sufficient conditions when such an enumeration can be stopped. The following example illustrates why in case $q' \not\longrightarrow^{\mathrm{r}}_S 0$ in procedure SATURATION 1 we have to consider q' for further computations, i.e., add it to our set H.

Example 4.3.18
Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow \lambda\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b$.
Then in modifying procedure SATURATION 1 to omit adding q' to H_i in case we already have $q' \longrightarrow^{\mathrm{r}}_S 0$ we would get the following computation on input $a^2 + a$: We start with $S := \{a^2 + a\}$ and $H_0 := \{a^2 + a\}$. Then $q := a^2 + a$ is removed from H_0 and we find $C(a^2) = \{b\}$ resulting in $q' = (a^2 + a) * b = a + \lambda$. Since $a + \lambda \longrightarrow^{\mathrm{r}}_S 0$ the procedure then halts with output $S = \{a^2 + a\}$. But the polynomial $(a^2 + a) * b^2 = \lambda + \underline{b}$ is not right reducible by S.
On the other hand, procedure SATURATION 1 terminates and computes the set $S = \{a^2 + a, b + \lambda\}$, which is a saturating set for $a^2 + a$. ◇

Lemma 4.3.19
Procedure SATURATION 1 *generates a saturating set for a polynomial.*

Proof :
Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$ and S the set generated by procedure SATURATION 1 on input p and (Σ, T). We have to show that for all $w \in \mathcal{M}$ we have $p * w \longrightarrow^{\mathrm{r}}_S 0$ in case $p * w \neq 0$. Since $p \in H_0$ this follows immediately by showing that for all $q \in \bigcup_{i \geq 0} H_i$ and all $w \in \mathcal{M}$ with $q * w \neq 0$ we have $q * w \longrightarrow^{\mathrm{r}}_S 0$. Notice that for all $q \in H_i$ we have $q \longrightarrow^{\mathrm{r}}_S 0$. Now let us assume that our claim is not true. Then we can choose a non-zero counter-example $q * w$, where $\mathsf{HT}(q)w$ is minimal (according to the ordering $\succeq_T$ on Σ^*) and $q * w \not\longrightarrow^{\mathrm{r}}_S 0$. Then $\mathsf{HT}(q)w$ must be T-reducible, as otherwise $q * w \longrightarrow^{\mathrm{r}}_q 0$ with $\mathsf{HT}(q * w) \equiv \mathsf{HT}(q)w$ and, as $q \in \bigcup_{i \geq 0} H_i$, then $q \longrightarrow^{\mathrm{r}}_{s \in S} 0$ implies $q * w \longrightarrow^{\mathrm{r}}_{s \in S} 0$. Let $\mathsf{HT}(q)w \equiv t_1 t_2 w_1 w_2$ where $\mathsf{HT}(q) \equiv t_1 t_2, t_2 \neq \lambda, w \equiv w_1 w_2$ and $l \equiv t_2 w_1$ for some $(l, r) \in T$. Furthermore, $w_1 \in \mathcal{M}$ as it is a prefix of $w \in \mathcal{M}$. As we use a fair strategy to remove elements from the sets H_i, q and $C(\mathsf{HT}(q))$ must

be considered and we have $w_1 \in C(\mathsf{HT}(q))$ by the definition of this set. Since we have $q * w_1 \in \bigcup_{i \geq 0} H_i$ by construction, $\mathsf{HT}(q)w \equiv \mathsf{HT}(q)w_1w_2 \succ \mathsf{HT}(q * w_1)w_2$ contradicts our assumption that $q * w$ was a minimal counter example.

q.e.d.

Another idea to compute saturating sets might be to gain more insight by taking a more constructive look at their definition.

Definition 4.3.20
Given a polynomial p, for each term $t \in \mathsf{T}(p)$ let $X_t = \{w \in \mathcal{M} \mid \mathsf{HT}(p * w) = t \circ w\}$, i.e., the set of all elements, which put t into head position[8]. Further let $Y_t = \{p * w \mid w \in X_t\}$. By choosing sets $B_t \subseteq Y_t$ such that for all polynomials $q \in Y_t$ we have $q \longrightarrow^{\mathrm{r}}_{B_t} 0$, we get a saturating set $\bigcup_{t \in \mathsf{T}(p)} B_t \in \mathcal{SAT}(p)$. $\diamond$

This definition does not specify how to choose the sets B_t, but setting $B_t = Y_t$ we always get the trivial saturating set $\{p * w \mid w \in \mathcal{M}\} \backslash \{0\}$. Of course $Y_{\mathsf{HT}(p)}$ must at least contain p, but all other Y_t can be empty. In case the multiplication on $\mathcal{M}$ is monotone, we get $Y_{\mathsf{HT}(p)} = \{p * w \mid w \in \mathcal{M}\}$ and $Y_t = \emptyset$ for $t \in \mathsf{T}(p) \backslash \{\mathsf{HT}(p)\}$. Then obviously the set $B_{\mathsf{HT}(p)} = \{p\}$ is a finite saturating set for p.

Unfortunately, one cannot hope for a terminating saturating procedure because finite saturating sets need not exist for certain monoid presentations, as the following examples reveal.

Example 4.3.21
Let $\Sigma = \{a, b, c, d, e, f\}$ and $T = \{abc \longrightarrow ba, bad \longrightarrow e, fbc \longrightarrow bf\}$ be a presentation[9] of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c \succ d \succ e \succ f$.
Looking at the polynomial $p = a + f \in \mathbf{Q}[\mathcal{M}]$ we find that with respect to this presentation we have the set $X_f = \{(bc)^i dw \mid i \in \mathbf{N}, w \in \mathcal{M}\}$, and it can be seen that the set $Y_f = \{b^{i+1}fdw + b^i ew \mid i \in \mathbf{N}, w \in \mathcal{M}\}$ has no finite basis. Since if there were a finite basis B_f for Y_f, we could choose $k \in \mathbf{N}$ such that $b^{k+1}fd + b^k e \notin B_f$. But then we get $b^{k+1}fd + b^k e \not\longrightarrow^{\mathrm{r}}_{B_f} 0$ as $b^{i+1}fdw \circ \mathrm{x} = b^{k+1}fd$ has no solution in $\mathcal{M}$ unless $\mathrm{x} = \lambda$ and $i = k$. Note that every saturating set $S \in \mathcal{SAT}(p)$ must right reduce all the elements of the set Y_f to zero in one step. However, if we change our precedence on Σ slightly to $f \succ a \succ b \succ c \succ d \succ e$, then the set $\{f + a\}$ is a saturating set for p. The phenomenon occurring is depicted below; the respective head terms of the polynomials are underlined. $\diamond$

[8] Note that if $\mathcal{M}$ is not right-cancellative one w may belong to different sets.

[9] Note that (Σ, T) is a convergent length-reducing presentation and the monoid is cancellative.

$$\begin{array}{lcl}
\underline{a} + f & & \\
\quad\Big|\, bc & & \\
\underline{ba} + bf & \underset{d}{\overline{\qquad}} & e + \underline{bdf} \\
\quad\Big|\, bc & & \\
\underline{b^2a} + b^2f & \underset{d}{\overline{\quad}} & be + \underline{b^2fd} \\
\quad\Big|\, bc & & \\
\quad\vdots & &
\end{array}$$

Example 4.3.22
Let $\Sigma = \{a, b, c, d, e, f\}$ and $T = \{abc \longrightarrow ba, bad \longrightarrow fe, fbc \longrightarrow bf, bfd \longrightarrow ae\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by an arbitrary precedence $\succ$ on Σ.
Then the polynomial $p = a + f \in \mathbf{Q}[\mathcal{M}]$ will allow no finite saturating sets independent of the chosen precedence: We have to distinguish two cases according to the relation of the two letters a and f:

1. Case $a \succ f$ (depicted in figure 1 below): Then we get the set $X_f = \{(bc)^i dw \mid i \in \mathbf{N}, w \in \mathcal{M}\}$, and the corresponding set $Y_f = \{b^i aew + b^i few \mid i \in \mathbf{N}, w \in \mathcal{M}\}$ has no finite basis. Since if there was a finite basis B_f, we could choose $k \in \mathbf{N}$ such that $b^k ae + b^k fe \notin B_f$ for Y_f. But then we get $b^k ae + b^k fe \not\longrightarrow^{\mathrm{r}}_{B_f} 0$ as $b^i ae \circ \mathrm{x} = b^k ae$ has no solution in $\mathcal{M}$ unless $\mathrm{x} = \lambda$ and $i = k$.

2. Case $f \succ a$ (depicted in figure 2 below): Then we get the set $X_a = \{(bc)^i dw \mid i \in \mathbf{N}, w \in \mathcal{M}\}$, and the corresponding set $Y_a = \{b^i few + b^i aew \mid i \in \mathbf{N}, w \in \mathcal{M}\}$ likewise has no finite basis. This can be shown as above. $\diamond$

$$\begin{array}{lcl}
\underline{a} + f & & \\
\quad\Big|\, bc & & \\
\underline{ba} + bf & \underset{d}{\overline{\qquad}} & e + \underline{bdf} \\
\quad\Big|\, bc & & \\
\underline{b^2a} + b^2f & \underset{d}{\overline{\quad}} & be + \underline{b^2fd} \\
\quad\Big|\, bc & & \\
\quad\vdots & &
\end{array}$$

Figure 1

$$\begin{array}{lcl}
\underline{f} + a & & \\
\quad\Big|\, bc & & \\
\underline{bf} + ba & \underset{d}{\overline{\qquad}} & ae + \underline{fe} \\
\quad\Big|\, bc & & \\
\underline{b^2f} + b^2a & \underset{d}{\overline{\quad}} & bae + \underline{bfe} \\
\quad\Big|\, bc & & \\
\quad\vdots & &
\end{array}$$

Figure 2

On the other hand in a group ring finite saturating sets always exist.

Lemma 4.3.23
For any polynomial p in a group ring $\mathbf{K}[\mathcal{G}]$ there exists a saturating set $S \in \mathcal{SAT}(p)$ containing at most $|\mathsf{T}(p)|$ elements.

Proof :
To show our claim let us review the more constructive definition of saturating sets as given in definition 4.3.20.
For a polynomial p, let us take a closer look at the sets $X_t = \{w \in \mathcal{M} \mid \mathsf{HT}(p*w) = t \circ w\}$ and $Y_t = \{p * w \mid w \in X_t\}$ for $t \in \mathsf{T}(p)$. Then in case $Y_t \neq \emptyset$, there exists a polynomial $q = p * w$ in Y_t. It remains to show that every polynomial in Y_t then is right reducible to zero in one step using q. As w is a group element, we know $p = q * \mathsf{inv}(w)$ and for every other polynomial $p * u \in Y_t$ we find $\mathsf{HT}(q * (\mathsf{inv}(w) \circ u)) = \mathsf{HT}((q * \mathsf{inv}(w)) * u) = \mathsf{HT}(p * u) = t \circ u = t \circ (w \circ \mathsf{inv}(w)) \circ u = \mathsf{HT}(q) \circ (\mathsf{inv}(w) \circ u)$ and hence $p * u \longrightarrow^{\mathrm{r}}_{q} 0$.
q.e.d.

The proof of this lemma might give rise to another idea how to compute saturating sets using the constructive approach in definition 4.3.20.

Procedure: SATURATION 2

Given: A polynomial $p \in \mathbf{K}[\mathcal{M}]$.
Find: A set $S \in \mathcal{SAT}(p)$.

$S := \emptyset$;
for all $t \in \mathsf{T}(p)$ **do**
  if $X_t \neq \emptyset$
    then $S := S \cup \{$ a suitable basis of Y_t $\}$;
endfor

Unfortunately this procedure is not effective. First of all, although each of the sets X_t is recursive, one cannot decide, whether it is empty or not. On the other hand of course even if one knows that $X_t \neq \emptyset$, a “suitable” finite basis for the set Y_t need not exist (compare example 4.3.22). We will see later on how this idea is used to compute saturating sets in special group rings (compare chapter 5).

The main reason why this procedure cannot be effective is that the following uniform problem is not solvable:

Given: A polynomial $p \in \mathbf{K}[\mathcal{M}]$, a term $t \in \mathsf{T}(p)$, and (Σ, T) a convergent semi-Thue system presenting $\mathcal{M}$.
Question: $X_t \neq \emptyset$?

Lemma 4.3.24
There exists a monoid $\mathcal{M}$ such that the above problem is undecidable.

Proof :
We give a finite, convergent semi-Thue system presenting a monoid $\mathcal{M}$ such that for a polynomial $p = t_1 - t_2$, $t_1, t_2 \in \mathcal{M}$ in the corresponding monoid ring $\mathbf{Q}[\mathcal{M}]$ in general

it is undecidable whether $X_{t_2} \neq \emptyset$. This proof will use the following lemma stated in [Sa90]:

For every primitive recursive function $\mathbf{f} : \mathbf{N}^2 \longrightarrow \mathbf{N}$ *there exists a finite convergent interreduced semi-Thue system* $T_{\mathbf{f}}$ *over an alphabet* $\Sigma_{\mathbf{f}}$ *with* $\{a, b, g, c, v, e\} \subseteq \Sigma_{\mathbf{f}}$ *and a symbol* $f \in \Sigma_{\mathbf{f}}$ *such that the following holds:*

1. *We have* $fb^{n_1}ab^{n_2}age \xrightarrow{*}_{T_{\mathbf{f}}} b^{n_1}ab^{n_2}agc^{\mathbf{f}(n_1,n_2)}ve$ *and* $b^{n_1}ab^{n_2}agc^{\mathbf{f}(n_1,n_2)}ve \in \mathrm{IRR}(T_{\mathbf{f}})$ *for* $n_1, n_2 \in \mathbf{N}$.
2. *There exists a precedence* $\succ \subseteq \Sigma_{\mathbf{f}} \times \Sigma_{\mathbf{f}}$ *satisfying* $a \succ b \succ g \succ c \succ v \succ e$ *such that for the induced syllable ordering with status right* $>_{\mathrm{syll}} \subseteq \Sigma_{\mathbf{f}}^* \times \Sigma_{\mathbf{f}}^*$ *the following holds:* $\xrightarrow{+}_{T_{\mathbf{f}}} \subseteq >_{\mathrm{syll}}$.
3. *For all* $(l, r) \in T_{\mathbf{f}}$ *we have* $|l| = 2$ *and the first letter of* l *is not in* $\{a, b, g, c, v, e\}$.

Reviewing the proof of this lemma, the precedence on $\Sigma_{\mathbf{f}}$ can be chosen such that f is maximal among all letters. Thus for the primitive recursive functions

$$\mathbf{f}_1(\mathrm{x}, \mathrm{y}) = \begin{cases} 0 & \exists \mathrm{z} \leq \mathrm{y} \text{ such that the computation of } \Phi_{\mathrm{x}}(\mathrm{x}) \text{ halts within} \\ & \ \text{z steps} \\ 2 & \text{otherwise} \end{cases}$$

where Φ is a universal function and $\mathbf{f}_2(\mathrm{x}, \mathrm{y}) = 1$ there exist finite convergent interreduced semi-Thue systems $(\Sigma_{\mathrm{f}_1}, T_{\mathrm{f}_1})$ and $(\Sigma_{\mathrm{f}_2}, T_{\mathrm{f}_2})$ with precedences $\succ_1, \succ_2$ as described above and without loss of generality we can assume that $\Sigma_{\mathrm{f}_1} \cap \Sigma_{\mathrm{f}_2} = \{a, b, g, c, v, e\}$. Let $\Sigma = \Sigma_{\mathrm{f}_1} \cup \Sigma_{\mathrm{f}_2}$ and $T = T_{\mathrm{f}_1} \cup T_{\mathrm{f}_2}$ with precedence $\succ$ such that $\succ$ extends $\succ_1$ and $\succ_2$ and further $f_1 \succ f_2 \succ \mathrm{x}$ for all $\mathrm{x} \in \Sigma \backslash \{f_1, f_2\}$. If we slightly modify Σ and T to

$$\begin{aligned}
\Sigma' &= \Sigma \cup \{L_1, L_2, Q_1, \ldots, Q_7, A, B, G, E\} \\
&\quad \text{without loss of generality we assume } \Sigma \cap \{L_1, L_2, Q_1, \ldots, Q_7, A, B, G, E\} = \emptyset \\
T' &= T \quad \cup \\
&\quad \{(1)\ L_2 b \longrightarrow BL_2, (2)\ L_2 a \longrightarrow AQ_1, (3)\ Q_1 b \longrightarrow BQ_1, (4)\ Q_1 a \longrightarrow AQ_2, \\
&\quad\ (5)\ Q_2 g \longrightarrow GQ_3, (6)\ Q_3 e \longrightarrow Q_4 e, (7)\ GQ_4 \longrightarrow Q_5 g, (8)\ AQ_5 \longrightarrow Q_6 a, \\
&\quad\ (9)\ BQ_6 \longrightarrow Q_6 b, (10)\ AQ_6 \longrightarrow Q_7 a, (11)\ BQ_7 \longrightarrow Q_7 b, (12)\ L_1 Q_7 \longrightarrow \lambda\}
\end{aligned}$$

with precedence $\succ'$ any total extension of $\succ$ satisfying $L_1 \succ' L_2 \succ' Q_1 \succ' Q_2 \succ' Q_3 \succ' Q_4 \succ' Q_5 \succ' G \succ' B \succ' A \succ' Q_6 \succ' Q_7$, then (Σ', T') is a finite convergent interreduced semi-Thue system such that for all $(l, r) \in T'$ we have $|l| = 2$ and the first letter of l is not in the set $\{a, b, g, c, v, e\}$.
Additionally we can state that for $w = b^n ab^m agew'$, where $w' \in \mathrm{IRR}(T')$, we get $f_i L_1 L_2 w \xrightarrow{*}_{T'} b^n ab^m agc^{\mathbf{f}_i(n,m)}vew'$ and this is irreducible.
Furthermore, for the elements $w \in \mathrm{IRR}(T')$ which do not have a prefix of the form

$b^n ab^m age$ for some $n, m \in \mathbf{N}$, we get $L_1 L_2 w \xrightarrow{*}_{T'} L_1 \tilde{w}$ where $L_1 \tilde{w}$ is irreducible and especially $\tilde{w}$ does not start with the letter Q_7. To prove these reduction sequences, we will use that $L_2 b^n \xrightarrow{n}_{(1)} B^n L_2$, $Q_1 b^n \xrightarrow{n}_{(3)} B^n Q_1$, $B^n Q_6 \xrightarrow{n}_{(9)} Q_6 b^n$ and $B^n Q_7 \xrightarrow{n}_{(11)} Q_7 b^n$ for $n \in \mathbf{N}$.
In case $w = b^n ab^m agew'$ we have

$$\begin{array}{rll}
f_i L_1 \underline{L_2 b^n} ab^m agew' & \xrightarrow{n}_{(1)} & f_i L_1 B^n \underline{L_2 a} b^m agew' \\
& \longrightarrow_{(2)} & f_i L_1 B^n A \underline{Q_1 b^m} agew' \\
& \xrightarrow{m}_{(3)} & f_i L_1 B^n AB^m \underline{Q_1 a} gew' \\
& \longrightarrow_{(4)} & f_i L_1 B^n AB^m A \underline{Q_2 g} ew' \\
& \longrightarrow_{(5)} & f_i L_1 B^n AB^m AG \underline{Q_3 e} w' \\
& \longrightarrow_{(6)} & f_i L_1 B^n AB^m A \underline{G Q_4} ew' \\
& \longrightarrow_{(7)} & f_i L_1 B^n AB^m \underline{A Q_5} gew' \\
& \longrightarrow_{(8)} & f_i L_1 B^n A \underline{B^m Q_6} agew' \\
& \xrightarrow{m}_{(9)} & f_i L_1 B^n \underline{A Q_6} b^m agew' \\
& \longrightarrow_{(10)} & f_i L_1 \underline{B^n Q_7} ab^m agew' \\
& \xrightarrow{n}_{(11)} & f_i \underline{L_1 Q_7} b^n ab^m agew' \\
& \longrightarrow_{(12)} & \underline{f_i b^n ab^m age} w' \\
& \xrightarrow{*}_{T_{\mathbf{f}_i}} & b^n ab^m agc^{\mathbf{f}_i(n,m)} vew'
\end{array}$$

and are done.
To show that $L_1 L_2 w$ reduces to a normal form $L_1 \tilde{w}$ where $\tilde{w}$ does not start with the letter Q_7 in case w does not have a prefix of the form $b^n ab^m age$ for some $n, m \in \mathbf{N}$, we use the following fact: For $w \in \mathrm{IRR}(T')$ there exists an element $w' \in \mathrm{IRR}(T')$ such that we have $L_2 w \xrightarrow{*}_{T'} Q_7 w'$ if and only if $w = b^n ab^m agew'$ for some $n, m \in \mathbf{N}$. The "if" part follows directly as above. It remains to show that when reducing $L_2 w$ for some $w \in \mathrm{IRR}(T')$[10] we can only reach a word starting with the letter Q_7 in case w has a prefix of the form $b^n ab^m age$ for some $n, m \in \mathbf{N}$. Since $w \in \mathrm{IRR}(T')$, the word $L_2 w$ is only reducible by T' in case one of the rules $L_2 b \longrightarrow BL_2$ or $L_2 a \longrightarrow AQ_1$ is applicable. Hence we get a reduction sequence $L_2 w \xrightarrow{n}_{(1)} B^n L_2 v_1$ in case $w \equiv b^n v_1$ which terminates as soon as no more letters b occur as a prefix of the remaining part v_1 of w and this reduction sequence is unique. Since B^n and v_1 are irreducible, the word $B^n L_2 v_1$ has to be reducible by $L_2 a \longrightarrow AQ_1$, as if v_1 would start with a letter different from a (and different from b by assumption) we would end up with an irreducible word $B^n L_2 v_1$ that cannot be further reduced to a word starting with the letter Q_7. Hence, without loss of generality we can assume,

$$L_2 w \xrightarrow{n}_{(1)} B^n L_2 v_1 \longrightarrow_{(2)} B^n AQ_1 v_2$$

[10] It is sufficient to look at irreducible elements, as the semi-Thue system is convergent.

and $v_1 \equiv av_2$. Since we have not reached a word starting with Q_7, again we can assume that v_2 starts with a prefix $b^m a$ for some $m \in \mathbf{N}$, as otherwise we would be stuck with an irreducible word starting with $B^n A$. This gives us the unique reduction sequences

$$B^n A Q_1 v_2 \xrightarrow{m}_{(3)} B^n A B^m Q_1 v_2' \longrightarrow_{(4)} B^n A B^m A Q_2 v_3$$

and $v_2 \equiv b^m a v_3$, $v_2' \equiv a v_3$. Again, to keep the word $B^n A B^m A Q_2 v_3$ reducible by rules in T', we find that ge must be a prefix of v_3, i.e., $v_3 \equiv g v_3' \equiv g e v_4$, giving us the only possible reductions

$$B^n A B^m A Q_2 v_3 \longrightarrow_{(5)} B^n A B^m A G Q_3 v_3' \longrightarrow_{(6)} B^n A B^m A G Q_4 e v_4.$$

Combining these informations we find $w \equiv b^n v_1 \equiv b^n a v_2 \equiv b^n a b^m a v_3 \equiv b^n a b^m a g e v_4$ and $L_2 w \xrightarrow{*}_{T'} B^n A B^m A G Q_4 e v_4$.
Now we can proceed with the proof of our initial claim:
For $n \in \mathbf{N}$ let $p_n = f_1 L_1 L_2 b^n a - f_2 L_1 L_2 b^n a$ denote a polynomial in the corresponding monoid ring over $\mathbf{Q}$ where $\mathcal{M}$ is presented by the semi-Thue system (Σ', T'). Then we get

$$X_{f_2 L_1 L_2 b^n a} \neq \emptyset$$

if and only if

$$\exists w \in \Sigma'^* : (f_2 L_1 L_2 b^n a w)\downarrow_{T'} >_{\mathrm{syll}} (f_1 L_1 L_2 b^n a w)\downarrow_{T'}$$

By the definition of the syllable ordering, the construction of T' and the resulting normal forms we know, that only a word starting with a prefix $b^m age$ can cause the letters f_1 respectively f_2 to be affected and this is the only possibility to cause $X_{f_2 L_1 L_2 b^n a}$ to be non-empty. Hence we can conclude

$$\exists w \in \Sigma'^* : (f_2 L_1 L_2 b^n a w)\downarrow_{T'} >_{\mathrm{syll}} (f_1 L_1 L_2 b^n a w)\downarrow_{T'}$$

if and only if

$$\exists m \in \mathbf{N}, w' \in \Sigma'^* \ (f_2 L_1 L_2 b^n a b^m a g e w')\downarrow_{T'} >_{\mathrm{syll}} (f_1 L_1 L_2 b^n a b^m a g e w')\downarrow_{T'}$$

if and only if

$$\exists m \in \mathbf{N}, w' \in \Sigma'^* : b^n a b^m a g c^{\mathbf{f}_2(n,m)} v e w' >_{\mathrm{syll}} b^n a b^m a g c^{\mathbf{f}_1(n,m)} v e w'$$

if and only if

$$\exists m \in \mathbf{N} : \mathbf{f}_2(n,m) > \mathbf{f}_1(n,m)$$

Remembering the definitions of $\mathbf{f}_1$ and $\mathbf{f}_2$ we get for all $\mathrm{x} \in \mathbf{N}$:

$$\exists \mathrm{y} \in \mathbf{N} \text{ with } \mathbf{f}_2(\mathrm{x},\mathrm{y}) > \mathbf{f}_1(\mathrm{x},\mathrm{y}) \text{ if and only if } \Phi_{\mathrm{x}}(\mathrm{x}) \text{ is defined}$$

and this would solve the halting problem for the universal function Φ.

q.e.d.

Nevertheless, we will later on see how saturating sets in special classes of monoids and groups can be computed by using additional information on the respective structure.

The following definition carries the advantages of saturating sets for one polynomial on to sets of polynomials.

Definition 4.3.25
A set F of polynomials in $\mathbf{K}[\mathcal{M}]$ is called **saturated**, if $\alpha \cdot f * w \longrightarrow^{\mathrm{r}}_{F} 0$ holds for all $f \in F$ and all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$ such that $\alpha \cdot f * w \neq 0$. $\diamond$

Note that saturating sets for a polynomial p are saturated. Moreover, for a set of polynomials F every union $S = \bigcup_{f \in F} S_f$ of saturating sets $S_f \in \mathcal{SAT}(f)$ is a saturated set. The next lemma shows how saturated sets allow special representations of the elements belonging to the right ideal they generate.

Lemma 4.3.26
Let F be a saturated set of polynomials in $\mathbf{K}[\mathcal{M}]$. Then every non-zero polynomial $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ has a representation[11] *of the form $g = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, where $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$, and $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ w_i$.*

Proof :
This follows immediately from definition 4.3.25, as in case $\mathsf{HT}(f_i * w_i) \neq \mathsf{HT}(f_i) \circ w_i$ for some f_i in our representation of g assuming that $f_i * w_i \neq 0$, we know $f_i * w_i \longrightarrow^{\mathrm{r}}_{F} 0$, i.e., $f_i * w_i = \beta_i \cdot f'_i * w'_i$ for some $\beta_i \in \mathbf{K}^*, f'_i \in F, w'_i \in \mathcal{M}$ and $\mathsf{HT}(f'_i * w'_i) = \mathsf{HT}(f'_i) \circ w'_i$. Thus we can substitute $f_i * w_i$ by $\beta_i \cdot f'_i * w'_i$ in the given representation of g.

q.e.d.

Similar to lemma 4.3.13 the following statement holds:

Lemma 4.3.27
For f, g some polynomials in $\mathbf{K}[\mathcal{M}]$ and F a saturated set with $p \in F$, $f \longrightarrow^{\mathrm{s}}_{p} g$ implies $f \longrightarrow^{\mathrm{r}}_{F} g$. $\square$

Now we are able to show that we can simulate $\overset{*}{\longleftrightarrow}^{\mathrm{s}}$ with $\overset{*}{\longleftrightarrow}^{\mathrm{r}}$ and capture the right ideal congruence by using saturated sets.

Theorem 4.3.28
Let F be a saturated set of polynomials and p, q some polynomials in $\mathbf{K}[\mathcal{M}]$. Then

$$p \overset{*}{\longleftrightarrow}^{\mathrm{r}}_{F} q \textit{ if and only if } p - q \in \mathsf{ideal}_r(F).$$

[11] Note that such representations are in some sense "stable" but no stable standard representations as the head term of g need not be a bound for the terms involved. Especially saturated sets need not be stable standard bases.

Proof :
This is an immediate consequence of lemma 4.2.11 and lemma 4.3.27.

q.e.d.

Similar to definition 4.2.12 we can define Gröbner bases with respect to $\longrightarrow^{\mathrm{r}}$.

Definition 4.3.29
A set $G \subseteq \mathbf{K}[\mathcal{M}]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{r}}$ or a **right (or stable) Gröbner basis**, if

(i) $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{G} \; = \; \equiv_{\mathsf{ideal}_r(G)}$, and

(ii) $\longrightarrow^{\mathrm{r}}_{G}$ is confluent. $\diamond$

Notice that saturating sets for a polynomial p satisfy statement (i) of this definition, but in general need not be Gröbner bases of $\mathsf{ideal}_r(p)$, i.e., the Noetherian relation $\longrightarrow^{\mathrm{r}}$ induced by them need not be confluent, even restricted to the set $\{p * w \mid w \in \mathcal{M}\}$ and so the elements in $\mathsf{ideal}_r(p)$ do not necessarily right reduce to zero.

Example 4.3.30
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b \succ c$. Further let us consider the polynomial $p = a + b + c \in \mathbf{Q}[\mathcal{M}]$.
Then $S = \{a+b+c, a+c+\lambda, bc+c^2+b\} \in \mathcal{SAT}(p)$, but $\longrightarrow^{\mathrm{r}}_{S}$ is not confluent on the set $\{p * w \mid w \in \mathcal{M}\}$. This follows as $a + b + c \longrightarrow^{\mathrm{r}}_{a+c+\lambda} b - \lambda$ and $a + b + c \longrightarrow^{\mathrm{r}}_{a+b+c} 0$, but $b - \lambda \stackrel{*}{\not\longrightarrow}^{\mathrm{r}}_{S} 0$. $\diamond$

Note that this corresponds to the fact that the set $\{a + b + c\}$ is no Gröbner basis with respect to $\longrightarrow^{\mathrm{s}}$ (compare example 4.2.13). The following example shows that right Gröbner bases are strong Gröbner bases but not vice versa.

Example 4.3.31
Let $\mathcal{M}$ be presented as in example 4.3.30 above and $F = \{a + c + \lambda, b - \lambda\} \subseteq \mathbf{Q}[\mathcal{M}]$.

1. F is a strong Gröbner basis.
   We have to show that all strong s-polynomials reduce to zero. A quick inspection reveals that $U_{a+c+\lambda,b-\lambda} = \{(bw, w) \mid w \in \mathcal{M}\backslash b\Sigma^*, w \neq \lambda\}$. Hence we have $\mathsf{spol}_s(a+c+\lambda, b-\lambda, bw, w) = (a+c+\lambda)*bw-(b-\lambda)*w = cw+a\circ w+\underline{bw}-\underline{bw}+w = a \circ w + cw + w = (a + c + \lambda) * w \longrightarrow^{\mathrm{s}}_{a+c+\lambda} 0$.

2. F is no right Gröbner basis.
   We have $(a+c+\lambda)*ba = ca+\lambda+\underline{ba} \in \mathsf{ideal}_r(a+c+\lambda, b-\lambda)$, and hence $ba+ca+\lambda$ is congruent to zero modulo this right ideal. But $ba+ca+\lambda$ does not right reduce to zero by F, as the following inspection shows. The polynomial $ba+ca+\lambda$ is not right reducible by $a+c+\lambda$: Trying to modify a in order to reduce ba or ca we get,

$(a+c+\lambda)*ca = ba+\underline{c^2a}+ca$ and $(a+c+\lambda)*ba = ca+\lambda+\underline{ba}$. Furthermore, $b-\lambda$ can only be applied to reduce terms beginning with b. Hence the only possible right reduction steps to take place are $ba+ca+\lambda \longrightarrow^{\mathrm{r}}_{b-\lambda} ca+a+\lambda \longrightarrow^{\mathrm{r}}_{a+c+\lambda} ca-c$ and this polynomial is F-irreducible.

3. The set $G = \{a+b+c, a+c+\lambda, bc+c^2+b, b-\lambda\}$ is a right Gröbner basis (compare example 4.3.39 for a proof). $\diamond$

The next example states that there are cases where finite strong Gröbner bases exist, but no finite right Gröbner bases.

Example 4.3.32
Let $\Sigma = \{a,b,c,d,e,f\}$ and $T = \{abc \longrightarrow ba, bad \longrightarrow fe, fbc \longrightarrow bf, bfd \longrightarrow ae\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by an arbitrary precedence $\succ$ on Σ.
We have seen in example 4.3.22 that the polynomial $p = a+f \in \mathbf{Q}[\mathcal{M}]$ has no finite saturating set and hence there exist no finite right Gröbner bases for the right ideal generated by p. On the other hand the set $\{p\}$ itself is a strong Gröbner basis (compare example 4.3.22 to see that no critical situations exist). $\diamond$

We move on now to study how right Gröbner bases are connected to stable standard bases and how they can be characterized by right reduction. Let us start by proving an analogon to lemma 4.2.14

Lemma 4.3.33
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$.

1. *Then $p \xrightarrow{*}^{\mathrm{r}}_F 0$ implies the existence of a stable standard representation for p.*

2. *In case p has a stable standard representation with respect to F, then p is right reducible at its head monomial by F, i.e., p is top-reducible by F.*

3. *In case F is a stable standard basis, every polynomial $p \in \mathsf{ideal}_r(F)\backslash\{0\}$ is top-reducible to zero by F using right reduction.*

Proof :

1. This follows directly by adding up the polynomials used in the right reduction steps occurring in $p \xrightarrow{*}^{\mathrm{r}}_F 0$.

2. This is an immediate consequence of definition 4.3.1 as the existence of a polynomial f in F and an element $w \in \mathcal{M}$ with $\mathsf{HT}(f*w) = \mathsf{HT}(f)\circ w = \mathsf{HT}(p)$ is guaranteed.

3. We show that every non-zero polynomial $p \in \mathsf{ideal}_r(F)\backslash\{0\}$ is top-reducible to zero using F by induction on $\mathsf{HT}(p)$. Thus let $\mathsf{HT}(p) = \min\{\mathsf{HT}(g) \mid g \in$

$\mathsf{ideal}_r(F)\backslash\{0\}\}$. Then as $p \in \mathsf{ideal}_r(F)$ and F is a stable standard basis, we have $p = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ and $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ w_i \succeq \mathsf{HT}(f_i * w_i)$ for all $1 \leq i \leq k$. Without loss of generality, let $\mathsf{HT}(p) = \mathsf{HT}(f_1) \circ w_1 = \mathsf{HT}(f_1 * w_1)$. Hence, the polynomial p is right reducible by f_1 at its head monomial. Let $p \longrightarrow^{\mathrm{r}}_{f_1} q$, i.e., $q = p - \mathsf{HC}(p) \cdot \mathsf{HC}(f_1 * w_1)^{-1} \cdot f_1 * w_1$, and by the definition of right reduction the term $\mathsf{HT}(p)$ is eliminated from p implying that $\mathsf{HT}(q) \prec \mathsf{HT}(p)$ as $q < p$. Thus, as $q \in \mathsf{ideal}_r(F)$ and $\mathsf{HT}(p)$ was minimal among the head terms of the elements in the right ideal generated by F, this implies $q = 0$, and, therefore, p is top-reducible to zero by f_1 in one step. On the other hand, in case $\mathsf{HT}(p) \succ \min\{\mathsf{HT}(g) \mid g \in \mathsf{ideal}_r(F)\backslash\{0\}\}$, by the same arguments used before we can top right reduce p to a polynomial q with $\mathsf{HT}(q) \prec \mathsf{HT}(p)$, and, thus, by our induction hypothesis we know that q and hence p is top-reducible to zero.

q.e.d.

As before we find that right Gröbner bases and stable standard bases are in fact equivalent.

Theorem 4.3.34
For a set of polynomials F in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *F is a right Gröbner basis.*
2. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}^{\mathrm{r}}_F 0$.*
3. *F is a stable standard basis.*

Proof :
$1 \Longrightarrow 2$: By (i) of definition 4.3.29 we know that $g \in \mathsf{ideal}_r(F)$ implies $g \xleftrightarrow{*}^{\mathrm{r}}_F 0$ and since $\longrightarrow^{\mathrm{r}}_F$ is confluent and 0 is irreducible $g \xrightarrow{*}^{\mathrm{r}}_F 0$ follows immediately.

$2 \Longrightarrow 3$: This follows directly by adding up the polynomials used in the right reduction steps of $g \xrightarrow{*}^{\mathrm{r}}_f 0$.

$3 \Longrightarrow 1$: In order to show that F is a Gröbner basis we have to prove two subgoals: $\xleftrightarrow{*}^{\mathrm{r}}_F = \equiv_{\mathsf{ideal}_r(F)}$ has already been shown in lemma 4.3.11. It remains to show that $\longrightarrow^{\mathrm{r}}_F$ is confluent. Since $\longrightarrow^{\mathrm{r}}_F$ is Noetherian, we only have to prove local confluence. Suppose $g \longrightarrow^{\mathrm{r}}_F g_1, g \longrightarrow^{\mathrm{r}}_F g_2$ and $g_1 \neq g_2$. Then $g_1 - g_2 \in \mathsf{ideal}_r(F)$ and, therefore, is top-reducible to zero by F as a result of lemma 4.3.33. Thus lemma 4.3.8 provides the existence of a polynomial $h \in \mathbf{K}[\mathcal{M}]$ such that $g_1 \xrightarrow{*}^{\mathrm{r}}_F h$ and $g_2 \xrightarrow{*}^{\mathrm{r}}_F h$, i.e., $\longrightarrow^{\mathrm{r}}_F$ is confluent.

q.e.d.

We continue by examining critical pairs of polynomials with respect to right reduction and defining corresponding s-polynomials in order to characterize right Gröbner bases.

Definition 4.3.35
Given two non-zero polynomials $p_1, p_2 \in \mathbf{K}[\mathcal{M}]$[12], every pair of elements w_1, w_2 in $\mathcal{M}$ such that $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_1) \circ w_1 = \mathsf{HT}(p_2) \circ w_2 = \mathsf{HT}(p_2 * w_2)$, defines a **(right) s-polynomial**

$$\mathsf{spol}(p_1, p_2, w_1, w_2) = \mathsf{HC}(p_1 * w_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2 * w_2)^{-1} \cdot p_2 * w_2.$$

Let $U_{p_1,p_2} \subseteq \mathcal{M} \times \mathcal{M}$ be the set containing *all* such pairs $w_1, w_2 \in \mathcal{M}$. $\diamond$

A right s-polynomial will be called non-trivial in case it is non-zero and notice that for non-trivial s-polynomials we always have $\mathsf{HT}(\mathsf{spol}(p_1, p_2, w_1, w_2)) \prec \mathsf{HT}(p_1) \circ w_1 = \mathsf{HT}(p_2) \circ w_2$. The set U_{p_1,p_2} can be empty, finite or even infinite depending on $\mathcal{M}$ as the following example reveals.

Example 4.3.36
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a,\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b \succ c$.
Then for the polynomials $c + \lambda, b + \lambda, a + c$ and $c^2 + b \in \mathbf{Q}[\mathcal{M}]$ we find that the set $U_{c+\lambda,b+\lambda}$ is empty, the set $U_{a+c,c+\lambda} = \{(\lambda, b)\}$ is finite and the set $U_{c+\lambda,c^2+b}$ contains all pairs (c^{n+1}, c^n), $n \in \mathbf{N}$, i.e., is infinite. $\diamond$

Unlike in Buchberger's approach and the previous section, s-polynomials as defined above are no longer strong enough to characterize Gröbner bases as they can only be used to give a confluence test but not to ensure that the right ideal congruence is expressible by reduction.

Example 4.3.37
Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow \lambda, ba \longrightarrow \lambda\}$ be a presentation of a group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b$.
Examining the set $F = \{b + \lambda\}$ we find that F has no non-trivial s-polynomials. On the other hand we get $(b + \lambda) - (b + \lambda) * a = a - b$ and hence $a - b \in \mathsf{ideal}_r(F)$. But the polynomial $a - b$ does not right reduce to zero by F. $\diamond$

This phenomenon is due to the fact that there are critical situations between the polynomial $b + \lambda$ and the rules in T viewed as polynomials in the free monoid ring, i.e., $ab - \lambda, ba - \lambda$. These situations are considered in the saturating process in procedure SATURATION 1 on page 74 (compare the definition of the sets $C(t)$ there). Nevertheless, if we require our set of polynomials to be saturated, we can characterize Gröbner bases in a familiar way.

Theorem 4.3.38
For a saturated set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$.*

[12]Notice that $p_1 = p_2$ is possible.

2. *For all not necessarily different polynomials $f_k, f_l \in F$ and every corresponding pair $(w_k, w_l) \in U_{f_k,f_l}$ we have $\mathsf{spol}(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{r}}_F 0$.*

Proof :

$1 \Longrightarrow 2$: Let $(w_k, w_l) \in U_{f_k,f_l}$ give us an s-polynomial belonging to the polynomials f_k, f_l. Then by definition 4.3.35 we get

$$\mathsf{spol}(f_k, f_l, w_k, w_l) = \mathsf{HC}(p_1 * w_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2 * w_2)^{-1} \cdot p_2 * w_2 \ \in \mathsf{ideal}_r(F)$$

and hence $\mathsf{spol}(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{r}}_F 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero polynomial $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{r}}_F$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{r}}_F h'$ implies $h' \in \mathsf{ideal}_r(F)$. Thus as $\longrightarrow^{\mathrm{r}}_F$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{r}}_F$-reducible. Now, let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}, f_j \in F, w_j \in \mathcal{M}$. By lemma 4.3.26 we can assume $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ w_i$ since F is saturated. Depending on this representation of g and a well-founded total ordering $\succeq$ on $\mathcal{M}$ we define $t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{r}}_F$-reducible. So by lemma 4.3.33 it is sufficient to show that g has a stable standard representation, as this implies that g is top-reducible using F. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[13]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[14] such that $t = \mathsf{HT}(f_k * w_k) = \mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l = \mathsf{HT}(f_l * w_l)$. Then by definition 4.2.16 we have a corresponding s-polynomial $\mathsf{spol}(f_k, f_l, w_k, w_l) = \mathsf{HC}(f_k * w_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l * w_l)^{-1} \cdot f_l * w_l$. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume $\mathsf{spol}(f_k, f_l, w_k, w_l) \neq 0$[15]. Hence, the reduction sequence $\mathsf{spol}(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{s}}_F 0$ results in a stable standard representation $\mathsf{spol}(f_k, f_l, w_k, w_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbf{K}^*$, $h_i \in F, v_i \in \mathcal{M}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}(f_k, f_l, w_k, w_l)) \prec t$. This gives us:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \quad & \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \quad & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{= \mathsf{spol}(f_k, f_l, w_k, w_l)}
\end{aligned}$$

[13]Note that this ordering is well-founded since $\succ$ is and $K \in \mathbf{N}$.

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

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

$$= \quad (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i) \tag{4.2}$$

where $\beta_k = \mathsf{HC}(f_k * w_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l * w_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (4.2) in our representation of g either t disappears or K is decreased.

q.e.d.

Note that reducing a Gröbner basis need not preserve the properties of Gröbner bases, since for polynomials $p, q, q_1, q_2 \in \mathbf{K}[\mathcal{M}]$, $p \longrightarrow^{\mathrm{r}}_{q}$ and $q \longrightarrow^{\mathrm{r}}_{q_1} q_2$ need not imply $p \longrightarrow^{\mathrm{r}}_{\{q_1,q_2\}}$.

Example 4.3.39
Let $\Sigma = \{a, b, c\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, cb \longrightarrow a\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b \succ c$.
Then the set $F = \{a + b + c, a + c + \lambda, bc + c^2 + b, b - \lambda\}$ is a Gröbner basis, as F is saturated and all possible s-polynomials right reduce to zero. To see this we have to examine the possible s-polynomials.

1. $U_{a+b+c,a+c+\lambda} = \{(\lambda, \lambda)\}$ as for all other solutions of the equation $a \circ \mathrm{x} = a \circ \mathrm{y}$ at least one of the polynomials is not stable and $\mathsf{spol}(a + b + c, a + c + \lambda, \lambda, \lambda) = a + b + c - a - c - \lambda = b - \lambda \longrightarrow^{\mathrm{r}}_{b-\lambda} 0$.
2. $U_{a+b+c,bc+c^2+b} = \emptyset$ and $U_{a+c+\lambda,bc+c^2+b} = \emptyset$ as for all solutions of the equation $a \circ \mathrm{x} = bc \circ \mathrm{y}$ one of the polynomials is not stable[16].
3. $U_{a+b+c,b-\lambda} = \emptyset$ and $U_{a+c+\lambda,b-\lambda} = \emptyset$ as for all solutions of the equation $a \circ \mathrm{x} = b \circ \mathrm{y}$ one of the polynomials is not stable[17].
4. $U_{bc+c^2+b,b-\lambda} = \{(b, a), (w, c \circ w) \mid w \in \mathcal{M}, c \circ w = cw\}$ and $\mathsf{spol}(bc + c^2 + b, b - \lambda, b, a) = ba + ca + \lambda - ba + a = ca + a + \lambda \longrightarrow^{\mathrm{r}}_{a+b+c} 0$, $\mathsf{spol}(bc + c^2 + b, b - \lambda, w, cw) = bcw + c^2 w + bw - bcw + w = c^2 w + bw + c \circ w \longrightarrow^{\mathrm{r}}_{a+b+c} 0$.

Now let us look at two possible ways of interreducing F:
If we first remove $bc + c^2 + b$ as

$$bc + c^2 + b \longrightarrow^{\mathrm{r}}_{b-\lambda} c^2 + b + c \longrightarrow^{\mathrm{r}}_{a+b+c} 0$$

and then $a + b + c$ since

$$a + b + c \longrightarrow^{\mathrm{r}}_{a+c+\lambda} b - \lambda \longrightarrow^{\mathrm{r}}_{b-\lambda} 0$$

this gives us a set $F' = \{a + c + \lambda, b - \lambda\}$ which is no longer a right Gröbner basis. This is due to the fact that we have $(a + c + \lambda) * c - (b - \lambda) = b + c^2 + c - b - \lambda = c^2 + c + \lambda \in \mathsf{ideal}_r(F) = \mathsf{ideal}_r(F')$ and this polynomial is not right reducible by the

[16] The solutions to this equation can be written as $\{(a \circ w, bc \circ w), (c \circ w, ba \circ w), (w, bca \circ w) \mid w \in \mathcal{M}\}$.
[17] The solutions to this equation can be written as $\{(a \circ w.b \circ w) \mid w \in \mathcal{M}\}$.

polynomials in the set F'.
On the other hand , if we first remove the polynomial $a+b+c$, then $bc+c^2+b$ no longer right reduces to zero with $\{a+c+\lambda, b-\lambda\}$. Instead we get

$$bc+c^2+b \longrightarrow^{\mathrm{r}}_{b-\lambda} c^2+b+c \longrightarrow^{\mathrm{r}}_{b-\lambda} c^2+c+\lambda$$

and the set $F''=\{a+c+\lambda, b-\lambda, c^2+c+\lambda\}$, although not saturated, is a right Gröbner basis. ◇

Unfortunately, theorem 4.3.38 is only of theoretical interest since in general the following uniform problem is undecidable, even in monoids where the solvability of equations of the form $u \circ \mathrm{x} = v \circ \mathrm{y}$ is decidable.

Given:	Two polynomials $p, q \in \mathbf{K}[\mathcal{M}]$, and
	(Σ, T) a convergent semi-Thue system presenting $\mathcal{M}$.
Question:	Does there exist an s-polynomial for p and q?

To see this we need a construction introduced in lemma 4.3.24.

Example 4.3.40
Let Φ be an universal function and $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3 : \mathbf{N}^2 \longrightarrow \mathbf{N}$ three primitive recursive functions, with

$$\mathbf{f}_1(\mathrm{x},\mathrm{y}) = \begin{cases} 0 & \exists \mathrm{z} \leq \mathrm{y} \text{ such that the computation of } \Phi_{\mathrm{x}}(\mathrm{x}) \text{ halts within z steps} \\ 2 & \text{otherwise,} \end{cases}$$

$\mathbf{f}_2(\mathrm{x},\mathrm{y}) = 1$ and $\mathbf{f}_3(\mathrm{x},\mathrm{y}) = 3$.
As described in the proof of lemma 4.3.24 we can construct a finite convergent interreduced semi-Thue system T' over an alphabet Σ'. Let $\mathcal{M}$ be the monoid presented by (Σ', T'). Then for $n \in \mathbf{N}$ and the corresponding polynomials $p_n = f_1L_1L_2b^na - f_2L_1L_2b^na$ and $q_n = f_1L_1L_2b^na - f_3L_1L_2b^na$ it is undecidable whether an s-polynomial exists in $\mathbf{Q}[\mathcal{M}]$. This is due to the fact that although the equation $f_1L_1L_2b^na \circ \mathrm{x} = f_1L_1L_2b^na \circ \mathrm{y}$ has all monoid elements (w, w) as trivial solutions, p_n and q_n have an s-polynomial if and only if $f_1L_1L_2b^na \circ w >_{\mathrm{syll}} f_2L_1L_2b^na \circ w$ for such a trivial solution. But as we have seen in the proof of lemma 4.3.24, it is not uniformly decidable given an arbitrary $n \in \mathbf{N}$ whether $f_2L_1L_2b^na \circ w >_{\mathrm{syll}} f_1L_1L_2b^na \circ w$. ◇

This example reveals how closely related the problems of saturation and s-polynomials are. All these problems stem from the fact that the ordering on the monoid need not be compatible and hence reduction need not be preserved under multiplication.

We will end this section by a remark on the algebraic characterization of Gröbner bases in terms of ideals in the set of terms, e.g., the free commutative monoid generated by the indeterminants in the usual polynomial ring. In the polynomial ring $\mathbf{K}[X_1, \ldots, X_n]$ we know that for a set of polynomials F we have that the set $\mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[X_1,\ldots,X_n]}(F)\backslash\{0\})$ itself is an ideal in the set of terms $\mathcal{T}$, in fact if F is a Gröbner basis then for the ideal generated by $\mathsf{HT}(F)$ in $\mathcal{T}$, we have $\mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[X_1,\ldots,X_n]}(F)\backslash\{0\}) = \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(F))$. This is crucial when proving termination of Buchberger's algorithm. Unfortunately, this no longer holds for arbitrary monoid rings.

Example 4.3.41
Let $\Sigma = \{a, b\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ba \longrightarrow ab\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a commutative group) with $a \prec b$ inducing a length-lexicographical ordering on $\mathcal{M}$. Note that $\mathcal{M}$ is a finite group consisting of the elements $\{\lambda, a, b, ab\}$. For $p = ab + \lambda \in \mathbf{Q}[\mathcal{M}]$, we get $\mathsf{ideal}_r^{\mathbf{Q}[\mathcal{M}]}(p) = \{\alpha \cdot (ab + \lambda) + \beta \cdot (b + a) \mid \alpha, \beta \in \mathbf{Q}\}$. Then the set $\{p\}$ itself is a right Gröbner basis, but we have $\mathsf{HT}(\mathsf{ideal}_r^{\mathbf{Q}[\mathcal{M}]}(p)\backslash\{0\}) = \{b, ab\} \neq \mathsf{ideal}_r^{\mathcal{M}}(ab) = \{\lambda, a, b, ab\}$. $\diamond$

In the next section we will introduce weakenings of right reduction which provide enough information to localize critical situations and characterize Gröbner bases in some way by the right ideals generated by their head terms. But, nothing really comes for free and we will have to do saturation with respect to these weaker reductions in order to establish the right ideal congruence.

4.4 The Concept of Prefix Reduction

In the previous section we have investigated stable standard representations of polynomials and we have seen how they are connected to right reduction. Hence, we start this section by refining our view on representations of polynomials which will lead to a refinement of right reduction. We will see later on that for certain classes of groups this enables us to compute finite Gröbner bases for finitely generated right ideals (compare chapter 5).

Definition 4.4.1
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$. A representation

$$p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i, \text{ with } \alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$$

is called a **prefix standard representation** with respect to the set of polynomials F, in case for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i$. A set $F \subseteq \mathbf{K}[\mathcal{M}]$ is called a **prefix standard basis** if every non-zero polynomial $g \in \mathsf{ideal}_r(F)$ has a prefix standard representation with respect to F. $\diamond$

Notice that $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i$ immediately implies $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i \succeq \mathsf{HT}(f_i * w_i)$ and in case $\mathsf{HT}(f_i) \circ w_i \equiv \mathsf{HT}(f_i)w_i$ even $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i \equiv \mathsf{HT}(f_i * w_i)$. On the other hand, in case $\mathsf{HT}(p) = \mathsf{HT}(f_i * w_i)$ we must have $\mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i)w_i$, i.e., $\mathsf{HT}(f_i)$ is a prefix of $\mathsf{HT}(p)$, and this situation occurs for at least one polynomial in the representation.

Before we move on, we give two technical but nevertheless useful lemmata comparable to lemma 4.3.2 which state when even more restricted prefix standard representations for polynomials exist.

Lemma 4.4.2
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ such that for all $f \in F$ and all $w \in \mathcal{M}$ the

polynomial $f * w$ has a prefix standard representation with respect to F in case it is non-zero. Then there even exists a prefix standard representation $f * w = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ such that $\mathsf{HT}(f * w) \succeq \mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i)w_i$.

Proof :
We will prove this lemma by contradiction. Let us assume this is not true. Then there exists a counter-example $f * w$ such that $\mathsf{HT}(f * w)$ is minimal among all counter-examples. By our assumption $f * w$ has a prefix standard representation, e.g. $f * w = \sum_{i=1}^{m} \alpha_i \cdot g_i * w_i$, with $\alpha_i \in \mathbf{K}^*, g_i \in F, w_i \in \mathcal{M}$. Without loss of generality we can assume that for some $k \leq m$, $g_1, \ldots, g_k$, are the polynomials involved in the head term of $f * w$, i.e., $\mathsf{HT}(f * w) \equiv \mathsf{HT}(g_i)w_i$ for all $1 \leq i \leq k$. Hence, we know $k < m$, as otherwise we would get a contradiction to $f * w$ being a counter-example. Furthermore, for all $k + 1 \leq j \leq m$ we know $\mathsf{HT}(g_j * w_j) \prec \mathsf{HT}(f * w)$ and hence every such polynomial has a prefix standard representation of the desired form, say $g_j * w_j = \sum_{l=1}^{n_l} \alpha'_{jl} \cdot g_{jl} * w'_{jl}$, with $\alpha'_{jl} \in \mathbf{K}^*$, $g_{jl} \in F$ and $w'_{jl} \in \mathcal{M}$. Thus the representation $f * w = \sum_{i=1}^{k} \alpha_i \cdot g_i * w_i + \sum_{i=k+1}^{n} \alpha_i \cdot (\sum_{l=1}^{n_l} \alpha'_{jl} \cdot g_{jl} * w'_{jl})$ is a prefix standard representation having the desired property, contradicting our assumption.

q.e.d.

Lemma 4.4.3
Let F be a prefix standard basis in $\mathbf{K}[\mathcal{M}]$. Then every non-zero polynomial $p \in \mathsf{ideal}_r(F)$ has a prefix standard representation $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F$, and $w_i \in \mathcal{M}$ such that for all $1 \leq i \leq n$ we even have

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i \equiv \mathsf{HT}(f_i * w_i).$$

Proof :
Since $p \in \mathsf{ideal}_r(F) \backslash \{0\}$, the polynomial p has a prefix standard representation with respect to F, say $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$ with $\alpha_i \in \mathbf{K}^*$, $f_i \in F$, and $w_i \in \mathcal{M}$. Moreover, by lemma 4.4.2 every multiple $f_i * w_i$ has a prefix standard representation with respect to F, say $f_i * w_i = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j$ with $\beta_j \in \mathbf{K}^*$, $g_j \in F$, and $v_j \in \mathcal{M}$, such that

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i * w_i) \succeq \mathsf{HT}(g_j * v_j) \equiv \mathsf{HT}(g_j)v_j.$$

q.e.d.

Notice that a prefix standard basis is a stable standard basis, as by lemma 4.4.3 the equation $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i = \mathsf{HT}(f_i) \circ w_i = \mathsf{HT}(f_i * w_i)$ holds. But the following example shows that the converse is not true.

Example 4.4.4
Let $\Sigma = \{a, b\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group), with $a \succ b$ inducing a length-lexicographical ordering on $\mathcal{M}$. Further take the set $F = \{ab\} \subseteq \mathbf{Q}[\mathcal{M}]$.

Then all non-zero polynomials $g \in \mathsf{ideal}_r(F)$ obviously have a stable standard representation in F, but e.g. the polynomial $a \in \mathsf{ideal}_r(F)$ has no prefix standard representation. $\diamond$

Prefix standard representations provide us with enough information to characterize prefix standard bases (which are closely related to special Gröbner bases as we will see later on) by their head terms in a way similar to the case of usual polynomial rings.

Theorem 4.4.5
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $G \subseteq \mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\}$. Then the following statements are equivalent:

1. *G is a prefix standard basis for $\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)$*[18].
2. *$\mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$.*

Notice that the set $\mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ in general is no right ideal in $\mathcal{M}$.

Proof :
$1 \Longrightarrow 2$: The inclusion $\mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M} \subseteq \mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ follows at once as $\mathsf{HT}(g)u \in \mathcal{M}$ for some $g \in G$, $u \in \Sigma^*$ implies $u \in \mathcal{M}$ and $\mathsf{HT}(g * u) \equiv \mathsf{HT}(g)u$, and as the multiple $g * u$ belongs to $\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)$. It remains to show that $\mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M} \supseteq \mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ holds. To see this, let $g \in \mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\}$. Then as G is a prefix standard basis for $\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)$, there exists a prefix standard representation $g = \sum_{i=1}^{n} \alpha_i \cdot g_i * w_i$ with $\alpha_i \in \mathbf{K}^*, g_i \in G$ and $w_i \in \mathcal{M}$ such that $\mathsf{HT}(g) \succeq \mathsf{HT}(g_i)w_i$. Furthermore there exists $1 \leq k \leq n$ such that $\mathsf{HT}(g) \equiv \mathsf{HT}(g_k)w_k$, i.e., $\mathsf{HT}(g) \in \mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M}$.

$2 \Longrightarrow 1$: We have to show that every $g \in \mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\}$ has a prefix standard representation with respect to G. This will be done by induction on the term $\mathsf{HT}(g)$. In the base case we can assume $\mathsf{HT}(g) = \min\{w | w \in \mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})\}$. Then since $\mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ there exists a polynomial $f \in G$ such that $\mathsf{HT}(g) \equiv \mathsf{HT}(f)w$ for some $w \in \mathcal{M}$. Eliminating the head term of g by subtracting an appropriate right multiple of f we get $h = g - \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$. As $g \in \mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)$, h lies in the right ideal generated by F. Moreover, since $\mathsf{HT}(g)$ is minimal and $\mathsf{HT}(h) \prec \mathsf{HT}(g)$, we can conclude $h = 0$ and g has a prefix standard representation $g = \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$. Now let us suppose $\mathsf{HT}(g) \succ \min\{w | w \in \mathsf{HT}(\mathsf{ideal}_r^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})\}$. Then again there exists a polynomial $f \in G$ such that $\mathsf{HT}(g) \equiv \mathsf{HT}(f)w$ for some $w \in \mathcal{M}$. Hence looking at the polynomial $h = g - \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$ we know that h lies in the right ideal generated by F and since $\mathsf{HT}(h) \prec \mathsf{HT}(g)$ either $h = 0$, giving us that $g = \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$, or our induction hypothesis yields the existence of a prefix standard representation for h

[18] I.e., $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$ and G is a prefix standard basis.

with respect to G, say $h = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j$ where $\beta_j \in \mathbf{K}^*$, $g_j \in G$ and $v_j \in \mathcal{M}$. Thus we have a prefix standard representation of the polynomial g, namely $g = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j + \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$.

q.e.d.

We continue by giving a weakening of right reduction that will correspond to the concepts of prefix standard representations and prefix standard bases.

Definition 4.4.6
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{M}]$. We say f **prefix reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\mathrm{p}} q$, if

(a) $\mathsf{HT}(f)w \equiv t$ for some $w \in \mathcal{M}$, i.e., $\mathsf{HT}(f)$ is a prefix of t, and

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

We write $p \longrightarrow_f^{\mathrm{p}}$ if there is a polynomial q as defined above and p is then called prefix reducible by f. Further we can define $\xrightarrow{*}^{\mathrm{p}}$, $\xrightarrow{+}^{\mathrm{p}}$, $\xrightarrow{n}^{\mathrm{p}}$ as usual. Prefix reduction by a set $F \subseteq \mathbf{K}[\mathcal{M}]$ is denoted by $p \longrightarrow_F^{\mathrm{p}} q$ and abbreviates $p \longrightarrow_f^{\mathrm{p}} q$ for some $f \in F$, which is also written as $p \longrightarrow_{f \in F}^{\mathrm{p}} q$. $\diamond$

Notice that in the above definition the equation in (a) has at most one solution and we then always have $\mathsf{HC}(f * w) = \mathsf{HC}(f)$. This is due to the fact that $t \equiv \mathsf{HT}(f)w$ implies $\mathsf{HT}(f)w = \mathsf{HT}(f * w)$ and $\mathsf{HT}(f)w \succ s \circ w$ for all $s \in \mathsf{T}(\mathsf{RED}(f))$. Further, in case f prefix reduces p to q at the monomial $\alpha \cdot t$, we have $t \notin \mathsf{T}(q)$ and $p > q$. Moreover, $\longrightarrow^{\mathrm{p}} \subseteq \longrightarrow^{\mathrm{r}}$ and the statements 1 to 3 of lemma 4.2.8 can be carried over to prefix reduction.

Lemma 4.4.7
Prefix reduction with respect to an arbitrary (possibly infinite) set $U \subseteq \mathbf{K}[\mathcal{M}]$ is Noetherian.

Proof :
This is an immediate consequence of the fact that $\geq$ is well-founded on $\mathbf{K}[\mathcal{M}]$ and $f \longrightarrow_g^{\mathrm{p}} f'$ implies $f > f'$. Hence an infinite reduction sequence $f \longrightarrow_{g_1}^{\mathrm{p}} f_1 \longrightarrow_{g_2}^{\mathrm{p}} f_2 \ldots$, $g_j \in U$, would imply the existence of an infinite strictly descending sequence of polynomials $f > f_1 > \ldots$ in $\mathbf{K}[\mathcal{M}]$ contradicting the fact that $\geq$ is well-founded on $\mathbf{K}[\mathcal{M}]$.

q.e.d.

Unlike in the case of strong right and right reduction now prefix reducing a polynomial using itself must result in zero. Therefore, we can define interreduced sets as follows.

Definition 4.4.8
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ **interreduced** or **reduced** with respect to $\longrightarrow^{\mathrm{p}}$, if no polynomial f in F is prefix reducible usinf the set $F \backslash \{f\}$. $\diamond$

As for right reduction, $p \longrightarrow^{\mathrm{p}}_{q_1} 0$ and $q_1 \longrightarrow^{\mathrm{r}}_{q_2} 0$ imply $p \longrightarrow^{\mathrm{p}}_{q_2} 0$. Furthermore, prefix reduction gives us additional information on the reduction step essential to the concept interreduction.

Remark 4.4.9
Let $p \longrightarrow^{\mathrm{p}}_{q}$ and $q \longrightarrow^{\mathrm{p}}_{q_1} q_2$. In case $\mathsf{HT}(q) = \mathsf{HT}(q_2)$ we immediately get $p \longrightarrow^{\mathrm{p}}_{q_2}$. Otherwise $\mathsf{HT}(q) \equiv \mathsf{HT}(q_1)w$ implies $p \longrightarrow^{\mathrm{p}}_{q_1}$. Hence we have $p \longrightarrow^{\mathrm{p}}_{\{q_1,q_2\}}$. ◇

Note that this property of prefix reduction corresponds to the fact that the existence of prefix standard representations with respect to a set of polynomials remains true for an interreduced version of the set.

Lemma 4.4.10
Let F and G be two sets of polynomials in $\mathbf{K}[\mathcal{M}]$ such that every polynomial in F has a prefix standard representation with respect to G. Then if a polynomial p has a prefix standard representation with respect to F it also has one with respect to G.

Proof :
Let $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ be a prefix standard representation of a polynomial p with respect to the set of polynomials F, i.e., for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i$. Furthermore, every polynomial f_i occurring in this sum has a prefix standard representation with respect to the set of polynomials G, say $f_i = \sum_{j=1}^{n_i} \beta_{i_j} \cdot g_{i_j} * v_{i_j}$, with $\beta_{i_j} \in \mathbf{K}^*, g_{i_j} \in G, v_{i_j} \in \mathcal{M}$ such that for all $1 \leq j \leq n_i$ we have $\mathsf{HT}(f_i) \succeq \mathsf{HT}(g_{i_j})v_{i_j}$.
These representations can be combined in the sum

$$p = \sum_{i=1}^{n} \alpha_i \cdot (\sum_{j=1}^{n_i} \beta_{i_j} \cdot g_{i_j} * v_{i_j}) * w_i.$$

It remains to show that this in fact is a prefix standard representation with respect to G, i.e., to prove that for all $1 \leq i \leq n$ and all $1 \leq j \leq n_i$, we get $\mathsf{HT}(p) \succeq \mathsf{HT}(g_{i_j})v_{i_j}w_i$. This now follows immediately as for all $1 \leq i \leq n$ and all $1 \leq j \leq n_i$ we have

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i \succeq \mathsf{HT}(g_{i_j})v_{i_j}w_i.$$

q.e.d.

One can even show that unique monic reduced standard bases exist.

Lemma 4.4.11
Let M be a subset of Σ^*. Then there exists a unique subset $M' \subseteq M$ such that

1. *for all $m \in M$ there exists an element $m' \in M'$ and an element $w \in \Sigma^*$ such that $m \equiv m'w$, and*
2. *for all $m \in M'$ no element $m' \in M' \backslash \{m\}$ is a prefix of m.* □

Note that the subset M' need not be finite , e.g., the set $M = \{ab^ic | i \in \mathbf{N}\}$ in $\{a, b, c\}^*$ contains no finite subset satisfying the properties above.

Theorem 4.4.12
Every right ideal in $\mathbf{K}[\mathcal{M}]$ contains a unique monic reduced prefix standard basis.

Proof :
Let $\mathfrak{i}_r$ be a right ideal in $\mathbf{K}[\mathcal{M}]$ and G a subset of $\mathfrak{i}_r$ such that we have

$$\mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathfrak{i}_r \backslash \{0\}).$$

Then by theorem 4.4.20 we know that G is a prefix standard basis of $\mathfrak{i}_r$. By lemma 4.4.11, as the set $\mathsf{HT}(G)$ is a subset of $\mathcal{M}$ which can be regarded as a subset of Σ^*, there exists a subset $H \subseteq \mathsf{HT}(G)$ such that

1. for all $m \in \mathsf{HT}(G)$ there exists an element $m' \in H$ and an element $w \in \Sigma^*$ such that $m \equiv m'w$,
2. for all $m \in H$ no element $m' \in H \backslash \{m\}$ is a prefix of m, and
3. $\mathsf{ideal}_r^{\Sigma^*}(H) \cap \mathcal{M} = \mathsf{ideal}_r^{\Sigma^*}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathfrak{i}_r \backslash \{0\})$.

Further for each term $t \in H$ there exists at least one polynomial in G with head term t. Thus we can choose one of them, say g_t, for every $t \in H$. If we then set $G' = \{g_t | t \in H\}$, by theorem 4.4.20 this is a prefix standard basis. Moreover, all polynomials in G' have different head terms and no head term is prefix reducible by the other polynomials in G'. Furthermore, if we prefix interreduce the set G' giving us another set of polynomials $G'' = \{\text{normalform}(g, \longrightarrow^{\mathrm{p}}_{G' \backslash \{g\}}) \mid g \in G'\}$, we know $\mathsf{HT}(G') = \mathsf{HT}(G'')$ and this set is a prefix standard basis. To see the latter, we show that for $f \in G$ with $f \longrightarrow^{\mathrm{p}}_{g' \in G \backslash \{f\}} f'$, the set $G' = (G \backslash \{f\}) \cup \{f'\}$ is a prefix standard basis. Since f has a prefix standard representation with respect to $(G \backslash \{f\}) \cup \{f'\}$, by lemma 4.4.10 we can conclude immediately that every polynomial in the right ideal generated by G also has a prefix standard representation with respect to G'.
It remains to show the uniqueness of the reduced prefix standard basis in case it is monic. Let us assume S is another monic reduced prefix standard basis of $\mathfrak{i}_r$. Further let $f \in S \bigtriangleup G'' = (S \backslash G'') \cup (G'' \backslash S)$ be a polynomial such that $\mathsf{HT}(f)$ is minimal in the set of terms $\mathsf{HT}(S \bigtriangleup G'')$. Without loss of generality we can assume that $f \in S \backslash G''$. As G'' is a reduced prefix standard basis and $f \in \mathfrak{i}_r$ there exists a polynomial $g \in G''$ such that $\mathsf{HT}(f) \equiv \mathsf{HT}(g)w$ for some $w \in \mathcal{M}$. We can even state that $g \in G'' \backslash S$ as otherwise S would not be prefix interreduced. Since f was chosen such that $\mathsf{HT}(f)$ was minimal in $\mathsf{HT}(S \bigtriangleup G'')$, we get $\mathsf{HT}(f) = \mathsf{HT}(g)$[19]. This gives us $\mathsf{HT}(f - g) \prec \mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HT}(f - g) \in \mathsf{T}(f) \cup \mathsf{T}(g)$ and without loss of generality let us assume $\mathsf{HT}(f - g) \in \mathsf{T}(f)$.

[19]Otherwise $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ would contradict our assumption.

But $f - g \in \mathfrak{i}_r$ and $f - g \neq 0$ implies the existence of a polynomial $h \in S$ such that $\mathsf{HT}(f - g) \equiv \mathsf{HT}(h)w$ for some $w \in \mathcal{M}$, implying that f is not prefix reduced. Hence we get that S is not prefix interreduced, contradicting our assumption.

q.e.d.

Before moving on to the study of prefix reduction we give some settings where bounds on special representations of polynomials are preserved under multiplication. These properties are of importance to establish a weaker form of the fact that $p \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ implies $\alpha \cdot p * w \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ used in the proof of Buchberger's characterization of Gröbner bases. They will be used in the proofs of different characterizations of prefix Gröbner bases later on.

Lemma 4.4.13
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $p \in \mathbf{K}[\mathcal{M}]$. Further let $p \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$ and let us assume this reduction sequence results in a representation $p = \sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$, where $\alpha_i \in \mathbf{K}^*$, $g_i \in F$, and $w_i \in \mathcal{M}$. Then for every term $t \in \mathcal{M}$ such that $t \succ \mathsf{HT}(p)$ and every term $w \in \mathcal{M}$ we get that if $s \in \bigcup_{i=1}^{k} \mathsf{T}(g_i * w_i * w)$ then $tw \succ s$ holds.

Proof :
As $\sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$ belongs to the reduction sequence $p \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$, for all $u \in \bigcup_{i=1}^{k} \mathsf{T}(g_i * w_i)$ we have $\mathsf{HT}(p) \succeq u$ implying $tw \succ \mathsf{HT}(p)w \succeq uw \succeq u \circ w$. Note that this proof uses the fact that the ordering $\succ$ on $\mathcal{M}$ is induced by the completion ordering $\succeq_T$ of the presentation (Σ, T) of $\mathcal{M}$, as we need that the ordering is compatible with concatenation, i.e., $uv \succeq_T (uv)\downarrow_T = u \circ v$ for all $u, v \in \mathcal{M}$.

q.e.d.

Similarly, some properties of Buchberger's reduction are regained, although not his lemma that $p \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$ implies $\alpha \cdot p * w \xrightarrow{*}{}^{\mathrm{b}}_{F} 0$.

Lemma 4.4.14
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $p, q \in \mathbf{K}[\mathcal{M}]$. Further let $p \longrightarrow^{\mathrm{p}}_{q} 0$ and $q \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$. Let these reduction sequences result in the representations $p = \alpha \cdot q * w$ and $q = \sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$, where $\alpha, \alpha_i \in \mathbf{K}^*, g_i \in F$, and $w, w_i \in \mathcal{M}$. Then the following statements hold:

1. *There exists $s \in \{1, \ldots, k\}$ such that $\mathsf{HT}(p) = \mathsf{HT}(g_s * w_s * w) = \mathsf{HT}(g_s * w_s)w$.*
2. *For all remaining terms $t \in \bigcup_{\substack{i=1 \\ i \neq s}}^{k} \mathsf{T}(g_i * w_i * w)$ we have $\mathsf{HT}(p) \succ t$.*

Notice that this also holds for a representation resulting from a right reduction sequence $p \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$.

Proof :
Since $p \longrightarrow^{\mathrm{p}}_{q} 0$ and $p = \alpha \cdot q * w$ we know $\mathsf{HT}(p) \equiv \mathsf{HT}(q)w$. As $\sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$ belongs to the reduction sequence $q \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$, there exists $s \in \{1, \ldots, k\}$ such that $\mathsf{HT}(q) \equiv$

$\mathsf{HT}(g_s)w_s \equiv \mathsf{HT}(g_s * w_s)$, $\mathsf{HC}(q) = \alpha_s \cdot \mathsf{HC}(g_s)$ and for all terms $t \in \bigcup_{\substack{i=1 \\ i \neq s}}^{k} \mathsf{T}(g_i * w_i)$ we have $\mathsf{HT}(q) \succ t$ implying $\mathsf{HT}(p) \equiv \mathsf{HT}(q)w \succ tw \succeq t \circ w$.

q.e.d.

A word of caution: This lemma does *not* imply $p \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$ or $p \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$, as there is no information on how multiplying the polynomials $g_i * w_i$ by w affects them in case $i \neq s$, especially prefix reduction is not preserved under right multiplication.

Example 4.4.15
Let $\Sigma = \{a, b\}$ and $T = \{ab \longrightarrow \lambda, ba \longrightarrow \lambda\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b$. Further let $F = \{a + \lambda, b + \frac{1}{2}\} \subseteq \mathbf{Q}[\mathcal{M}]$ and $p = a^2 + 2 \cdot a + 2$, $q = a + 2 \cdot b + 2$ be two polynomials in $\mathbf{Q}[\mathcal{M}]$.
Then we have

$$p \longrightarrow^{\mathrm{p}}_{q} a^2 + 2 \cdot a + 2 - (a + 2 \cdot b + 2) * a = 0$$

and

$$q \longrightarrow^{\mathrm{p}}_{a+\lambda} a + 2 \cdot b + 2 - (a + \lambda) = 2 \cdot b + \lambda \longrightarrow^{\mathrm{p}}_{b+\frac{1}{2}} 2 \cdot b + \lambda - 2 \cdot (b + \frac{1}{2}) = 0,$$

but $p \longrightarrow^{\mathrm{p}}_{a+\lambda} a^2 + 2 \cdot a + 2 - (a + \lambda) * a = a + 2 \longrightarrow^{\mathrm{p}}_{a+\lambda} \lambda$, i.e., $p \overset{*}{\not\longrightarrow}{}^{\mathrm{p}}_{F} 0$. $\diamond$

As before, we show that the translation lemma holds for prefix reduction.

Lemma 4.4.16
Let F be a set of polynomials and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$.

1. *Let $p - q \longrightarrow^{\mathrm{p}}_{F} h$. Then there are $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{p}}_{F} p'$, $q \xrightarrow{*}{}^{\mathrm{p}}_{F} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{p}}_{F}$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{p}}_{F} g$ and $q \xrightarrow{*}{}^{\mathrm{p}}_{F} g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{p}}_{F} h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*$, $f \in F$, $w \in \mathcal{M}$ and $\mathsf{HT}(f)w = t$, i.e., $\alpha \cdot \mathsf{HC}(f)$ is the coefficient of t in $p - q$. We have to distinguish three cases:
   (a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$: Then we can eliminate the term t in the polynomials p respectively q by prefix reduction and get $p \longrightarrow^{\mathrm{p}}_{f} p - \alpha_1 \cdot f * w = p'$, $q \longrightarrow^{\mathrm{p}}_{f} q - \alpha_2 \cdot f * w = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f)$ and $\alpha_2 \cdot \mathsf{HC}(f)$ are the coefficients of t in p respectively q.
   (b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$: Then we can eliminate the term t in the polynomial p by prefix reduction and get $p \longrightarrow^{\mathrm{p}}_{f} p - \alpha \cdot f * w = p'$ and $q = q'$.

(c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$: Then we can eliminate the term t in the polynomial q by prefix reduction and get $q \longrightarrow^{\mathrm{p}}_{f} q + \alpha \cdot f * w = q'$ and $p = p'$.

In all three cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

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

q.e.d.

Notice that prefix reduction like right reduction in general does not capture the right ideal congruence, but for special bases of right ideals this can be regained.

Lemma 4.4.17
Let F be a prefix standard basis and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$. Then

$$p \overset{*}{\longleftrightarrow}^{\mathrm{p}}_{F} q \text{ if and only if } p - q \in \mathsf{ideal}_r(F).$$

Proof :
In order to prove our claim we have to show two subgoals. The inclusion $\overset{*}{\longleftrightarrow}^{\mathrm{p}}_{F} \subseteq \equiv_{\mathsf{ideal}_r(F)}$ is an immediate consequence of the definition of prefix reduction and can be shown by induction as in lemma 4.2.11. To prove the converse inclusion $\equiv_{\mathsf{ideal}_r(F)} \subseteq \overset{*}{\longleftrightarrow}^{\mathrm{p}}_{F}$ we can modify the proof given in lemma 4.2.11. Remember that $p \equiv_{\mathsf{ideal}_r(F)} q$ implies $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$, where $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{M}$. Since every multiple $f_j * w_j$ lies in $\mathsf{ideal}_r(F)$ and F is a prefix standard basis, by lemma 4.4.3, we can assume $\mathsf{HT}(f * w) \equiv \mathsf{HT}(f)w$ for all polynomials occurring in the sum. Now we can prove our claim straightforward as in lemma 4.2.11 by induction on m.

q.e.d.

We can define Gröbner bases with respect to prefix reduction by slightly changing our previous definitions.

Definition 4.4.18
A set $G \subseteq \mathbf{K}[\mathcal{M}]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{p}}$ or a **prefix Gröbner basis**, if

(i) $\overset{*}{\longleftrightarrow}^{\mathrm{p}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$, and

(ii) $\longrightarrow^{\mathrm{p}}_{G}$ is confluent. ◇

As in the previous section there is a natural connection between prefix standard bases and prefix reduction.

Lemma 4.4.19
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$.

1. *Then $p \xrightarrow{*}^{\mathrm{p}}_{F} 0$ implies the existence of a prefix standard representation for p.*
2. *In case p has a prefix standard representation with respect to F, then p is prefix reducible at its head monomial by F, i.e., p is prefix top-reducible by F.*
3. *In case F is a prefix standard basis, every non-zero polynomial p in $\mathsf{ideal}_r(F)\backslash\{0\}$ is prefix top-reducible to zero by F.*

Proof :

1. This follows directly by adding up the polynomials used in the prefix reduction steps occurring in $p \xrightarrow{*}^{\mathrm{p}}_{F} 0$.
2. This is an immediate consequence of definition 4.4.1 as the existence of a polynomial f in F and an element $w \in \mathcal{M}$ with $\mathsf{HT}(p) \equiv \mathsf{HT}(f)w$ is guaranteed.
3. We show that every non-zero polynomial $p \in \mathsf{ideal}_r(F)\backslash\{0\}$ is top-reducible to zero using F by induction on the term $\mathsf{HT}(p)$. Let $\mathsf{HT}(p) = \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}_r(F)\backslash\{0\}\}$. Then, as $p \in \mathsf{ideal}_r(F)$ and F is a prefix standard basis, we have $p = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ and $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i)w_i$ for all $1 \leq i \leq k$. Without loss of generality, let us assume $\mathsf{HT}(p) \equiv \mathsf{HT}(f_1)w_1$. Hence, the polynomial p is prefix reducible by f_1. Let $p \longrightarrow^{\mathrm{r}}_{f_1} q$, i.e., $q = p - \mathsf{HC}(p) \cdot \mathsf{HC}(f_1)^{-1} \cdot f_1 * w_1$, and by the definition of prefix reduction the term $\mathsf{HT}(p)$ is eliminated from p implying that $\mathsf{HT}(q) \prec \mathsf{HT}(p)$ as $q < p$. Now, as $\mathsf{HT}(p)$ was minimal among the head terms of the elements in the right ideal generated by F, this implies $q = 0$, and, therefore, p is prefix top-reducible to zero by f_1 in one step. On the other hand, in case $\mathsf{HT}(p) \succ \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}_r(F)\backslash\{0\}\}$, by the same arguments used before we can prefix reduce the polynomial p to a polynomial q with $\mathsf{HT}(q) \prec \mathsf{HT}(p)$, and, thus, by our induction hypothesis we know that q is prefix top-reducible to zero. Therefore, as the reduction step $p \longrightarrow^{\mathrm{p}}_{f_1} q$ takes place at the head term of p, the polynomial p is also prefix top-reducible to zero.

q.e.d.

Using the results of this lemma we can show that prefix standard bases in fact are prefix Gröbner bases.

Theorem 4.4.20
For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *F is a prefix Gröbner basis.*

2. *For all polynomials* $g \in \mathsf{ideal}_r(F)$ *we have* $g \xrightarrow{*}^{\mathrm{p}}_F 0$.

3. *F is a prefix standard basis.*

Proof :
$1 \Longrightarrow 2$: By (i) of definition 4.4.18 we know that $g \in \mathsf{ideal}_r(F)$ implies $g \overset{*}{\longleftrightarrow}^{\mathrm{p}}_F 0$ and since $\longrightarrow^{\mathrm{p}}_F$ is confluent and 0 is irreducible, $g \xrightarrow{*}^{\mathrm{p}}_F 0$ follows immediately.

$2 \Longrightarrow 3$: This follows directly by adding up the polynomials used in the prefix reduction steps $g \xrightarrow{*}^{\mathrm{p}}_F 0$.

$3 \Longrightarrow 1$: In order to show that F is a prefix Gröbner basis we have to prove two subgoals: $\overset{*}{\longleftrightarrow}^{\mathrm{p}}_F = \equiv_{\mathsf{ideal}_r(F)}$ has already been shown in lemma 4.4.17. It remains to show that $\longrightarrow^{\mathrm{p}}_F$ is confluent. Since $\longrightarrow^{\mathrm{p}}_F$ is Noetherian, we only have to prove local confluence. Suppose $g \longrightarrow^{\mathrm{p}}_F g_1$, $g \longrightarrow^{\mathrm{p}}_F g_2$ and $g_1 \neq g_2$. Then $g_1 - g_2 \in \mathsf{ideal}_r(F)$ and, therefore, is prefix top-reducible to zero as a result of lemma 4.4.19. Hence lemma 4.4.16 provides the existence of a polynomial $h \in \mathbf{K}[\mathcal{M}]$ such that $g_1 \xrightarrow{*}^{\mathrm{p}}_F h$ and $g_2 \xrightarrow{*}^{\mathrm{p}}_F h$, i.e., $\longrightarrow^{\mathrm{p}}_F$ is confluent.

q.e.d.

Since in general for a set of polynomials F we get $\overset{*}{\longleftrightarrow}^{\mathrm{r}}_F \neq \overset{*}{\longleftrightarrow}^{\mathrm{p}}_F \neq \overset{*}{\longleftrightarrow}^{\mathrm{s}}_F$, we again enrich our set of polynomials used for reduction in order to regain the expressiveness of strong right reduction respectively right reduction combined with saturation.

Definition 4.4.21
A set of polynomials $F \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}\}$ is called a **prefix saturating set** for a non-zero polynomial $p \in \mathbf{K}[\mathcal{M}]$, if for all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$, in case $\alpha \cdot p * w \neq 0$ then $\alpha \cdot p * w \longrightarrow^{\mathrm{p}}_F 0$ holds[20]. $\mathcal{SAT}_p(p)$ denotes the family of all prefix saturating sets for p. We call a set $F \subseteq \mathbf{K}[\mathcal{M}]$ **prefix saturated**, if for all $f \in F$ and all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$, $\alpha \cdot f * w \longrightarrow^{\mathrm{p}}_F 0$ holds in case $\alpha \cdot f * w \neq 0$. ◇

As in the case of right reduction, for a set of polynomials F every union $S = \bigcup_{f \in F} S_f$ of prefix saturating sets $S_f \in \mathcal{SAT}_p(f)$ is a prefix saturated set. But in general this union contains too many polynomials, as the following example shows.

Example 4.4.22
Let $\Sigma = \{a, b\}$ and $T = \{ba \longrightarrow ab\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $b \succ a$.
For the set $F = \{a, b\}$ we find that b has no finite prefix saturating set, since there exists no finite set $S \subseteq \{a^n b \mid n \in \mathbf{N}\}$ such that all polynomials $a^n b$, $n \in \mathbf{N}$ are prefix reducible to zero in one step using S. But the set F itself is prefix saturated, since obviously $a^n b \longrightarrow^{\mathrm{p}}_a 0$ holds. ◇

At this point, before we continue to give a characterization of Gröbner bases in this context, let us take a look at the relations between the reductions studied so far and

[20]Since $\mathbf{K}$ is a field it is sufficient to demand $p * w \xrightarrow{\leq 1}^{\mathrm{p}}_F 0$ for all $w \in \mathcal{M}$.

the concepts of saturation induced by them. Remember that saturation enabled us to simulate strong right reduction by right reduction (compare lemma 4.3.13). The same is true for prefix saturation.

Lemma 4.4.23
Let f, g, p be some polynomials in $\mathbf{K}[\mathcal{M}]$, $S \in \mathcal{SAT}(p)$, and $S_p \in \mathcal{SAT}_p(p)$. Then the following statements hold:

1. $f \longrightarrow^{\mathrm{r}}_{S} g$ *if and only if* $f \longrightarrow^{\mathrm{r}}_{S_p} g$.
2. $f \longrightarrow^{\mathrm{r}}_{S} g$ *if and only if* $f \longrightarrow^{\mathrm{p}}_{S_p} g$.

Proof :
We will only prove statement 1, as 2 can be shown analogously. First, suppose $f \longrightarrow^{\mathrm{r}}_{p_1 \in S} g$, i.e., $g = f - \alpha_1 \cdot p_1 * w_1$ for some $\alpha_1 \in \mathbf{K}^*, w_1 \in \mathcal{M}$. Since S_p is a prefix saturating set for p and $p_1 \in S$ implies $p_1 = \alpha \cdot p * u$ for some $\alpha \in \mathbf{K}^*$, $u \in \mathcal{M}$ this gives us $p_1 * w_1 = (\alpha \cdot p * u) * w_1 = \alpha \cdot p * (u \circ w_1)$, i.e., $p_1 * w_1$ is a multiple of p. Thus $p_1 * w_1 \longrightarrow^{\mathrm{p}}_{p_2 \in S_p} 0$ and $p_1 * w_1 = \beta \cdot p_2 * w_2$ for some $\beta \in \mathbf{K}^*$, $w_2 \in \mathcal{M}$. Furthermore, as $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_1) \circ w_1 = \mathsf{HT}(p_2) w_2$, we get $f \longrightarrow^{\mathrm{r}}_{p_2 \in S_p} g$ and even $f \longrightarrow^{\mathrm{p}}_{p_2} g$. On the other hand, suppose $f \longrightarrow^{\mathrm{r}}_{p_1 \in S_p} g$, i.e., $g = f - \alpha_1 \cdot p_1 * w_1$ for some $\alpha_1 \in \mathbf{K}^*, w_1 \in \mathcal{M}$ and $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_1) \circ w_1$. As $p_1 = \alpha \cdot p * u$ for some $\alpha \in \mathbf{K}^*$, $u \in \mathcal{M}$ and $p_1 * w_1 = (\alpha \cdot p * u) * w_1 = \alpha \cdot p * (u \circ w_1)$ i.e., $p_1 * w_1$ is a multiple of p. Hence we get $p_1 * w_1 \longrightarrow^{\mathrm{r}}_{p_2 \in S} 0$ and $p_1 * w_1 = \beta \cdot p_2 * w_2$ for some $\beta \in \mathbf{K}^*$, $w_2 \in \mathcal{M}$ with $\mathsf{HT}(p_1 * w_1) = \mathsf{HT}(p_2) \circ w_2$ implying $f \longrightarrow^{\mathrm{r}}_{p_2 \in S} g$.

q.e.d.

Note that prefix saturated sets are also saturated sets. Furthermore, they give us additional information as they allow special representations of elements in the right ideals they generate which are weaker than prefix standard representations, but sufficient to give a localized confluence criteria. The following lemma is an analogon to lemma 4.3.26.

Lemma 4.4.24
Let $F \subseteq \mathbf{K}[\mathcal{M}]$ be a prefix saturated set. Then every non-zero polynomial g in $\mathsf{ideal}_r(F)$ has a representation[21] of the form $g = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$ with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$, and $\mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i) w_i$. □

Prefix reduction combined with prefix saturation is strong enough to capture the right ideal congruence.

Lemma 4.4.25
Let F be a prefix saturated set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $p, q, h \in \mathbf{K}[\mathcal{M}]$. Then

$$p \overset{*}{\longleftrightarrow}^{\mathrm{p}}_{F} q \text{ if and only if } p - q \in \mathsf{ideal}_r(F).$$

[21]Note that such a representation need not be a prefix standard representation as we cannot conclude that $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i) w_i$ holds.

Proof :
This lemma follows directly from theorem 4.3.28 and lemma 4.4.23.

q.e.d.

In the following we will give a procedure, which similar to SATURATION 1 on page 74 enumerates a prefix saturating set for a polynomial in $\mathbf{K}[\mathcal{M}]$ depending on a convergent presentation (Σ, T) of $\mathcal{M}$. We compute critical situations between the head terms of multiples of the polynomial being saturated and the left hand sides of the rules in T. Later on we will see how this can be compared to computing special s-polynomials between polynomials and the set of "polynomials" $\{l - r \mid (l, r) \in T\}$ in the free monoid ring generated by Σ.

Procedure: PREFIX SATURATION

Given: A polynomial $p \in \mathbf{K}[\mathcal{M}]$ and (Σ, T) a convergent presentation of $\mathcal{M}$.
Find: $S_p \in \mathcal{SAT}_p(p)$.

$S_p := \{p\}$;
$H := \{p\}$;
while $H \neq \emptyset$ **do**
  $q :=$ remove(H);
  % Remove an element using a fair strategy
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda$ for some $(l, r) \in T\}$ **do**
    % $C(t)$ contains special overlaps between t and left hand sides of rules in T
    $q' := q * w$;
    if $q' \not\longrightarrow^{\mathrm{p}}_{S_p} 0$ and $q' \neq 0$
      then $S_p := S_p \cup \{q'\}$;
        $H := H \cup \{q'\}$;
    endif
  endfor
endwhile

Notice that in contrary to procedure SATURATION 1 in case we have $q' \longrightarrow^{\mathrm{p}}_{S} 0$ then q' does not have to be considered for further computations.

Theorem 4.4.26
For a given polynomial $p \in \mathbf{K}[\mathcal{M}]$ let S_p be the set generated by procedure PREFIX SATURATION. *Then for all elements $w \in \mathcal{M}$ the polynomial $p * w$ is prefix reducible to zero in one step using S_p in case it is non-zero.*

Proof :
We show that for all $q \in S_p$,$w \in \mathcal{M}$ we have $q * w \longrightarrow^{\mathrm{p}}_{S_p} 0$ in case $q * w \neq 0$. Suppose this is not true. Then we can choose a non-zero counter-example $q * w$, where $\mathsf{HT}(q)w$ is minimal (according to the ordering $\succeq_T$ on Σ^*) and $q * w \not\longrightarrow^{\mathrm{p}}_{S_p} 0$. Thus $\mathsf{HT}(q)w$

must be T-reducible, as otherwise $q * w \longrightarrow^{\rm p}_{q \in S_p} 0$. Let $\mathsf{HT}(q)w \equiv t_1 t_2 w_1 w_2$ such that $\mathsf{HT}(q) \equiv t_1 t_2, t_2 \neq \lambda, w \equiv w_1 w_2$ and $l \equiv t_2 w_1$ for some $(l, r) \in T$. Furthermore, $w_1 \in \mathcal{M}$ as it is a prefix of $w \in \mathcal{M}$. Since $q \in S_p$ the polynomial q must have been added to the set H at some step and as we use a fair strategy to remove elements from H, q and $C(\mathsf{HT}(q))$ are considered. Thus, we have $w_1 \in C(\mathsf{HT}(q))$ by the definition of this set and we can distinguish two cases. If we have $q * w_1 \in S_p$ then $q * w = (q * w_1) * w_2 \longrightarrow^{\rm p}_{S_p} 0$, since $w_1 \in \mathcal{M}$ and $\mathsf{HT}(q)w \equiv \mathsf{HT}(q)w_1 w_2 \succ \mathsf{HT}(q * w_1)w_2$, contradicting our assumption. On the other hand, $q * w_1 \notin S_p$ implies $q * w_1 \longrightarrow^{\rm p}_{q' \in S_p} 0$ and we know $\mathsf{HT}(q)w_1 \succ \mathsf{HT}(q * w_1) \equiv \mathsf{HT}(q')z$ for some $z \in \mathcal{M}$. Further $q * w = (q * w_1) * w_2 = (\alpha \cdot q' * z) * w_2$, and $\mathsf{HT}(q)w \succ \mathsf{HT}(q')z w_2 \succeq \mathsf{HT}(q')(z \circ w_2)$. Therefore, we have $q * w = (\alpha \cdot q' * z) * w_2 = \alpha \cdot q' * (z \circ w_2) \longrightarrow^{\rm p}_{S_p} 0$, contradicting our assumption.

q.e.d.

Hence, procedure PREFIX SATURATION enumerates a prefix saturating set for a polynomial. The next lemma states that this process will terminate in case a finite prefix saturating set exists.

Lemma 4.4.27
In case a polynomial has a finite prefix saturating set, then procedure PREFIX SATURATION *terminates.*

Proof :
Let $p \in \mathbf{K}[\mathcal{M}]$ be the polynomial which is being saturated and $S \in \mathcal{SAT}_p(p)$ finite. Further let S_p be the set generated by the procedure. Since we have a correct enumeration of a prefix saturating set for p, each polynomial $q \in S$ has to be prefix reducible to zero by a polynomial in S_p[22]. Therefore, there exists a finite set $S' \subseteq S_p$ such that for every polynomials $q \in S$ there exists a polynomial $q' \in S'$ such that $q \longrightarrow^{\rm p}_{q'} 0$. Thus as soon as all polynomials in S' have been enumerated, we have the situation that for every remaining polynomial $h \in H$ on one hand $h \longrightarrow^{\rm p}_{s \in S} 0$ and on the other hand $s \longrightarrow^{\rm p}_{s' \in S'} 0$ hold, implying $h \longrightarrow^{\rm p}_{S'} 0$. Hence the **while** loop terminates, as no more elements are added to the set H.

q.e.d.

The following lemma gives some more information on the structure of a prefix saturating set for a polynomial in case our monoid is presented by a convergent monadic semi-Thue system with a length-lexicographical completion ordering ensuring that in this case finite prefix saturating sets exist.

Lemma 4.4.28
Let (Σ, T) be a convergent monadic presentation of a monoid $\mathcal{M}$. For a non-zero polynomial p in $\mathbf{K}[\mathcal{M}]$, let $S \in \mathcal{SAT}_p(p)$. Then for each non-zero right multiple $\tilde{q} = p * w$, $w \in \mathcal{M}$ there is a $q \in S$ such that

[22] Especially there is a polynomial $q' \in S_p$ such that $\mathsf{HT}(q) \equiv \mathsf{HT}(q')z$ for some $z \in \mathcal{M}$.

1. $|\mathsf{HT}(q)| \leq |\mathsf{HT}(p)| + \max\{|l| \mid (l,a) \in T\} - 1 =: K$.
2. $\tilde{q} \longrightarrow^{\mathrm{p}}_{q} 0$.

Proof :
Let us assume that our ordering on $\mathcal{M}$ is length-lexicographical. As T is monadic, for a polynomial $p = \sum_{i=1}^{n} \alpha_i \cdot t_i$ the right multiplication $p * w$ results in the terms of the form $t_1 \circ w \equiv t'_1 a_1 w_1, \ldots, t_n \circ w \equiv t'_n a_n w_n$, where t'_i is a prefix of t_i, $a_i \in \Sigma \cup \{\lambda\}$ and $w_1, \ldots, w_n$ are (possibly empty) suffixes of w. Now let us assume there exists a polynomial $\tilde{q} = p * w$ with $|\mathsf{HT}(\tilde{q})| > K$. Then we can decompose $w \equiv w_1 w_2 w_3$ in such a way that $\mathsf{HT}(\tilde{q}) = t_j \circ w \equiv t'_j a_j w_2 w_3$, i.e., $t_j \circ w_1 = t'_j a_j$ and $|t'_j a_j w_2| = K$. Let us consider the polynomial $p * w_1 w_2$. We claim that $\mathsf{HT}(p * w_1 w_2) \equiv t'_j a_j w_2$. Suppose this is not true. Then there exists a term $t_i \in \mathsf{T}(p)$ such that $\mathsf{HT}(p * w_1 w_2) = t_i \circ w_1 w_2 \succ t'_j a_j w_2$. Hence $|t_i \circ w_1 w_2| \geq K$ gives us $t_i \circ w_1 w_2 \equiv t'_i a_i w'$, where $|t'_i a_i| \leq |\mathsf{HT}(p)|$ and thus $|w'| \geq \max\{|l| \mid (l,a) \in T\} - 1$. Since furthermore w' is a suffix of $w_1 w_2$ and $w_1 w_2 w_3 \in \mathit{IRR}(T)$ we get that $t'_i a_i w' w_3$ is T-irreducible giving us $t'_i a_i w' w_3 \succ t_j \circ w_1 w_2 w_3 = \mathsf{HT}(\tilde{q})$ contradicting our assumption. Therefore, we can conclude $\mathsf{HT}(p * w_1 w_2) \equiv t'_j a_j w_2$. In case $p * w_1 w_2 \in S$ we can set $q = p * w_1 w_2$ and get $|\mathsf{HT}(q)| = |\mathsf{HT}(p * w_1 w_2)| = |t'_j a_j w_2| = K$ and we are done. On the other hand, since S is a prefix saturating set for p, there exists an element $q \in S$ such that $p * w_1 w_2 \longrightarrow^{\mathrm{p}}_{q} 0$ and $|\mathsf{HT}(q)| \leq |\mathsf{HT}(p * w_1 w_2)| = K$. As $\mathsf{HT}(p * w) \equiv \mathsf{HT}(p * w_1 w_2) w_3$ we know $p * w \longrightarrow^{\mathrm{p}}_{q} 0$ and are done.

q.e.d.

Corollary 4.4.29
Procedure Prefix Saturation *terminates for monoids $\mathcal{M}$ with a convergent monadic presentation.*

Proof :
This follows immediately from lemma 4.4.27 since lemma 4.4.28 provides the existence of finite prefix saturating sets for polynomials.

q.e.d.

Corollary 4.4.30
Procedure Prefix Saturation *terminates for finite monoids $\mathcal{M}$.*

Proof :
Let $\mathcal{M}$ be a finite monoid and p a polynomial in $\mathbf{K}[\mathcal{M}]$. Then obviously the set $S = \{p * w \mid w \in \mathcal{M}\}$ is finite and hence the procedure must terminate.

q.e.d.

The next lemma states the existence of minimal prefix saturating sets.

Lemma 4.4.31
Let p be a polynomial in $\mathbf{K}[\mathcal{M}]$ and $S \in \mathcal{SAT}_p(p)$ a prefix saturating set for p. Then if there is a polynomial $q \in S$ such that $q \longrightarrow^{\mathrm{p}}_{S \backslash \{q\}} 0$, the set $S \backslash \{q\}$ is a prefix saturating set for p.

Proof :
This follows immediately as $p \longrightarrow^{\mathrm{p}}_{q_1} 0$ and $q_1 \longrightarrow^{\mathrm{p}}_{q_2} 0$ imply $p \longrightarrow^{\mathrm{p}}_{q_2} 0$ (compare item 3 of lemma 4.2.8 which also holds for prefix reduction).

q.e.d.

It is now possible to introduce simplification to procedure PREFIX SATURATION by removing polynomials which are prefix reducible to zero in one step by later generated polynomial multiples.

Procedure: PREFIX SATURATION USING SIMPLIFICATION

Given: A polynomial $p \in \mathbf{K}[\mathcal{M}]$, and
(Σ, T) a convergent semi-Thue system presenting $\mathcal{M}$.
Find: $S_p \in \mathcal{SAT}_p(p)$.

$S_0 := \{p\}$;
$H := \{p\}$;
$i := 0$;
while $H \neq \emptyset$ **do**
  $i := i + 1$;
  $S_i := S_{i-1}$;
  $q :=$ remove(H);
  % Remove an element using a fair strategy
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda$ for some $(l, r) \in T\}$ **do**
    % $C(t)$ contains special overlaps between t and left hand sides of rules in T
    $q' := q * w$;
    if $q' \not\longrightarrow^{\mathrm{p}}_{S_i} 0$ and $q' \neq 0$
      then $S_i :=$ simplify$(S_i, q') \cup \{q'\}$;
        % Simplify removes elements s from S_i in case $s \longrightarrow^{\mathrm{p}}_{q'} 0$
        $H := H \cup \{q'\}$;
    endif
  endfor
endwhile
$S_p := S_i$

Theorem 4.4.32
Let S_p be the set generated by procedure PREFIX SATURATION USING SIMPLIFICATION *for a given polynomial $p \in \mathbf{K}[\mathcal{M}]$. Then for all elements $w \in \mathcal{M}$ the polynomial $p * w$ is prefix reducible to zero using S_p.*

Proof :
First we specify the output of procedure PREFIX SATURATION USING SIMPLIFICATION. In case H becomes empty in some iteration k we have $S_p = S_k$. Otherwise, as a fair strategy is used to remove elements from the set H, this guarantees that all polynomials added to H are also considered and we can characterize the output as $S_p = \bigcup_{i \geq 0} \bigcap_{j \geq i} S_i$. The fact that no polynomial is entered twice into H is due to the following observation: Since for polynomials q, q_1, q_2, $q \longrightarrow^{\mathrm{p}}_{q_1} 0$ and $q_1 \longrightarrow^{\mathrm{p}}_{q_2} 0$ yield $q \longrightarrow^{\mathrm{p}}_{q_2} 0$, we get that for all polynomials $f \longrightarrow^{\mathrm{p}}_{S_i} 0$ implies $f \longrightarrow^{\mathrm{p}}_{S_{i+n}} 0$, $n \in \mathbf{N}$. In particular, as $p \in S_0$, we get $p \longrightarrow^{\mathrm{p}}_{S_i} 0$ for all $i \in \mathbf{N}$.
We continue by proving that for all $q \in \bigcup_{i \geq 0} S_i$, $w \in \mathcal{M}$ we have $q * w \longrightarrow^{\mathrm{p}}_{S_p} 0$ as this implies $p * v \longrightarrow^{\mathrm{p}}_{S_p} 0$ for all $v \in \mathcal{M}$. Suppose this is not true. Then we can choose a counter-example $q * w$ such that $\mathsf{HT}(q)w$ is minimal (according to the ordering $\succeq_T$ on Σ^*) among all counter-examples and $q * w \not\longrightarrow^{\mathrm{p}}_{S_p} 0$. Then $\mathsf{HT}(q)w$ must be T-reducible, as otherwise $q \in S_j$ for some $j \in \mathbf{N}$ and $q \notin S_p$ implies $q \longrightarrow^{\mathrm{p}}_{s \in S_{j+k}} 0$ for some $k \in \mathbf{N}$ and either $s \in S_p$ contradicting our assumption or s is again removed by simplification. Now the latter cannot occur infinitely often, as in case a polynomial s is removed due to simplification with a polynomial q' we know $\mathsf{HT}(q')$ is a proper prefix of $\mathsf{HT}(s)$ as otherwise we would have $q' \longrightarrow^{\mathrm{p}}_{s} 0$ contradicting the fact that q' is used for simplification of the set containing s. Therefore, the existence of a polynomial $s \in S_p$ such that $q * w \longrightarrow^{\mathrm{p}}_{s} 0$ is guaranteed contradicting our assumption. Therefore, we can assume that for our counter-example $\mathsf{HT}(q)w$ is T-reducible. Hence, let $\mathsf{HT}(q)w \equiv t_1 t_2 w_1 w_2$ such that $\mathsf{HT}(q) \equiv t_1 t_2, t_2 \neq \lambda, w \equiv w_1 w_2$ and $l \equiv t_2 w_1$ for some rule $(l, r) \in T$. Since $q \in \bigcup_{i \geq 0} S_i$ the polynomial q must have been added to the set H at some step and as we use a fair strategy to remove elements from H, q and $C(\mathsf{HT}(q))$ are considered. Thus, we can conclude $w_1 \in C(\mathsf{HT}(q))$ by the definition of this set. Now we have to take a closer look at what happens to $q * w_1$. In case $q * w_1$ is added to the respective set S_j, then $\mathsf{HT}(q)w \equiv \mathsf{HT}(q)w_1 w_2 \succ \mathsf{HT}(q * w_1)w_2$ and $q * w_1 \in \bigcup_{i \geq 0} S_i$ imply $q * w = (q * w_1) * w_2 \longrightarrow^{\mathrm{p}}_{S_p} 0$ contradicting our assumption. Otherwise we have $q * w_1 \longrightarrow^{\mathrm{p}}_{S_j} 0$ for the set S_j actual when considering $q * w_1$ in the **for all** loop. But then $q * w_1 = \alpha \cdot q' * z$ for some $\alpha \in \mathbf{K}^*$, $q' \in S_j$, $z \in \mathcal{M}$ and $\mathsf{HT}(q)w_1 \succ \mathsf{HT}(q * w_1) \equiv \mathsf{HT}(q')z$. Moreover, $\mathsf{HT}(q)w \equiv \mathsf{HT}(q)w_1 w_2 \succ \mathsf{HT}(q')z w_2 \succeq \mathsf{HT}(q')(z \circ w_2)$ and $q * w = (q * w_1) * w_2 = (\alpha \cdot q' * z) * w_2 = \alpha \cdot q' * (z \circ w_2)$. Thus $q' * (z \circ w_2) \longrightarrow^{\mathrm{p}}_{S_p} 0$ implies $q * w \longrightarrow^{\mathrm{p}}_{S_p} 0$ contradicting our assumption.

q.e.d.

Before we move on to show how the property of being prefix saturated can be used to characterize prefix Gröbner bases, we prove that this property is decidable for finite sets of polynomials.

Lemma 4.4.33
It is decidable, whether a finite subset F of $\mathbf{K}[\mathcal{M}]$ is prefix saturated.

Proof :
We can slightly modify the procedure Prefix Saturation to give us a decision procedure, whether a finite set of polynomials is prefix saturated.

Procedure: Prefix Saturated Check

Given: A finite set $F \subseteq \mathbf{K}[\mathcal{M}]$ and (Σ, T) a convergent presentation of $\mathcal{M}$.
Answer: *yes*, if F is prefix saturated,
no, otherwise.

answer := yes
for all $q \in F$ **do**
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda \text{ for some } (l,r) \in T\}$ **do**
  % $C(t)$ contains words that will lead to cancellation when right multiplied to t
    $q' := q * w$
    if $q' \neq 0$ and $q' \not\longrightarrow^{\mathrm{p}}_{F} 0$
      then answer := no
    endif
  endfor
endfor

It remains to show that the answer of our procedure is "no" if and only if F is not prefix saturated. Obviously, the answer "no" implies the existence of an element $w \in \mathcal{M}$ such that for some $f \in F$, $f * w \not\longrightarrow^{\mathrm{p}}_{F} 0$. On the other hand, let us assume that our procedure gives us "yes", but F is not prefix saturated. Then there exist $w \in \mathcal{M}$ and $f \in F$ such that $\mathsf{HT}(f)w$ is minimal according to the ordering $\succeq_T$ on Σ^*, $f * w \neq 0$ and $f * w \not\longrightarrow^{\mathrm{p}}_{F} 0$. In case $w \in C(\mathsf{HT}(f))$ the procedure would give us "no" contradicting our assumption. Thus suppose $w \notin C(\mathsf{HT}(f))$. $\mathsf{HT}(f)w$ must be T-reducible as otherwise $f * w \longrightarrow^{\mathrm{p}}_{F} 0$. Let $\mathsf{HT}(f)w \equiv \mathsf{HT}(f)w_1 w_2$ such that $w_1 \in C(\mathsf{HT}(f))$. Now $f * w_1$ is considered by our procedure and since the answer given is "yes", we either get $f * w_1 = 0$ contradicting that $f * w \neq 0$, or $f * w_1 \longrightarrow^{\mathrm{p}}_{F} 0$. This gives us the existence of a polynomial $f' \in F$ such that $\mathsf{HT}(f)w_1 \succ \mathsf{HT}(f * w_1) \equiv \mathsf{HT}(f')z$ for some $z \in \mathcal{M}$. Now $\mathsf{HT}(f)w \equiv \mathsf{HT}(f)w_1 w_2 \succ \mathsf{HT}(f')zw_2 \succeq \mathsf{HT}(f')(z \circ w_2)$ gives us $f * w = f' * (z \circ w_2) \longrightarrow^{\mathrm{p}}_{F} 0$ contradicting our assumption.
Further this procedure terminates, as the sets $C(t)$ are always finite.
The complexity in the number of monoid multiplications can be described as follows: Let $n = \max\{|l| \mid (l,r) \in T\}$, $m = |T|$, and $k = \max\{|\mathsf{T}(f)| \mid f \in F\}$. Then the first **for all** loop is executed $|F|$-times. A computation of a set $C(t)$ can be bounded by $n \cdot m$ and the second **for all** loop is then executes $|C(t)|$-times. Within this loop there is one multiplication of a polynomial by a term involving at most k monoid multiplications and a test whether the result is zero or prefix reducible to zero in one step. The latter involves at most $|F|$ reduction tests, i.e., again $|F|$-times multiplying a polynomial with a term and checking for equality. Hence a bound in monoid multiplications is

$$\underbrace{|F|}_{\text{1st loop}} \cdot \underbrace{n \cdot m}_{\text{2nd loop}} \cdot (\underbrace{k}_{q*w} + \underbrace{|F| \cdot k}_{\text{reducibility check}}).$$

q.e.d.

Prefix saturation enriches a polynomial p to a set $S \in \mathcal{SAT}_p(p)$ such that we can substitute $q \longrightarrow_p^{(\mathrm{s,r})} q'$ by $q \longrightarrow_{p' \in S}^{\mathrm{p}} q'$. We use this additional information to give a finite confluence criterion that will use a refined definition of s-polynomials.

Definition 4.4.34
Given two non-zero polynomials $p_1, p_2 \in \mathbf{K}[\mathcal{M}]$, such that $\mathsf{HT}(p_1) \equiv \mathsf{HT}(p_2)w$ for some $w \in \mathcal{M}$ the **prefix s-polynomial** is defined as

$$\mathsf{spol}_p(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w.$$

$\diamond$

As before non-zero prefix s-polynomials are called non-trivial and for non-trivial s-polynomials we have $\mathsf{HT}(\mathsf{spol}_p(p_1, p_2)) \prec \mathsf{HT}(p_1) \equiv \mathsf{HT}(p_2)w$. Notice that a finite set $F \subseteq \mathbf{K}[\mathcal{M}]$ defines finitely many prefix s-polynomials. As before, these s-polynomials alone are not sufficient to characterize prefix Gröbner bases, but lemma 4.4.13 enables us to localize our confluence test in case we demand our set of polynomials to be prefix saturated.

Theorem 4.4.35
For a prefix saturated set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}_F^{\mathrm{p}} 0$.*
2. *For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}{}_F^{\mathrm{p}} 0$.*

Proof :
$1 \Longrightarrow 2$: Let $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)w$ for $w \in \mathcal{M}$. Then by definition 4.4.34 we get

$$\mathsf{spol}_p(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * w \ \in \mathsf{ideal}_r(F),$$

and hence $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}{}_F^{\mathrm{p}} 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow_F^{\mathrm{p}}$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow_F^{\mathrm{p}} h'$ implies $h' \in \mathsf{ideal}_r(F)$. Hence as $\longrightarrow_F^{\mathrm{p}}$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow_F^{\mathrm{p}}$-reducible. Now, let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{M}$. By lemma 4.4.24 we can assume $\mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i)w_i$. This will enable a restriction to prefix s-polynomials in order to modify the representation of g. Depending on the above representation of g and a well-founded total ordering $\succeq$ on $\mathcal{M}$ we define $t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \dots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$

and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{p}}_{F}$-reducible. So by lemma 4.4.19 it is sufficient to show that g has a prefix standard representation, as this implies that g is top-reducible using F. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or $(t' = t$ and $K' < K)$[23]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[24] such that $\mathsf{HT}(f_k)w_k \equiv \mathsf{HT}(f_l)w_l$. We have either $\mathsf{HT}(f_k)z \equiv \mathsf{HT}(f_l)$ or $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)z$ for some $z \in \mathcal{M}$. Without loss of generality let us assume $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)z$ and hence $w_l \equiv z w_k$. Then definition 4.4.34 provides us with a prefix s-polynomial $\mathsf{spol}_p(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * z$. Note that, while in the proofs of theorem 4.2.17 and 4.3.38 the s-polynomials correspond directly to the overlap $\mathsf{HT}(f_k * w_k) = \mathsf{HT}(f_l * w_l)$, i.e., w_k and w_l are involved in the s-polynomial, now we have an s-polynomial corresponding directly to the two polynomials f_k and f_l. We will see later on that this localization is strong enough because this situation has a prefix of the term t as an upper border and lemma 4.4.13 can be applied. We will now change our representation of g by using the additional information on the above prefix s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of t are decreased by at least 1. Let us assume $\mathsf{spol}_p(f_k, f_l) \neq 0$[25]. Hence, the reduction sequence $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$ results in a prefix standard representation of the form $\mathsf{spol}_p(f_k, f_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$, where $\delta_i \in \mathbf{K}^*$, $h_i \in F$, $v_i \in \mathcal{M}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_p(f_k, f_l))$. Now as $\mathsf{HT}(\mathsf{spol}_p(f_k, f_l)) \prec \mathsf{HT}(f_k) \preceq t \equiv \mathsf{HT}(f_k)w_k$, by lemma 4.4.13 we then can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * w_k$. Without loss of generality we can assume that for all polynomials occurring in this representation we have $\mathsf{HT}(h_i * v_i * w_k) \equiv \mathsf{HT}(h_i)(v_i \circ w_k)$ as F is prefix saturated and in case $\mathsf{HT}(h_i * v_i * w_k) \neq \mathsf{HT}(h_i)(v_i \circ w_k)$ we can substitute the polynomial $h_i * v_i * w_k$ by a product $\tilde{\alpha_i} \cdot \tilde{h_i} * u_i$ such that $h_i * v_i * w_k = \tilde{\alpha_i} \cdot \tilde{h_i} * u_i$ and $\mathsf{HT}(h_i * v_i * w_k) \equiv \mathsf{HT}(\tilde{h_i})u_i$ without increasing neither t nor K. This gives us:

$$
\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \;& \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}_p(f_k, f_l) * w_k} \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * w_k) \qquad (4.3)
\end{aligned}
$$

[23] Note that this ordering is well-founded since $\succ$ is and $K \in \mathbf{N}$.

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

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

where $\beta_k = \mathsf{HC}(f_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (4.3) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

q.e.d.

Buchberger's characterization of Gröbner bases by s-polynomials in the commutative polynomial ring provided a finite test to decide whether a finite set of polynomials is a Gröbner basis. Theorem 4.4.35 only provides such a test for finite prefix saturated sets. Since the property of being prefix saturated is also decidable for finite sets of polynomials, we can hence decide whether a finite set of polynomials is a prefix saturated Gröbner basis. We will see later on that prefix Gröbner bases need not be prefix saturated and how they then can be characterized. Theorem 4.4.35 gives rise to the following procedure to compute prefix Gröbner bases.

Procedure: PREFIX GRÖBNER BASES

Given: A finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$.
Find: $\text{GB}(F)$, a prefix Gröbner basis of F.
Using: SAT_p a prefix saturating procedure for polynomials.
$G := \bigcup_{f \in F} \text{SAT}_p(f)$;
% G is prefix saturated
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do**
  % Test if statement 2 of theorem 4.4.35 is valid
  $(q_1, q_2) :=$ remove(B);
  % Remove an element using a fair strategy
  if $\mathsf{spol}_p(q_1, q_2)$ exists
    % The s-polynomial is not trivial
    then $h :=$ normalform$(\mathsf{spol}_p(q_1, q_2), \longrightarrow^{\mathrm{p}}_{G})$;
      % Compute a normal form using prefix reduction
      if $h \neq 0$
        then $G := G \cup \text{SAT}_p(h)$;
          % G is prefix saturated
          $B := B \cup \{(f, \tilde{h}), (\tilde{h}, f) \mid f \in G, \tilde{h} \in \text{SAT}_p(h)\}$;
      endif
  endif
endwhile
$\text{GB}(F) := G$

There are two crucial points, why procedure PREFIX GRÖBNER BASES might not terminate: prefix saturation of a polynomial need not terminate and the set B need not become empty.

Note that in case prefix saturation does not terminate it is possible to modify this procedure in order to enumerate a (prefix) Gröbner basis by using fair enumerations of the prefix saturating sets needed.

The sets characterized in theorem 4.4.35 are prefix Gröbner bases and hence right Gröbner bases, but they are required to be prefix saturated. Reviewing example 4.3.41 we see that there exist right Gröbner bases which are not prefix saturated.

Example 4.4.36
Let $\Sigma = \{a, b\}$ and $T = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda, ba \longrightarrow ab\}$ be a presentation of a monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $b \succ a$. Then the set $\{ab + \lambda\} \subseteq \mathbf{Q}[\mathcal{M}]$ itself is a right Gröbner basis, but is neither prefix saturated nor a prefix Gröbner basis, as we have $b+a \in \mathsf{ideal}_r(ab+\lambda)$ but $b+a \not\longrightarrow^{\mathrm{p}}_{ab+\lambda} 0$. ◇

Note that even a prefix Gröbner basis need not be prefix saturated.

Example 4.4.37
Let $\Sigma = \{a, b, c, d, e\}$ and $T = \{ac \longrightarrow d, bc \longrightarrow e\}$ be a presentation of a monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c \succ d \succ e$.
Then the set $F = \{a + b, d + \lambda, e - \lambda\}$ is a prefix Gröbner basis in $\mathbf{Q}[\mathcal{M}]$. This can be seen by studying the right ideal generated by F, $\mathsf{ideal}_r(F) = \{\alpha_1 \cdot (a + b) * w_1 + \alpha_2 \cdot (d - \lambda) * w_2 + \alpha_3 \cdot (e - \lambda) * w_3 + \alpha_4 \cdot (d + e) * w_4 | \alpha_i \in \mathbf{Q}, w_i \in \mathcal{M}, w_1 \neq cw'\}$. But F is not prefix saturated, as $(a + b) * c = d + e \not\longrightarrow^{\mathrm{p}}_F 0$. We only have $d + e \xrightarrow{2}{}^{\mathrm{p}}_F 0$. ◇

In the previous section we have seen that we can have a finite strong Gröbner basis although no finite right Gröbner basis exists (compare example 4.3.32). Similarly a finite right Gröbner basis can exist while there is no finite prefix Gröbner basis.

Example 4.4.38
Let $\Sigma = \{a, b\}$ and $T = \{ba \longrightarrow ab\}$ be a presentation of a commutative monoid $\mathcal{M}$. Then the set $F = \{b + \lambda\}$ is a right Gröbner basis but no finite prefix Gröbner basis exists. ◇

Next we will give a characterization of prefix Gröbner bases without demanding that the set of polynomials is prefix saturated. This is important as interreducing a set of prefix saturated polynomials destroys this property, but in case the set being interreduced is a prefix Gröbner basis the resulting set will again be a prefix Gröbner basis (compare theorem 4.4.12). Remember that this is not true for right Gröbner bases in general (compare example 4.3.39).

Theorem 4.4.39
For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, equivalent are:

1. *Every polynomials $g \in \mathsf{ideal}_r(F)$ has a prefix standard representation.*
2. (a) *For all polynomials $f \in F$ and all elements $w \in \mathcal{M}$, the polynomial $f * w$ has a prefix standard representation.*
   (b) *For all polynomials $f_k, f_l \in F$ the non-trivial prefix s-polynomials have prefix standard representations.*

Proof :

$1 \Longrightarrow 2$: This follows immediately.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ has a prefix standard representation. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be an arbitrary representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*$, $f_j \in F$, $w_j \in \mathcal{M}$. By our assumption and lemma 4.4.2 we can assume that $\mathsf{HT}(f_i * w_i) \equiv \mathsf{HT}(f_i)w_i$ as $f_i \in F$ and every $f_i * w_i$ has a standard prefix representation. Note that these prefix standard representations do not yield a prefix standard representation for the polynomial g, as $\mathsf{HT}(g) \prec \mathsf{HT}(f_i)w_i$ is possible. Using statement (a) and (b) we then can proceed straightforward as in theorem 4.4.35 to show that such a representation can be transformed into a prefix standard representation for g with respect to F.

q.e.d.

Note that this theorem gives us a stronger characterization of prefix Gröbner bases in so far as it does not require the sets to be prefix saturated. We can further use it to prove the following lemma.

Lemma 4.4.40
It is decidable, whether a finite subset F of $\mathbf{K}[\mathcal{M}]$ is a prefix Gröbner basis.

Proof :
The following procedure decides, whether a finite set of polynomials is a prefix Gröbner basis.

Procedure: PREFIX GRÖBNER BASIS CHECK

Given: A finite set $F \subseteq \mathbf{K}[\mathcal{M}]$ and (Σ, T) a convergent presentation of $\mathcal{M}$.
Answer: *yes*, if F is a prefix Gröbner basis,
no, otherwise.

answer := yes;
$B := \{(f, g) \mid f, g \in F, f \neq g\}$;
for all $(f, g) \in B$ **do**
  if $\mathsf{spol}_p(f, g)$ exists
    then $q :=$ normalform($\mathsf{spol}_p(f, g)$, $\longrightarrow_F^{\mathrm{p}}$);
      if $q \neq 0$
        then answer := no;
      endif
  endif
endfor
for all $q \in F$ **do**
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda$ for some $(l, r) \in T\}$ **do**
  % $C(t)$ contains words that will lead to cancellation when right multiplied to t
    $q' :=$ normalform($q * w$, $\longrightarrow_F^{\mathrm{p}}$);

if $q' \neq 0$
  then answer := no;
endif
endfor
endfor

It remains to show that the answer of our procedure is "no" if and only if F is no prefix Gröbner basis. Obviously, the answer "no" implies the existence of a polynomial in the right ideal generated by F which is not prefix reducible to zero using F, i.e., F is no prefix Gröbner basis. On the other hand, let us assume that our procedure gives us "yes", although F is no prefix Gröbner basis. We then know that all prefix s-polynomials originating from polynomials in F prefix reduce to zero as the answer is not set to "no". Hence, by theorem 4.4.39 there must exist $f \in F$ and $w \in \mathcal{M}$ such that $f * w$ has no prefix standard representation with respect to F as otherwise F would be a prefix Gröbner basis. Let us assume that $\mathsf{HT}(f)w$ is minimal according to the ordering $\succeq_T$ on Σ^* such that the multiple $f * w \neq 0$ has no prefix standard representation with respect to F. Notice that $w \in C(\mathsf{HT}(f))$ is not possible as it would contradict that the answer given by the procedure is supposed to be "yes". Furthermore, $\mathsf{HT}(f)w$ must be T-reducible as otherwise we would get a contradiction by $f * w \longrightarrow^{\mathrm{p}}_{f} 0$. Since w is not T-reducible there exist $w_1, w_2 \in \mathcal{M}$ such that $\mathsf{HT}(f)w \equiv \mathsf{HT}(f)w_1w_2$ and $w_1 \in C(\mathsf{HT}(f))$. As the answer is "yes" and w_1 has been checked, we can conclude $f * w_1 \stackrel{*}{\longrightarrow}^{\mathrm{p}}_{F} 0$ implying the existence of a prefix standard representation for $f * w_1$, say $f * w_1 = \sum_{i=1}^{k} \alpha_i \cdot f_i * u_i$ for some $\alpha_i \in \mathbf{K}$, $f_i \in F$ and $u_i \in \mathcal{M}$. Moreover we know that $\mathsf{HT}(f)w_1 \succ \mathsf{HT}(f * w_1) \succeq \mathsf{HT}(f_i * u_i) \equiv \mathsf{HT}(f_i)u_i$ for all $1 \leq i \leq k$. This immediately provides $\mathsf{HT}(f)w \equiv \mathsf{HT}(f)w_1w_2 \succ \mathsf{HT}(f_i)u_iw_2 \succeq \mathsf{HT}(f_i)(u_i \circ w_2)$. Therefore, by our assumption that $\mathsf{HT}(f)w$ was chosen minimal, we can assume that every multiple $f_i * (u_i \circ w_2)$ has a prefix standard representation with respect to F, say $f_i * (u_i \circ w_2) = \sum_{j=1}^{k_i} \beta_{i_j} \cdot f_{i_j} * u_{i_j}$ with $\beta_{i_j} \in \mathbf{K}$, $f_{i_j} \in F$ and $u_{i_j} \in \mathcal{M}$. Hence, we find that $f * w = (\sum_{i=1}^{k} \alpha_i \cdot f_i * u_i) * w_2 = \sum_{i=1}^{k} \alpha_i \cdot f_i * (u_i \circ w_2) = \sum_{i=1}^{k} \alpha_i \cdot (\sum_{j=1}^{k_i} \beta_{i_j} \cdot f_{i_j} * u_{i_j})$ is a prefix standard representation of $f * w$ with respect to F, contradicting our assumption that $f * w$ has none.

q.e.d.

The next remark illuminates the differences between the two characterizations given for prefix Gröbner bases so far.

Remark 4.4.41
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$.

1. If F is prefix saturated, then for every polynomial $f \in F$ and every element $w \in \mathcal{M}$ the polynomial $f * w$ has a prefix standard representation.
   This follows immediately, since $f * w \longrightarrow^{\mathrm{p}}_{F} 0$ implies that there exists a polynomial

$f' \in F$ such that $f * w \longrightarrow^{\mathrm{p}}_{f'} 0$ and $\mathsf{HT}(f * w) \equiv \mathsf{HT}(f')u$ for some $u \in \mathcal{M}$. Note that F need not be a prefix standard basis.

2. On the other hand, if for every polynomial $f \in F$ and every element $w \in \mathcal{M}$ the polynomial $f * w$ has a prefix standard representation, this need not imply that F is prefix saturated. To see this, let us review example 4.4.37.
   Let $\Sigma = \{a, b, c, d, e\}$ and $T = \{ac \longrightarrow d, bc \longrightarrow e\}$ be a presentation of a monoid $\mathcal{M}$ with a length lexicographical ordering induced by $a \succ b \succ c \succ d \succ e$.
   Then for every polynomials f in the set $F = \{a + b, d + \lambda, e - \lambda\}$ and every element $w \in \mathcal{M}$ we can show that the multiple $f * w$ has a prefix standard representation. For the multiples $(a + b) * w = aw + bw$, $(d + \lambda) * w = dw + w$ and $(e - \lambda) * w = ew - w$, these are prefix standard representations. It remains to check the case $(a + b) * cw = dw + ew$. Since $d + e \longrightarrow^{\mathrm{p}}_{d+\lambda} e - \lambda \longrightarrow^{\mathrm{p}}_{e-\lambda} 0$, we have a prefix standard representation $dw + ew = (d + \lambda) * w + (e - \lambda) * w$, but as seen before, $dw + ew$ does not prefix reduce to zero using F in *one* step. ◇

Definition 4.4.42
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ **weakly prefix saturated**, if for all $f \in F$ and all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$, we have $\alpha \cdot f * w \xrightarrow{*}^{\mathrm{p}}_{F} 0$. ◇

If a set of polynomials F is weakly prefix saturated this implies that for all $f \in F$ and all $w \in \mathcal{M}$ the polynomial $f * w$, in case it is non-zero, has a prefix standard representation. Thus we can give the following procedure to compute reduced prefix Gröbner bases. Notice that in this procedure no prefix s-polynomials are computed. This is due to the fact that we are computing a basis of the right ideal generated by the input set such that no head terms of the polynomials in the basis are prefix reducible by the other polynomials in the set and hence no prefix s-polynomials exist.

Procedure: Reduced Prefix Gröbner Bases

Given: A finite set $F \subseteq \mathbf{K}[\mathcal{M}]$.
Find: $\textsc{Gb}(F)$, a (prefix) Gröbner basis of F.
Using: $\textsc{Sat}_p$ a prefix saturating procedure for polynomials.

$G_0 := \emptyset$;
$S_0 := F$;
$i := 0$;
while $S_i \neq \emptyset$ do
  $i := i + 1$;
  $q_i :=$ remove(S_{i-1});
  % Remove an element using a fair strategy
  $q_i' :=$ normalform$(q_i, \longrightarrow^{\mathrm{p}}_{G_{i-1}})$;
  % Compute a normal form using prefix reduction
  if $q_i' \neq 0$
    then $H_i := \{g \in G_{i-1} | \mathsf{HT}(g)$ is prefix reducible using $q_i'\}$;
      % These polynomials would have new head terms after prefix reduction

% using q_i'
$G_i := \text{reduce}((G_{i-1}\backslash H_i) \cup \{q_i'\});$
% $\text{reduce}(F) = \{\text{normalform}(f, \longrightarrow^{\text{p}}_{F\backslash\{f\}})|f \in F\}$[26]
% No head term of a polynomial in G_i is prefix reducible by the other
% polynomials in G_i
$S_i := S_{i-1} \cup H_i \cup \bigcup_{g\in(G_i\backslash G_{i-1})}(\text{SAT}_p(g)\backslash\{g\});$
else $G_i := G_{i-1};$
$S_i := S_{i-1};$
endif
endwhile
$\text{GB}(F) := G_i$

Notice that adding a polynomial to a set G_i we also add the saturating polynomials to S_i. This will ensure that the final set is weakly prefix saturated. But in doing so, the sets S_i will in general contain many unnecessary polynomials, as in removing a polynomial from a set G_i one could also think of changing the set S_i. We will later on realize this idea for the special case of free group rings. In order to show that the procedure actually constructs a prefix reduced Gröbner basis we first prove some lemmata. Let us start by showing that the sets $G_i \cup S_i$ constructed generate the same right ideal as F.

Lemma 4.4.43
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and G_i, S_i, $i \in \mathbf{N}$ the respective sets in procedure REDUCED PREFIX GRÖBNER BASES. *Then we have*

$$\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_i \cup S_i).$$

Proof :
For $i = 0$ we have $F = G_0 \cup S_0$ and hence $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_0 \cup S_0)$. On the other hand, for $i > 0$ let G_{i-1}, S_{i-1} be the respective sets before entering the **while** loop for its i-th iteration. Further let q_i be the polynomial chosen from S_{i-1} and q_i' a prefix normal from of q_i with respect to G_{i-1}.
Then in case $q_i' = 0$ we know $q_i \in \mathsf{ideal}_r(G_{i-1})$ and thus as $G_i = G_{i-1}$ and $S_i = S_{i-1}\backslash\{q_i\}$ we can conclude

$$\mathsf{ideal}_r(G_i \cup S_i) = \mathsf{ideal}_r(G_{i-1} \cup S_{i-1}) = \mathsf{ideal}_r(F).$$

In case $q_i' \neq 0$, then $\mathsf{ideal}_r(\text{reduce}((G_{i-1}\backslash H_i) \cup \{q_i'\})) = \mathsf{ideal}_r((G_{i-1}\backslash H_i) \cup \{q_i'\})$, $\mathsf{ideal}_r(G_{i-1} \cup \{q_i'\} \cup (S_{i-1}\backslash\{q_i\})) = \mathsf{ideal}_r(G_{i-1} \cup S_{i-1})$, $\mathsf{ideal}_r(\bigcup_{g\in(G_i\backslash G_{i-1})}(\text{SAT}_p(g)\backslash\{g\})) \subseteq \mathsf{ideal}_r(G_i)$ yield

$$\begin{aligned} & \mathsf{ideal}_r(G_i \cup S_i) \\ = \; & \mathsf{ideal}_r(G_i \cup (S_{i-1}\backslash\{q_i\}) \cup H_i \cup \bigcup_{g\in(G_i\backslash G_{i-1})} (\text{SAT}_p(g)\backslash\{g\})) \end{aligned}$$

[26]Notice that only the reducts of the polynomials are touched in this procedure.

$$\begin{aligned}
&= \mathsf{ideal}_r(G_i \cup (S_{i-1}\backslash\{q_i\}) \cup H_i) \\
&= \mathsf{ideal}_r(\text{reduce}((G_{i-1}\backslash H_i) \cup \{q_i'\}) \cup (S_{i-1}\backslash\{q_i\}) \cup H_i) \\
&= \mathsf{ideal}_r((G_{i-1}\backslash H_i) \cup \{q_i'\} \cup (S_{i-1}\backslash\{q_i\}) \cup H_i) \\
&= \mathsf{ideal}_r(G_{i-1} \cup \{q_i'\} \cup (S_{i-1}\backslash\{q_i\})) \\
&= \mathsf{ideal}_r(G_{i-1} \cup S_{i-1}) \\
&= \mathsf{ideal}_r(F).
\end{aligned}$$

q.e.d.

Remark 4.4.44

Taking a close look at the construction of the sets G_i, $i \in \mathbf{N}$, we find that the following observations for the head terms of the polynomials generated during computation hold: A set G_i, $i > 0$, is constructed from a set G_{i-1} by removing a polynomial q_i from S_i, reducing it to q_i' and in case q_i' is non-zero setting $G_i := \text{reduce}((G_{i-1}\backslash H_i)\cup\{q_i'\})$. Notice that H_i contains those polynomials in G_{i-1} that have a head term prefix reducible by q_i', i.e., these polynomials when reduced with q_i' will lead to polynomials with different head terms. Thus in removing these polynomials we find that reducing the polynomials in $(G_{i-1}\backslash H_i) \cup \{q_i'\}$ does not touch the head terms and since q_i' was in prefix normal form with respect to G_{i-1} it is not changed in this step. Hence we can conclude $q_i' \in G_i$ and $\mathsf{HT}(G_i) = \mathsf{HT}((G_{i-1}\backslash H_i) \cup \{q_i'\})$. Moreover, we know that every term in $\mathsf{HT}(H_i)$ has $\mathsf{HT}(q_i')$ as a proper prefix, i.e., all terms in $\mathsf{HT}(G_{i-1})$ have prefixes in the set $\mathsf{HT}(G_i)$. Therefore, if a polynomial is prefix reducible with respect to some set G_k it will also be prefix reducible with respect to all sets G_{k+n}, $n \in \mathbf{N}$. In particular, in case a polynomial g is removed from a set G_k no polynomial with head term $\mathsf{HT}(g)w$, $w \in \mathcal{M}$, will be added to a later set G_{k+n}, $n \in \mathbf{N}^+$. This implies that no cycles occur.
$\diamond$

The next lemma states that these properties of the sets G_i carry over to the set G. This is obvious in case the procedure terminates.

Lemma 4.4.45

Let G be the set generated by procedure Reduced Prefix Gröbner Bases. *Then if $f \in G_k$ for some $k \in \mathbf{N}$ there exists a polynomial $g \in G$ such that $\mathsf{HT}(g)$ is a prefix of $\mathsf{HT}(f)$.*

Proof :

In case our procedure terminates or $f \in G$ we are done at once. Hence, let us assume there exists a polynomial f such that $f \in G_k$ for some $k \in \mathbf{N}$ but no $g \in G$ exists such that $\mathsf{HT}(g)$ is a prefix of $\mathsf{HT}(f)$. Further let f be a counter-example with minimal head term. As $f \notin G$ there exists an index $j > k$ such that $f \in G_{j-1}$ but $f \notin G_j$. Let $q_j' \neq 0$ be the polynomial computed in this j-th execution of the **while** loop. In case $\mathsf{HT}(f)$ is prefix reducible by q_j', we know that $\mathsf{HT}(q_j')$ is a proper prefix of $\mathsf{HT}(f)$ and hence

$q'_j \in G_j$ implies the existence of a polynomial $g \in G$ such that $\mathsf{HT}(g)$ is a prefix of $\mathsf{HT}(q'_j)$ and hence of $\mathsf{HT}(f)$, contradicting our assumption. On the other hand the case that f is replaced in G_{j-1} by a polynomial f' after reducing the set $(G_{j-1} \backslash H_j) \cup \{q'_j\}$ with $\mathsf{HT}(f) = \mathsf{HT}(f')$ cannot occur infinitely often since this would imply the existence of an infinite prefix reduction sequence $f \xrightarrow{+}^{\mathrm{p}} f_0 \xrightarrow{+}^{\mathrm{p}} f_1 \ldots$ inducing an infinite strictly descending chain $f > f_0 > f_1 \ldots$ in $\mathbf{K}[\mathcal{M}]$ (compare lemma 4.4.7). Hence there exists an index $l \geq j$ such that for a descendant f' of f either no more changes occur, i.e., $f' \in G$, or f' is removed from G_l because its head term is prefix reducible by a polynomial q'_{l+1} added to G_{l+1} where $\mathsf{HT}(q'_{l+1})$ is a proper prefix of $\mathsf{HT}(f')$ and then we can now proceed as above and get a contradiction.

q.e.d.

Lemma 4.4.46
Let G be the set generated by procedure Reduced Prefix Gröbner Bases. *Then if $f \in S_k \cup G_k$ for some $k \in \mathbf{N}$, f has a prefix standard representation with respect to G.*

Proof :
In proving our claim we will distinguish two cases. Suppose first that $f \in G_k$ but f has no prefix standard representation with respect to G. Let us further assume that f is a minimal counter-example. Since $f \notin G$ there exists an index $j > k$ such that $f \in G_{j-1}$, but $f \notin G_j$. Let $q'_j \neq 0$ be the polynomial corresponding to this **while** loop. In case f is removed since $\mathsf{HT}(q'_j)$ is a proper prefix of $\mathsf{HT}(f)$ it is put into S_j. As we are using a fair strategy to remove elements from the respective sets S_i, there exists an index $l > j$ such that f is chosen to compute q'_l. Then $f \xrightarrow{+}^{\mathrm{p}}_{G_{l-1}} q'_l$, $q'_l < f$ and either $q'_l = 0$ or $q'_l \in G_l$. In both cases f has a prefix standard representation with respect to $G_{l-1} \cup \{q'_l\}$ and by lemma 4.4.10 also with respect to $G_l = \mathrm{reduce}((G_{l-1} \backslash H_l) \cup \{q'_l\})$. Note that all polynomials involved in this prefix standard representation are in G_l and are smaller than f, i.e., they have prefix standard representations with respect to G yielding such a representation for f contradicting our assumption. In case f is replaced by a polynomial f' while computing the set $G_j = \mathrm{reduce}((G_{j-1} \backslash H_j) \cup \{q'_j\})$ we know that all reductions involved take place at $\mathsf{RED}(f)$ and hence all polynomials used for prefix reduction are smaller than f. So are again the polynomials used to prefix reduce these polynomials and so on. Then lemma 4.4.10 gives us the existence of a prefix standard representation with respect to G_l for f and the existence of prefix standard representations with respect to G for all polynomials involved in this representation yield a prefix standard representation with respect to G for f. On the other hand, suppose that $f \in S_k$. Then let $l \geq k$ be the iteration where f is chosen to compute q'_l, i.e., $f \xrightarrow{*}^{\mathrm{p}}_{G_{l-1}} q'$. Thus f has a prefix standard representation with respect to $G_l = \mathrm{reduce}((G_{l-1} \backslash H_l) \cup \{q'_l\})$ and since every polynomial in this set has a prefix standard representation with respect to G, lemma 4.4.10 yields the existence of a prefix standard representation for f

q.e.d.

Theorem 4.4.47
Let G be the set generated by procedure Reduced Prefix Gröbner Bases *on a finite input $F \subseteq \mathbf{K}[\mathcal{M}]$. Then G is a reduced prefix Gröbner basis.*

Proof :
In case procedure Reduced Prefix Gröbner Bases terminates we have $G = G_k$ for some $k \in \mathbf{N}$. Otherwise, as we assume that elements are removed from the respective sets S_i in a fair way, we have $\bigcup_{i \geq 0} \bigcap_{j \geq i} S_j = \emptyset$ and $G = \bigcup_{i \geq 0} \bigcap_{j \geq i} G_j$.
By construction no prefix s-polynomials exist for the polynomials in G. Hence, in order to show that G is a Gröbner basis, by theorem 4.4.39 it remains to show that $g \in G$ implies that for all $w \in \mathcal{M}$ the multiple $g * w$ has a prefix standard representation with respect to G. In case $g \in G$, there exists an index $k \in \mathbf{N}$ such that g is added to G_k and hence $\mathrm{SAT}_p(g) \subseteq G_k \cup S_k$. Hence we know $g * w \longrightarrow^{\mathrm{p}}_{g' \in \mathrm{SAT}_p(g)} 0$ and $g' \in S_k \cup G_k$. Thus lemma 4.4.46 yields the existence of a prefix standard representation for g' with respect to G which can be extended to a prefix standard representation for $g * w$ by lemma 4.4.10.

q.e.d.

Theorem 4.4.48
Let F be a finite set of polynomials in $\mathbf{K}[\mathcal{M}]$. In case $\mathsf{ideal}_r(F)$ has a finite reduced prefix Gröbner basis, procedure Reduced Prefix Gröbner Basis *terminates.*

Proof :
Theorem 4.4.20 implies that reduced prefix Gröbner bases are unique up to multiplication with coefficients. Hence in case a finite reduced prefix Gröbner basis exists, all reduced prefix Gröbner bases must be finite including the one computed by procedure Reduced Prefix Gröbner Basis.

q.e.d.

Theorem 4.4.49
Let $\mathcal{M}$ be a finite monoid presented by the finite convergent semi-Thue system. Further let the prefix saturation procedure SAT_p be specified e.g. as in procedure Prefix Saturation. *Then the procedure* Reduced Prefix Gröbner Bases *terminates.*

Proof :
This follows immediately as for a reduced prefix Gröbner basis all head terms are different elements of $\mathcal{M}$ and since $\mathcal{M}$ is finite such a basis must also be finite.

q.e.d.

Theorem 4.4.50
Let $\mathcal{M}$ be a free monoid finitely generated by an alphabet Σ and presented by the

finite convergent semi-Thue system $(\Sigma, \emptyset)$. *Further let the prefix saturation procedure* $\textsc{Sat}_p$ *be specified as* $\textsc{Sat}_p(p) = \{p\}$ *for a polynomial* $p \in \mathbf{K}[\mathcal{M}]$. *Then the procedure* Reduced Prefix Gröbner Bases *terminates.*

Proof :
Let $F \subseteq \mathbf{K}[\mathcal{M}]$ be the finite input set of polynomials. Reviewing the definition of prefix reduction we find that all polynomials added must have head terms of length less equal to $\max\{|\mathsf{HT}(f)| \mid f \in F\} = K$. Hence there exists a prefix Gröbner basis whose head terms are all different and bounded in their length by K, i.e., there exists a finite prefix Gröbner basis.

q.e.d.

Note that with the modifications described in theorem 4.4.50 procedure Reduced Prefix Gröbner Bases directly corresponds to Mora's algorithm for computing Gröbner bases for finitely generated right ideals in non-commutative polynomial rings as specified in [Mo85] (compare also section 3.1).

Chapter 5 will give some more detailed examples where finite reduced prefix Gröbner bases can be computed, namely in group rings of the class of free groups, the class of plain groups and the class of context-free groups.

Let us close this section by considering our monoid ring as a quotient structure of a free monoid ring. As we have mainly investigated the right ideal congruence in monoid rings, we will modify our quotient in order to introduce right reduction. In the following we will assume that (Σ, T) is a finite, convergent, and even reduced presentation of a monoid $\mathcal{M}$. As before, Σ^* is a free monoid generated by Σ with concatenation as multiplication. Let $P_T = \{l - r \mid (l, r) \in T\}$ be the set of polynomials in $\mathbf{K}[\Sigma^*]$ associated to T. Further let $\tilde{T} = \{(xl, xr) \mid (l, r) \in T, x \in \Sigma^* \text{ and no proper prefix of } xl \text{ is } T\text{-reducible}\}$ denote the **prefix-rewriting system** belonging to T as described in [KuMa89] and we can associate the set of polynomials $P_{\tilde{T}} = \{xl - xr \mid (xl, xr) \in \tilde{T}\}$ to $\tilde{T}$.

Lemma 4.4.51
Let $\mathcal{M}$ *be a monoid with a finite, convergent, reduced presentation* (Σ, T). *Then the following statements hold:*

1. $\longrightarrow^{\mathrm{p}}_{P_{\tilde{T}}}$ *is confluent on* $\mathbf{K}[\Sigma^*]$.
2. $\mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T) = \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ *in* $\mathbf{K}[\Sigma^*]$.
3. *The quotient* $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ *is a ring.*
4. *The monoid ring* $\mathbf{K}[\mathcal{M}]$ *is isomorphic to the quotient ring* $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.

Proof :

1. Since the prefix reduction induced by $P_{\tilde{T}}$ is Noetherian, in order to show confluence, we only have to take a look at critical pairs of different polynomials $xl_i - xr_i, x'l_j - x'r_j \in P_{\tilde{T}}$, caused by a superposition $xl_i \equiv x'l_jz$, where $z \in \Sigma^*$. We have to distinguish two cases:

   (a) Let $|x| < |x'|$, i.e., $x' \equiv xw, w \in \Sigma^*\backslash\{\lambda\}$.
   Looking at $xl_i \equiv xwl_jz$ we get $l_i \equiv wl_jz$ contradicting the fact that T is supposed to be reduced.

   (b) Let $|x| \geq |x'|$, i.e., $x \equiv x'w, w \in \Sigma^*$.
   Looking at $x'wl_i \equiv x'l_jz$ we have to consider two cases. In case $z \neq \lambda$ we find that $x'l_j$ is a proper prefix of $xl_i \equiv x'wl_i$ and as $x'l_j$ is T-reducible, this is a contradiction to the definition of $\tilde{T}$. The case $z = \lambda$ likewise gives us a contradiction to T being reduced, as $wl_i \equiv l_j$.

   Hence the set $P_{\tilde{T}}$ leads to no superpositions, and therefore is confluent.

2. $\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}}) \subseteq \mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$ follows immediately. To show $\mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T) \subseteq \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ it suffices to prove that $x \in \Sigma^*$ and $l - r \in P_T$ implies $xl - xr \in \mathsf{ideal}_r(P_{\tilde{T}})$. In case $xl - xr \in P_{\tilde{T}}$ there is nothing to show. Suppose $xl - xr \notin P_{\tilde{T}}$, i.e., we can decompose xl into $xl \equiv x'l'w$ for some $x', l', w \in \Sigma^*$, where $x'l'$ is the first proper T-reducible prefix of xl. Then we get the following reduction sequences, where $\longrightarrow^{\mathrm{l}}_T$ stands for leftmost reduction:

   $$xr \longleftarrow_T x\underline{l} \equiv x'\underline{l'}w \longrightarrow^{\mathrm{l}}_T x'r'w.$$

   Since T is convergent this situation is confluent, even when we restrict the reduction strategy to left-most reduction. As a consequence there exists an element $z \in IRR(T)$ such that $xr \stackrel{*}{\longrightarrow}^{\mathrm{l}}_T z$ and $xl \longrightarrow^{\mathrm{l}}_T x'r'w \stackrel{*}{\longrightarrow}^{\mathrm{l}}_T z$. This means that xl and xr have a common normal form with respect to left-most reduction. Reviewing the definition of left-most reduction, we find that a reduction step $ul_1v \longrightarrow_T ur_1v$ with $(l_1, r_1) \in T, u, v \in \Sigma^*$ is a left-most reduction step if and only if and no proper prefix of ul_1 is T-reducible. This can be compared to subtracting the polynomial $ul_1v - ur_1v$ from ul_1v in $\mathbf{K}[\Sigma^*]$ and by the definition of $P_{\tilde{T}}$ we know that $ul_1 - ur_1 \in P_{\tilde{T}}$. Therefore $ul_1v \longrightarrow^{\mathrm{l}}_T ur_1v$ can be simulated in $\mathbf{K}[\Sigma^*]$ by prefix reduction as follows:

   $$ul_1v \longrightarrow^{\mathrm{p}}_{P_{\tilde{T}}} ul_1v - (ul_1 - ur_1) * v = ur_1v.$$

   Hence, $ul_1v = ur_1v + (ul_1 - ur_1) * v$ and any reduction sequence $w \stackrel{*}{\longrightarrow}^{\mathrm{p}}_{P_{\tilde{T}}} y$ induces $w = y + h$ for some $h \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. As a consequence, $xl \stackrel{*}{\longrightarrow}^{\mathrm{l}}_{P_{\tilde{T}}} z$ and $xr \stackrel{*}{\longrightarrow}^{\mathrm{l}}_{P_{\tilde{T}}} z$ imply that $xl = z + g$ and $xyr = z + g'$ for some $g, g' \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Therefore, $xl - xr = g - g' \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.

3. This follows immediately as $\mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T) = \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ in $\mathbf{K}[\Sigma^*]$ implies that $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ and $\mathbf{K}[\Sigma^*]/\mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T)$ are equal as sets and even as rings.

4. Let $\varphi : \mathbf{K}[\Sigma^*] \longrightarrow \mathbf{K}[\mathcal{M}]$ be the natural ring homomorphisms defined by setting $\varphi(\sum_{i=1}^k \alpha_i \cdot w_i) = \sum_{i=1}^k \alpha_i \cdot [w_i]_{\mathcal{M}}$ with $\alpha_i \in \mathbf{K}, w_i \in \Sigma^*$. We will show that the kernel of φ is a two-sided ideal in $\mathbf{K}[\Sigma^*]$, namely $\mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_T) = \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$, and hence $\mathbf{K}[\mathcal{M}]$ is isomorphic to the ring $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. To see our claim we prove that for any polynomial $g \in \mathbf{K}[\Sigma^*]$ we have $\varphi(g) = 0$ if and only if $g \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. First for $g = \sum_{i=1}^k \alpha_i \cdot w_i$ with $\alpha_i \neq 0$ we show that $\varphi(g) = 0$ implies $g \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ by induction on k. In case $k = 0$ we have $g = 0$ and are done. The case $k = 1$ is not possible, as $g = \alpha \cdot w$ and $\alpha \cdot [w]_{\mathcal{M}} = 0$ imply $\alpha = 0$ contradicting our assumption. In the induction step let us assume $g = \sum_{i=1}^k \alpha_i \cdot w_i + \alpha_{k+1} \cdot w_{k+1}$. Then $\varphi(g) = \sum_{i=1}^{k+1} \alpha_i \cdot [w_i]_{\mathcal{M}} = 0$ gives us $\sum_{i=1}^k \alpha_i \cdot [w_i]_{\mathcal{M}} = -\alpha_{k+1} \cdot [w_{k+1}]_{\mathcal{M}}$ and since $\alpha_{k+1} \neq 0$ there exists $1 \leq j \leq k$ such that $[w_j]_{\mathcal{M}} = [w_{k+1}]_{\mathcal{M}}$. Hence $w_j \overset{*}{\longleftrightarrow}{}^{\mathrm{p}}_{P_{\tilde{T}}} w_{k+1}$ and $w_{k+1} - w_j \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Now we can set $\sum_{i=1}^{k+1} \alpha_i \cdot [w_i]_{\mathcal{M}} = \sum_{i=1}^k \beta_i \cdot [w_i]_{\mathcal{M}}$ with $\beta_i = \alpha_i$ for $1 \leq i \leq k$, $i \neq j$ and $\beta_j = \alpha_j + \alpha_{k+1}$. Thus, as $\varphi(\sum_{i=1}^{k+1} \alpha_i \cdot [w_i]_{\mathcal{M}}) = \varphi(\sum_{i=1}^k \beta_i \cdot [w_i]_{\mathcal{M}}) = 0$, the induction hypothesis yields $\sum_{i=1}^k \beta_i \cdot w_i \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Furthermore, $\sum_{i=1}^k \beta_i \cdot w_i = g - \alpha_{k+1} \cdot w_{k+1} + \alpha_{k+1} \cdot w_j$ and hence, as $w_{k+1} - w_j \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$, $g \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ holds. To see on the other hand that $g \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ implies $\varphi(g) = 0$, let $g = \sum_{i=1}^n \gamma_i \cdot (x_i l_i - x_i r_i) * y_i \in \mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Remember that $[x_i l_i y_i]_{\mathcal{M}} = [x_i r_i y_i]_{\mathcal{M}}$ and hence $\varphi(x_i l_i y_i - x_i r_i y_i) = 0$. This immediately yields $\varphi(g) = 0$ and we are done.

q.e.d.

Thus we have set up a one-to-one correspondence between monoid rings and certain quotient rings of free monoid rings. Now let us state how computation in our quotient structure is done. For a polynomial $p = \sum_{i=1}^m \alpha_i \cdot t_i \in \mathbf{K}[\Sigma^*]$ we define

$$[p]_{\mathsf{ideal}_r(P_{\tilde{T}})} = \sum_{i=1}^m \alpha_i \cdot [t_i]_{\mathcal{M}} = \sum_{i=1}^m \alpha_i \cdot (t_i){\downarrow}_{P_{\tilde{T}}}$$

and we will write p instead of $[p]_{\mathsf{ideal}_r(P_{\tilde{T}})}$ to denote elements of $\mathbf{K}[\Sigma^*]/\mathsf{ideal}(P_{\tilde{T}})$ or $p{\downarrow}_{P_{\tilde{T}}}$ if we want to turn a polynomial in $\mathbf{K}[\Sigma^*]$ into an element of the quotient.

Definition 4.4.52
Let $p, q \in \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Then we can define **addition** and **multiplication** as follows:

1. $p \oplus q = [p +_{\mathbf{K}[\Sigma^*]} q]_{\mathsf{ideal}_r(P_{\tilde{T}})} = (p +_{\mathbf{K}[\Sigma^*]} q){\downarrow}_{P_{\tilde{T}}}$

2. $p \otimes q = [p *_{\mathbf{K}[\Sigma^*]} q]_{\mathsf{ideal}_r(P_{\tilde{T}})} = (p *_{\mathbf{K}[\Sigma^*]} q){\downarrow}_{P_{\tilde{T}}}$

where $+_{\mathbf{K}[\Sigma^*]}$ and $*_{\mathbf{K}[\Sigma^*]}$ are the corresponding ring operations in $\mathbf{K}[\Sigma^*]$. ◇

Then $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ together with $\oplus$ and $\otimes$ is a ring with unit. We will now introduce quotient prefix reduction to the quotient structure by lifting prefix reduction.

Definition 4.4.53
Let p, q, f be some polynomials in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Then we set $p \Longrightarrow_f^{\mathrm{p}} q$ at a monomial $\alpha \cdot t$ of p if there exists a polynomial $q' \in \mathbf{K}[\Sigma^*]$ such that $p \longrightarrow_f^{\mathrm{p}} q'$ at $\alpha \cdot t$ and $q = q' \downarrow_{P_{\tilde{T}}}$, in particular $p \longrightarrow_f^{\mathrm{p}} q' \overset{*}{\longrightarrow}_{P_{\tilde{T}}}^{\mathrm{p}} q$ where q is in prefix normal form with respect to $P_{\tilde{T}}$. We can define $\overset{*}{\Longrightarrow}^{\mathrm{p}}$, $\overset{+}{\Longrightarrow}^{\mathrm{p}}$, $\overset{n}{\Longrightarrow}^{\mathrm{p}}$ as usual. Reduction by a set $F \subseteq \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ is denoted by $p \Longrightarrow_F^{\mathrm{p}} q$ and stands for $p \Longrightarrow_f^{\mathrm{p}} q$ for some $f \in F$, also written as $p \Longrightarrow_{f \in F}^{\mathrm{p}} q$. $\diamond$

Then for this reduction we can state:

Lemma 4.4.54
Let F be a set of polynomials and p, q some polynomials in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Then the following statements hold:

1. $\Longrightarrow_F \subseteq \overset{*}{\longrightarrow}_{F \cup P_{\tilde{T}}}^{\mathrm{p}}$.
2. $p \Longrightarrow_F q$ *implies* $p > q$.
3. $\Longrightarrow_F$ *is Noetherian.*

Proof :

1. This follows by the definition of reduction, since $p \Longrightarrow_{f \in F}^{\mathrm{p}} q$ can be simulated by $p \longrightarrow_f^{\mathrm{p}} q' \overset{*}{\longrightarrow}_{P_{\tilde{T}}}^{\mathrm{p}} q$.
2. This follows immediately as prefix reduction already has this property.
3. This follows from the fact that prefix reduction is Noetherian.

q.e.d.

But many other properties of prefix reduction on $\mathbf{K}[\Sigma^*]$ are lost.

Lemma 4.4.55
Let p, q, h be some polynomials in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$, $h \neq 0$.

1. $q < p$ *no longer implies* $q \otimes h < p \otimes h$.
2. $p \Longrightarrow_p^{\mathrm{p}} 0$ *no longer implies* $p \otimes h \Longrightarrow_p^{\mathrm{p}} 0$.

Example 4.4.56
Let $\Sigma = \{a\}$ and $P_T = \{a^2 - \lambda\}$. Then $p = a$, $q = \lambda$ and $h = a$ gives us an appropriate counter-example, since we have $q < p$ but $q \otimes h = a > p \otimes h = \lambda$, and $p \otimes h = \lambda$ cannot be quotient prefix reduced by p. $\diamond$

We now can give a definition for Gröbner bases in this setting.

Definition 4.4.57
A set $G \subseteq \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ is said to be a **prefix Gröbner basis** with respect to $\Longrightarrow^{\mathrm{p}}$, if

1. $\overset{*}{\Longleftrightarrow}^{\mathrm{p}}_G \; = \; \equiv_{\mathsf{ideal}_r(G)}$, and
2. $\Longrightarrow^{\mathrm{p}}_G$ is confluent.

Reviewing example 4.4.56 we find that a polynomial alone need no longer be a prefix Gröbner basis of the right ideal it generates. The set $\{a\}$ is no prefix Gröbner basis as we do not have $\overset{*}{\Longleftrightarrow}^{\mathrm{p}}_a \; = \; \equiv_{\mathsf{ideal}_r(a)}$.

The following lemma gives a sufficient condition for confluence and we will see later on that we can also regain the expressiveness of the right ideal congruence.

Lemma 4.4.58
Let $P_{\tilde{T}}$ be a prefix Gröbner basis in $\mathbf{K}[\Sigma^*]$, $F \subseteq \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ and let $\longrightarrow^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$ be confluent on $\mathbf{K}[\Sigma^*]$. Then $\Longrightarrow^{\mathrm{p}}_F$ is confluent on $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.

Proof :
Suppose there exist $f, h_1, h_2 \in \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ such that $f \Longrightarrow^{\mathrm{p}}_F h_1$ and $f \Longrightarrow^{\mathrm{p}}_F h_2$. Then we can view these polynomials as elements of $\mathbf{K}[\Sigma^*]$ and simulate $\Longrightarrow^{\mathrm{p}}_F$ by $\longrightarrow^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$ giving us $f \overset{*}{\longrightarrow}^{\mathrm{p}}_{F \cup P_{\tilde{T}}} h_1$ and $f \overset{*}{\longrightarrow}^{\mathrm{p}}_{F \cup P_{\tilde{T}}} h_2$. Hence, as $\longrightarrow^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$ is confluent, there exists a polynomial $g \in \mathbf{K}[\Sigma^*]$ such that $h_1 \overset{*}{\longrightarrow}^{\mathrm{p}}_{F \cup P_{\tilde{T}}} g$ and $h_2 \overset{*}{\longrightarrow}^{\mathrm{p}}_{F \cup P_{\tilde{T}}} g$. Since $\longrightarrow^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$ is convergent we can use the following reduction strategy:

1. Do as many prefix reduction steps as possible using $P_{\tilde{T}}$.
2. If possible apply one prefix reduction step using F and return to 1.

We stop as soon as no more prefix reduction steps are possible. Note that we can combine these reduction steps and add some more using $P_{\tilde{T}}$ to get a sequence as required in the definition of $\Longrightarrow^{\mathrm{p}}_F$. This gives us that $h_1 \overset{*}{\Longrightarrow}^{\mathrm{p}}_F \tilde{g}$ and $h_2 \overset{*}{\Longrightarrow}^{\mathrm{p}}_F \tilde{g}$, where $\tilde{g} = g\!\downarrow_{P_{\tilde{T}}}$.

q.e.d.

Reviewing example 4.4.56 we see that the converse is not true.

Example 4.4.59
Let $\Sigma = \{a\}$ and $P_T = \{a^2 - \lambda\}$. Then $P_{\tilde{T}} = P_T$. For $F = \{a\}$ we get that $\Longrightarrow^{\mathrm{p}}_a$ is confluent on $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$, but for the set $F \cup P_{\tilde{T}} = \{a, a^2 - \lambda\}$, $\longrightarrow^{\mathrm{p}}_{\{a, a^2 - \lambda\}}$ is not confluent on $\mathbf{K}[\Sigma^*]$. ◇

In order to use the previous lemma to sketch how a Gröbner basis with respect to $\Longrightarrow^{\mathrm{p}}$ can be computed, we review the definition of prefix s-polynomials for the special case of the free monoid ring $\mathbf{K}[\Sigma^*]$. Given two polynomials $p_1, p_2 \in \mathbf{K}[\Sigma^*]$ such that $\mathsf{HT}(p_1) \equiv \mathsf{HT}(p_2)w$ for some $w \in \Sigma^*$, this gives us the prefix s-polynomial

$$\mathsf{spol}(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w.$$

Then we can compute a Gröbner basis as follows:

Compute a Gröbner basis G' of $F \cup P_{\tilde{T}}$ in $\mathbf{K}[\Sigma^*]$[27] with respect to prefix reduction without changing the polynomials in $P_{\tilde{T}}$. Then the set $G := G' \backslash P_{\tilde{T}}$ is a Gröbner basis of F in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.

Computing a prefix Gröbner basis of $F \cup P_{\tilde{T}}$ in $\mathbf{K}[\Sigma^*]$ three kinds of prefix s-polynomials can arise:

1. $f, g \in P_{\tilde{T}}$: Then the corresponding prefix s-polynomial can be omitted as $P_{\tilde{T}}$ is already a Gröbner basis.

2. $f, g \in F$: Then the prefix s-polynomial corresponds to the prefix s-polynomial as defined in section 4.4.

3. $f \in F$, $g \in P_{\tilde{T}}$: Then the s-polynomial corresponds to the process of saturating f as described in procedure PREFIX SATURATION on page 102. In particular this can be compared to overlapping the head term of f with the rule $l \longrightarrow r \in T$ where $g = xl - xr$. Notice that although $P_{\tilde{T}}$ maybe infinite only finitely many such overlaps can arise.

The correctness of this approach follows from the next theorem.

Theorem 4.4.60
Let $P_{\tilde{T}} \subseteq \mathbf{K}[\Sigma^*]$ be a prefix Gröbner basis and $F \subseteq \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Then the following statements are equivalent:

1. *F is a prefix Gröbner basis in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.*

2. (a) *For all $f, g \in F$ we have $\mathsf{spol}(f, g) \overset{*}{\Longrightarrow}^{\mathrm{p}}_F 0$ and*

   (b) *for all $f \in F$, $g \in P_{\tilde{T}}$ we have $(\mathsf{spol}(f, g))\!\downarrow_{P_{\tilde{T}}} \overset{*}{\Longrightarrow}^{\mathrm{p}}_F 0$.*

Proof :
$1 \Longrightarrow 2$: This follows immediately from the fact that the polynomials themselves are elements of $\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})}(F)$ and therefore congruent to zero. Thus the confluence of F implies that they can be quotient prefix reduced to zero using F.

[27]Note that as $P_{\tilde{T}}$ in general is infinite we have to use additional information on the structure of $P_{\tilde{T}}$ to specify critical overlaps between polynomials in F and $P_{\tilde{T}}$.

$2 \Longrightarrow 1$: The items (a) and (b) imply that $F \cup P_{\tilde{T}}$ is a prefix Gröbner basis in $\mathbf{K}[\Sigma^*]$, i.e., $\longrightarrow^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$ is confluent. Hence, by lemma 4.4.58, $\Longrightarrow^{\mathrm{p}}_{F}$ is also confluent. It remains to show that $\overset{*}{\Longleftrightarrow}^{\mathrm{p}}_{F} = \equiv_{\mathsf{ideal}_r(F)}$. Obviously, $\overset{*}{\Longleftrightarrow}^{\mathrm{p}}_{F} \subseteq \equiv_{\mathsf{ideal}_r(F)}$. On the other hand, let p and q be polynomials in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. Then $p \equiv_{\mathsf{ideal}_r(F)} q$ in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ implies $p \equiv_{\mathsf{ideal}_r(F \cup P_{\tilde{T}})} q$ in $\mathbf{K}[\Sigma^*]$. Further, as $F \cup P_{\tilde{T}}$ is a prefix Gröbner basis in $\mathbf{K}[\Sigma^*]$, we know $\equiv_{\mathsf{ideal}_r(F \cup P_{\tilde{T}})} = \overset{*}{\longleftrightarrow}^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$, and as $\longrightarrow^{\mathrm{p}}_{F \cup P_{\tilde{T}}}$ is confluent, $p \overset{*}{\longleftrightarrow}^{\mathrm{p}}_{F \cup P_{\tilde{T}}} q$ implies $p \downarrow_{F \cup P_{\tilde{T}}} q$. Thus, as in lemma 4.4.58, we can conclude $p \Downarrow_F q$ giving us $p \overset{*}{\Longleftrightarrow}^{\mathrm{p}}_{F} q$. This completes the proof that F is a prefix Gröbner basis in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.

q.e.d.

We now move on to compare prefix reduction defined here for the quotient structure to prefix and right reduction in the corresponding monoid ring. For a polynomial $p \in \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ let $\tilde{p}$ be the corresponding polynomial in the monoid ring $\mathbf{K}[\mathcal{M}]$. Note that we can identify the elements of $\mathcal{M}$ with their normalforms with respect to $P_{\tilde{T}}$ in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$.

Lemma 4.4.61
Let p, q, f be some polynomials in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ and let $\tilde{p}, \tilde{q}, \tilde{f}$ be the corresponding polynomials in $\mathbf{K}[\mathcal{M}]$. Then $p \Longrightarrow^{\mathrm{p}}_{f} q$ if and only if $\tilde{p} \longrightarrow^{\mathrm{p}}_{\tilde{f}} \tilde{q}$.

Proof :
Before entering the proof of our claim let us first take a closer look at reduction in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$. If $p \Longrightarrow^{\mathrm{p}}_{f} q$ at a monomial $\alpha \cdot t$ with $t \equiv \mathsf{HT}(f)u$, then we can express this reduction step by $p \longrightarrow^{\mathrm{p}}_{f} q' \overset{*}{\longrightarrow}^{\mathrm{p}}_{P_{\tilde{T}}} q$ and we have $q' = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f *_{\mathbf{K}[\Sigma^*]} u$ and $q = p \oplus (-\alpha) \cdot \mathsf{HC}(f)^{-1} \cdot f \otimes u$. In this context it is easy to see that $p \Longrightarrow^{\mathrm{p}}_{f} q$ implies $\tilde{p} \longrightarrow^{\mathrm{p}}_{\tilde{f}} \tilde{q}$. On the other hand, prefix reduction in the monoid ring requires that the head term of the polynomial is a prefix of the term to be reduced. Hence, such a prefix reduction step can be split into first doing one step using prefix reduction in the free monoid ring and then normalizing the new monomials using $P_{\tilde{T}}$.

q.e.d.

Corollary 4.4.62
Let $G \subseteq \mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ and let $\tilde{G}$ be the corresponding set in $\mathbf{K}[\mathcal{M}]$. Then G is a prefix Gröbner basis with respect to $\Longrightarrow^{\mathrm{p}}$ if and only if $\tilde{G}$ is a prefix Gröbner basis with respect to $\longrightarrow^{\mathrm{p}}$. □

Obviously, then $\Longrightarrow^{\mathrm{p}}$ must be weaker than $\longrightarrow^{\mathrm{r}}$.

Corollary 4.4.63
Let p, q, f be some polynomials in $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ and let $\tilde{p}, \tilde{q}, \tilde{f}$ be the corresponding polynomials in $\mathbf{K}[\mathcal{M}]$. Then $p \Longrightarrow^{\mathrm{p}}_{f} q$ implies $\tilde{p} \longrightarrow^{\mathrm{r}}_{\tilde{f}} \tilde{q}$ but not vice versa.
□

Example 4.4.64
Let $\Sigma = \{a\}$ and $T = \{a^3 \longrightarrow \lambda\}$ be a presentation of a group $\mathcal{G}$ with a length-lexicographical ordering on $\mathcal{G}$. Further let $\tilde{p} = a$ and $\tilde{f} = a^2$ be polynomials in $\mathbf{K}[\mathcal{G}]$. Then $\tilde{p} \longrightarrow^{\mathrm{r}}_{\tilde{f}} 0$, but for the corresponding polynomials $p = a$ and $f = a^2$ in the quotient $\mathbf{K}[\Sigma^*]/\mathsf{ideal}_r^{\mathbf{K}[\Sigma^*]}(P_{\tilde{T}})$ we have $p \not\Longrightarrow^{\mathrm{p}}_f$ as a^2 is no prefix of a. Notice that the set $\{\tilde{f}\}$ itself is a Gröbner basis with respect to $\longrightarrow^{\mathrm{r}}$ but neither with respect to $\Longrightarrow^{p}$ nor $\longrightarrow^{\mathrm{p}}$. $\diamond$

4.5 The Concept of Commutative Reduction

The concept of prefix reduction as introduced in the previous section is a very strong restriction as only few classes of monoids respectively groups allow finite prefix Gröbner bases. For example, commutative monoids in general cannot be treated by this approach. Let $\Sigma = \{a, b\}$ be generators for a free commutative monoid $\mathcal{T} = \{a^i b^j \mid i, j \in \mathbf{N}\}$ with a length-lexicographical ordering induced by $b \succ a$. Then the right ideal generated by the polynomial $ab + \lambda$ does not have a finite prefix Gröbner basis. Therefore, we will introduce another way of weakening right reduction for commutative monoids which makes use of the fact that they can be presented by ordered words and semi-Thue systems modulo commutativity. We will introduce the same ideas used in prefix reduction by generalizing the term "prefix" in order to refine right reduction. Remember that for an alphabet $\Sigma = \{a_1, \ldots, a_n\}$, $\mathcal{T} = \{a_1^{i_1} \ldots a_n^{i_n} \mid i_j \in \mathbf{N}\}$ is a free commutative monoid with multiplication $\circ_{\mathcal{T}}$ (compare definition 2.4.15). We can define a tuple-ordering on $\mathcal{T}$ as follows:

Definition 4.5.1
Let $u \equiv a_1^{i_1} \ldots a_n^{i_n}, v \equiv a_1^{j_1} \ldots a_n^{j_n}$ be two elements of $\mathcal{T}$. We define $u \geq_{\mathrm{tup}} v$ if for each $1 \leq l \leq n$ we have $i_l \geq j_l$. Further we define $u >_{\mathrm{tup}} v$ if $u \geq_{\mathrm{tup}} v$ and $i_l > j_l$ for some $1 \leq l \leq n$. $\diamond$

Notice that for terms $u, v \in \mathcal{T}$, u is a divisor of v if and only if $u \leq_{\mathrm{tup}} v$. u then can be viewed as a "commutative prefix" of v and we have similar properties as in the case of prefixes in the free monoid Σ^*.

Let $\mathcal{M}$ be given by a semi-Thue systems modulo commutativity (Σ, T_c) which is convergent with respect to an admissible total ordering $\succeq_{\mathcal{T}}$ on $\mathcal{T}$ (e.g. a length-lexicographical ordering)[28]. Then the elements of $\mathcal{M}$ are denoted by irreducible ordered words, i.e., $\mathcal{M} \subseteq \mathcal{T}$, and $\succeq_{\mathcal{T}}$ is an extension of $\geq_{\mathrm{tup}}$ and its restriction to the irreducible representatives of the monoid elements is a total, well-founded ordering $\succeq$ on $\mathcal{M}$. An important fact is that we have $u \circ_{\mathcal{T}} v \succeq_{\mathcal{T}} u \circ v$ for all $u, v \in \mathcal{M}$, but the ordering $\succeq$ in general need not be admissible on $\mathcal{M}$.

Since for commutative monoids the right ideals and the ideals in the corresponding monoid ring coincide, we will study ideals. Let us start with refining our view on

[28] Remember that such a finite convergent semi-Thue system modulo commutativity always exists for a finitely generated commutative monoid.

representations of polynomials for commutative monoid rings as follows.

Definition 4.5.2
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$. A representation

$$p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i, \quad \text{with } \alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$$

is called a **free commutative standard representation** in case for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$. A set $F \subseteq \mathbf{K}[\mathcal{M}]$ is called a **free commutative standard basis** if every non-zero polynomial in $\mathsf{ideal}(F)$ has a free commutative standard representation with respect to F. $\diamond$

Notice that $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$ immediately implies $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i \succeq \mathsf{HT}(f_i * w_i)$. Furthermore, $\mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i = \mathsf{HT}(f_i) \circ w_i$ implies $\mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i = \mathsf{HT}(f_i * w_i)$. On the other hand, in case $\mathsf{HT}(p) = \mathsf{HT}(f_i * w_i)$ this yields $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$ and $\mathsf{HT}(p) \geq_{\mathrm{tup}} \mathsf{HT}(f_i)$. This situation must occur for at least one polynomial in the representation. The following lemmata give some more information on special free commutative standard representations.

Lemma 4.5.3
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ such that for all $f \in F$ and all $w \in \mathcal{M}$ the polynomial $f * w$ has a free commutative standard representation with respect to F. Then the polynomial $f * w$ has a free commutative standard representation $f * w = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ such that $\mathsf{HT}(f * w) \succeq \mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$.

Proof :
We will prove this lemma by contradiction. Let us assume the claim is not true. Then there exists a counter-example $f * w$ such that $\mathsf{HT}(f * w)$ is minimal among all counter-examples. By our assumption $f * w$ has a free commutative standard representation, e.g. $f * w = \sum_{i=1}^{m} \alpha_i \cdot g_i * w_i$, such that $\alpha_i \in \mathbf{K}^*, g_i \in F, w_i \in \mathcal{M}$. Without loss of generality we can assume that for some $k \leq m$, $g_1, \ldots, g_k$, are the polynomials involved in the head term of $f * w$, i.e., $\mathsf{HT}(f * w) = \mathsf{HT}(g_i) \circ_{\mathcal{T}} w_i$ for all $1 \leq i \leq k$. Hence, we know $k < m$, as otherwise we would get a contradiction to $f * w$ being a counter-example. Furthermore, for all $k + 1 \leq j \leq m$ we know $\mathsf{HT}(g_j * w_j) \prec \mathsf{HT}(f * w)$ and hence every such polynomial has a free commutative standard representation of the desired form, say $g_j * w_j = \sum_{l=1}^{n_l} \alpha'_{j_l} \cdot g_{j_l} * w'_{j_l}$, with $\alpha'_{j_l} \in \mathbf{K}^*$, $g_{j_l} \in F$ and $w'_{j_l} \in \mathcal{M}$. Thus the representation $f * w = \sum_{i=1}^{k} \alpha_i \cdot g_i * w_i + \sum_{i=k+1}^{n} \alpha_i \cdot (\sum_{l=1}^{n_l} \alpha'_{j_l} \cdot g_{j_l} * w'_{j_l})$ is a free commutative standard representation of the desired form, contradicting our assumption.

q.e.d.

Lemma 4.5.4
Let F be a free commutative standard basis in $\mathbf{K}[\mathcal{M}]$. Then every non-zero polynomial $p \in \mathsf{ideal}(F)$ has a free commutative standard representation $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ such that for all $1 \leq i \leq n$ we even have

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i = \mathsf{HT}(f_i * w_i).$$

Proof :
Since $p \in \mathsf{ideal}(F)\backslash\{0\}$, p has a free commutative standard representation with respect to F, say $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*$, $f_i \in F$, $w_i \in \mathcal{M}$. Further, by lemma 4.5.3 every multiple $f_i * w_i$ has a free commutative standard representation, say $f_i * w_i = \sum_{j=1}^{m} \delta_j \cdot g_j * v_j$ with $\delta_j \in \mathbf{K}^*$, $g_j \in F$ and $v_j \in \mathcal{M}$ such that

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i * w_i) \succeq \mathsf{HT}(g_j * v_j) = \mathsf{HT}(g_j) \circ_{\mathcal{T}} v_j.$$

q.e.d.

In particular this lemma implies that a free commutative standard basis is a stable standard basis but the converse need not hold as the next example shows.

Example 4.5.5
Let $\Sigma = \{a, b\}$ and $T_c = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda\}$ be a presentation of a commutative group $\mathcal{G}$ with a length-lexicographical ordering induced by $a \succ b$. Further take the set $F = \{ab\}$.
Then all polynomials $g \in \mathsf{ideal}(F)$ have a stable standard representation in F, but e.g. the polynomial b has no free commutative standard representation. ◇

Now we can use the lemma of Dickson to show the existence of finite commutative standard bases.

Lemma 4.5.6 (Dickson)
For every infinite sequence of elements $m_s \in \mathcal{T}$, $s \in \mathbf{N}$, there exists an index $k \in \mathbf{N}$ such that for every index $i > k$ there exists and index $j \leq k$ and an element $w \in \mathcal{T}$ such that $m_i = m_j \circ_{\mathcal{T}} w$. □

Free commutative standard representations provide us with enough information to characterize free commutative standard bases (which are closely related to special Gröbner bases as we will see later on) by their head terms in a way similar to the case of usual polynomial rings.

Theorem 4.5.7
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and $G \subseteq \mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\}$. Then the following statements are equivalent:

1. *G is a free commutative standard basis for $\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)$*[29].

[29] I.e., $\mathsf{ideal}(F) = \mathsf{ideal}(G)$ and G is a free commutative standard basis.

2. $\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$.

Note that the set $\mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ *in general is no ideal in* $\mathcal{M}$.

Proof :
$1 \Longrightarrow 2$: The inclusion $\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M} \subseteq \mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ follows as $\mathsf{HT}(g) \circ_{\mathcal{T}} u \in \mathcal{M}$ for some $g \in G$, $u \in \mathcal{T}$ implies $\mathsf{HT}(g * u) = \mathsf{HT}(g) \circ_{\mathcal{T}} u$, $u \in \mathcal{M}$ and as the multiple $g * u$ belongs to $\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)$. It remains to show that $\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M} \supseteq \mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ holds. Let $g \in \mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\}$. Then since G is a free commutative standard basis for $\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)$, there exists a free commutative standard representation $g = \sum_{i=1}^{n} \alpha_i \cdot g_i * w_i$ with $\alpha_i \in \mathbf{K}^*, g_i \in G$ and $w_i \in \mathcal{M}$ such that $\mathsf{HT}(g) \succeq \mathsf{HT}(g_i) \circ_{\mathcal{T}} w_i$. Furthermore there exists $1 \leq k \leq n$ such that $\mathsf{HT}(g) = \mathsf{HT}(g_k) \circ_{\mathcal{T}} w_k$, i.e., $\mathsf{HT}(g) \in \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M}$.

$2 \Longrightarrow 1$: We have to show that every $g \in \mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\}$ has a free commutative standard representation with respect to G. This will be done by induction on the term $\mathsf{HT}(g)$. In the base case we can assume $\mathsf{HT}(g) = \min\{w \mid w \in \mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})\}$. Then, since $\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})$ there exists a polynomial $f \in G$ such that $\mathsf{HT}(g) = \mathsf{HT}(f) \circ_{\mathcal{T}} w$ for some $w \in \mathcal{M}$. Eliminating the head term of g by subtracting an appropriate multiple of f we get the polynomial $h = g - \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$. As $g \in \mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)$, h also lies in the ideal generated by F. Moreover, since $\mathsf{HT}(g)$ is minimal and $\mathsf{HT}(h) \prec \mathsf{HT}(g)$, we can conclude $h = 0$ and g has a free commutative standard representation $g = \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$. Now let us suppose $\mathsf{HT}(g) \succ \min\{w \mid w \in \mathsf{HT}(\mathsf{ideal}^{\mathbf{K}[\mathcal{M}]}(F)\backslash\{0\})\}$. Then again there exists a polynomial $f \in G$ such that $\mathsf{HT}(g) = \mathsf{HT}(f) \circ_{\mathcal{T}} w$ for some $w \in \mathcal{M}$. Hence looking at the polynomial $h = g - \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$ we know that h lies in the ideal generated by F and since $\mathsf{HT}(h) \prec \mathsf{HT}(g)$ either $h = 0$, giving us that $g = \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$, or our induction hypothesis yields the existence of a free commutative standard representation for h with respect to G, say $h = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j$ where $\beta_j \in \mathbf{K}^*$, $g_j \in G$ and $v_j \in \mathcal{M}$. Thus we have a free commutative standard representation of the polynomial g, namely $g = \sum_{j=1}^{m} \beta_j \cdot g_j * v_j + \mathsf{HC}(g) \cdot \mathsf{HC}(f)^{-1} \cdot f * w$.

q.e.d.

Theorem 4.5.8
Every ideal in $\mathbf{K}[\mathcal{M}]$ *has a finite free commutative standard basis.*

Proof :
Let $\mathfrak{i}$ be an ideal in $\mathbf{K}[\mathcal{M}]$. Then we can view $\mathsf{HT}(\mathfrak{i}\backslash\{0\})$ as a subset of $\mathcal{T}$. Further by Dickson's lemma every (infinite) set in $\mathcal{T}$ is finitely generated, i.e., $\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(\mathfrak{i}\backslash\{0\}))$ is finitely generated, with respect to the multiplication $\circ_{\mathcal{T}}$. In case $\mathsf{HT}(\mathfrak{i}\backslash\{0\})$ is finite, we can set $S = \mathsf{HT}(\mathfrak{i}\backslash\{0\})$. Furthermore, for each $t \in \mathsf{HT}(\mathfrak{i}\backslash\{0\})$ we take a polynomial $g_t \in \mathfrak{i}$ such that $\mathsf{HT}(g_t) = t$ and let $G = \{g_t \mid t \in \mathsf{HT}(\mathfrak{i}\backslash\{0\})\}$. Otherwise if $\mathsf{HT}(\mathfrak{i}\backslash\{0\}) =$

$\{t_i \mid i \in \mathbf{N}\}$ is infinite, let $S = \{s_1, \ldots, s_k\}$ be such a subset of $\mathsf{HT}(\mathfrak{i}\backslash\{0\})$ as described in Dickson's lemma. Then for each $1 \leq j \leq k$ again take a polynomial $g_{s_j} \in \mathfrak{i}$ such that $\mathsf{HT}(g_{s_j}) = s_j$ and let $G = \{g_{s_j} | s_j \in S\}$. Now in both cases we get

$$\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) = \mathsf{ideal}^{\mathcal{T}}(S) = \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(\mathfrak{i}\backslash\{0\}))$$

and

$$\mathsf{HT}(\mathfrak{i}\backslash\{0\}) = \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(\mathfrak{i}\backslash\{0\})) \cap \mathcal{M} = \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M},$$

i.e., by theorem 4.5.7, since $G \subseteq \mathfrak{i}$, G is a free commutative standard basis of $\mathfrak{i}$.

q.e.d.

As in the previous section we can characterize free commutative standard bases by weakening right reduction.

Definition 4.5.9
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{M}]$. We say f **commutatively reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\mathrm{c}} q$, if

(a) $\mathsf{HT}(f) \circ_{\mathcal{T}} w = t$ for some $w \in \mathcal{M}$, i.e., $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, and

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

We write $p \longrightarrow_f^{\mathrm{c}}$ if there is a polynomial q as defined above and p is then called commutatively reducible by f. Further we can define $\xrightarrow{*}^{\mathrm{c}}$, $\xrightarrow{+}^{\mathrm{c}}$, $\xrightarrow{n}^{\mathrm{c}}$ as usual. Commutative reduction by a set $F \subseteq \mathbf{K}[\mathcal{M}]$ is denoted by $p \longrightarrow_F^{\mathrm{c}} q$ and abbreviates $p \longrightarrow_f^{\mathrm{c}} q$ for some $f \in F$, which is also written as $p \longrightarrow_{f \in F}^{\mathrm{c}} q$. ◇

Notice that if f commutatively reduces p to q at a monomial $\alpha \cdot t$ then $t \notin \mathsf{T}(q)$ and $p > q$. Furthermore, commutative reduction is Noetherian and $p \longrightarrow_{q_1}^{\mathrm{c}} 0$ and $q_1 \longrightarrow_{q_2}^{\mathrm{c}} 0$ imply $p \longrightarrow_{q_2}^{\mathrm{c}} 0$ (compare lemma 4.2.8). Moreover, as prefix reduction, commutative reduction is terminating with respect to arbitrary sets of polynomials.

Definition 4.5.10
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ **interreduced** or **reduced** with respect to $\longrightarrow^{\mathrm{c}}$, if no polynomial f in F is commutatively reducible by the other polynomials in $F\backslash\{f\}$. ◇

As in the case of prefix reduction, commutatively reducing a polynomial by itself results in zero and hence so-defined reduced sets can be compared to the concept of reduced sets in the usual commutative polynomial ring. We have $\longrightarrow^{\mathrm{c}} \subseteq \longrightarrow^{\mathrm{r}}$ and similar to prefix reduction, we have more information on the reduction step.

Remark 4.5.11
Let $p \longrightarrow_q^{\mathrm{c}}$ and $q \longrightarrow_{q_1}^{\mathrm{c}} q_2$. Then in case $\mathsf{HT}(q) = \mathsf{HT}(q_2)$ we immediately get $p \longrightarrow_{q_2}^{\mathrm{c}}$. Otherwise $\mathsf{HT}(q) = \mathsf{HT}(q_1) \circ_{\mathcal{T}} y$, for some $y \in \mathcal{M}$ implies $p \longrightarrow_{q_1}^{\mathrm{c}}$. Hence, we have $p \longrightarrow_{\{q_1, q_2\}}^{\mathrm{c}}$. ◇

This property of commutative reduction corresponds to the fact that the existence of free commutative standard representations with respect to a set of polynomials remains true for an interreduced version of the set (compare lemma 4.5.12). Therefore, we will later on be able to compute reduced Gröbner bases in this setting.

Lemma 4.5.12
Let F and G be two sets of polynomials in $\mathbf{K}[\mathcal{M}]$ such that every polynomial in F has a free commutative standard representation with respect to G. Then if a polynomial p has a free commutative standard representation with respect to F it also has one with respect to G.

Proof :
Let $p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ be a free commutative standard representation of a polynomial p with respect to the set of polynomials F, i.e., for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$. Furthermore, every polynomial f_i occurring in this sum has a free commutative standard representation with respect to the set of polynomials G, say $f_i = \sum_{j=1}^{n_i} \beta_{i_j} \cdot g_{i_j} * v_{i_j}$, with $\beta_{i_j} \in \mathbf{K}^*, g_{i_j} \in G$, and $v_{i_j} \in \mathcal{M}$ such that for all $1 \leq j \leq n_i$ we have $\mathsf{HT}(f_i) \succeq \mathsf{HT}(g_{i_j}) \circ_{\mathcal{T}} v_{i_j}$. These representations can be combined in the sum

$$p = \sum_{i=1}^{n} \alpha_i \cdot (\sum_{j=1}^{n_i} \beta_{i_j} \cdot g_{i_j} * v_{i_j}) * w_i.$$

It remains to show that this in fact is a free commutative standard representation, i.e., to prove that for all $1 \leq i \leq n$ and all $1 \leq j \leq n_i$, we get $\mathsf{HT}(p) \succeq \mathsf{HT}(g_{i_j}) \circ_{\mathcal{T}} (v_{i_j} \circ w_i)$. This now follows immediately as for all $1 \leq i \leq n$ and all $1 \leq j \leq n_i$ we have

$$\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i \succeq (\mathsf{HT}(g_{i_j}) \circ_{\mathcal{T}} v_{i_j}) \circ_{\mathcal{T}} w_i \succeq \mathsf{HT}(g_{i_j}) \circ_{\mathcal{T}} (v_{i_j} \circ w_i).$$

q.e.d.

Using this lemma we can show that finite monic reduced free commutative standard bases are unique with respect to the presentation of the monoid.

Theorem 4.5.13
Every ideal in $\mathbf{K}[\mathcal{M}]$ contains a unique monic finite reduced free commutative standard basis.

Proof :
Let G be a finite free commutative standard basis of the ideal $\mathfrak{i}$ which must exist by theorem 4.5.8. Then by theorem 4.5.20 we know

$$\mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathfrak{i} \backslash \{0\}).$$

As the set $\mathsf{HT}(G)$ is finite[30], there exists a subset $H \subseteq \mathsf{HT}(G)$ such that

[30]The sets $\mathsf{HT}(G)$ and $\mathsf{HT}(\mathfrak{i} \backslash \{0\})$ of course depend on the presentation of $\mathcal{M}$ chosen, especially on the ordering induced on $\mathcal{M}$.

1. for all $m \in \mathsf{HT}(G)$ there exists an element $m' \in H$ and an element $w \in \mathcal{T}$ such that $m = m' \circ_{\mathcal{T}} w$,

2. for all $m \in H$ there exists no element $m' \in H \backslash \{m\}$ such that $m' <_{\text{tup}} m$, and

3. $\mathsf{ideal}^{\mathcal{T}}(H) \cap \mathcal{M} = \mathsf{ideal}^{\mathcal{T}}(\mathsf{HT}(G)) \cap \mathcal{M} = \mathsf{HT}(\mathfrak{i}\backslash\{0\})$.

Since for each term $t \in H$ there exists at least one polynomial in G with head term t we can choose one of them, say g_t, for every $t \in H$. Then as in theorem 4.5.8 the set $G' = \{g_t | t \in H\}$ is a free commutative standard basis. Further all polynomials in G' have different head terms and no head term is commutatively reducible by the other polynomials in G'. Hence, if we commutatively interreduce G' giving us another set of polynomials G'', we know $\mathsf{HT}(G') = \mathsf{HT}(G'')$ and this set is a free commutative standard basis as well. To see the latter we use the fact that for a free commutative standard basis G, if $f \in G$ and $f \longrightarrow^{\mathrm{c}}_{G\backslash\{f\}} f'$, then $(G\backslash\{f\}) \cup \{f'\}$ again is a free commutative standard basis of the same ideal. This follows immediately by lemma 4.5.12 as f has a free commutative standard representation with respect to $(G\backslash\{f\}) \cup \{f'\}$.
It remains to show the uniqueness of the reduced free commutative standard basis if we restrict ourselves to sets of monic polynomials. Let us assume S is another monic reduced free commutative standard basis of $\mathfrak{i}$. Further let $f \in S \triangle G'' = (S\backslash G'') \cup (G''\backslash S)$ be a polynomial such that $\mathsf{HT}(f)$ is minimal in the set of terms $\mathsf{HT}(S \triangle G'')$. Without loss of generality we can assume that $f \in S\backslash G''$. As G'' is a free commutative standard basis and $f \in \mathfrak{i}$ there exists a polynomial $g \in G''$ such that $\mathsf{HT}(f) = \mathsf{HT}(g) \circ_{\mathcal{T}} w$ for some $w \in \mathcal{M}$. We can even state that $g \in G''\backslash S$ as otherwise S would not be commutatively interreduced. Since f was chosen such that $\mathsf{HT}(f)$ was minimal in $\mathsf{HT}(S \triangle G'')$, we get $\mathsf{HT}(f) = \mathsf{HT}(g)$[31]. As we assume $f \neq g$ this gives us $f - g \neq 0$, $\mathsf{HT}(f-g) \prec \mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HT}(f-g) \in \mathsf{T}(f) \cup \mathsf{T}(g)$. But $f - g \in \mathfrak{i}$ implies the existence of a polynomial $h \in S$ such that $\mathsf{HT}(f-g) = \mathsf{HT}(h) \circ_{\mathcal{T}} w'$ for some $w' \in \mathcal{M}$, implying that f is not commutatively reduced. Hence we get that S is not commutatively interreduced, contradicting our assumption.

q.e.d.

The following example shows that different presentations for the monoid can result in different reduced free commutative standard bases.

Example 4.5.14
Let $\Sigma = \{a, b, c\}$ and $T_c = \emptyset$ be a presentation of a commutative monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c$. Then the set $F = \{a + c + \lambda, b + c + \lambda\}$ is a reduced free commutative standard basis. This is no longer true if we assume that the ordering on $\mathcal{M}$ is induced by $c \succ a \succ b$. Then the set $F' = \{c + b + \lambda, a - b\}$ is a reduced free commutative standard basis. $\diamond$

[31] Otherwise $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ would contradict our assumption.

Another setting in which a bound of a representation is preserved under multiplication is specified in the next lemma. This observations will be a weaker substitute for the fact that in a commutative polynomial ring $p \xrightarrow{*}^{\mathrm{b}}_{F} 0$ implies $\alpha \cdot p * w \xrightarrow{*}^{\mathrm{b}}_{F} 0$.

Lemma 4.5.15
Let F be a set of polynomials and p a polynomial in $\mathbf{K}[\mathcal{M}]$. Further let $p \xrightarrow{*}^{\mathrm{c}}_{F} 0$ and this reduction sequence results in a representation $p = \sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$, where $\alpha_i \in \mathbf{K}^*$, $g_i \in F$, and $w_i \in \mathcal{M}$. Then for every term $t \in \mathcal{M}$ such that $t \succ \mathsf{HT}(p)$ and every term $w \in \mathcal{M}$ we get that $s \in \bigcup_{i=1}^{k} \mathsf{T}(g_i * w_i * w)$ implies $t \circ_{\mathcal{T}} w \succ s$.

Proof :
As $\sum_{i=1}^{k} \alpha_i \cdot g_i * w_i$ belongs to the reduction sequence $p \xrightarrow{*}^{\mathrm{c}}_{F} 0$, for all $u \in \bigcup_{i=1}^{k} \mathsf{T}(g_i * w_i)$ we have $\mathsf{HT}(p) \succeq u$ implying $t \circ_{\mathcal{T}} w \succ \mathsf{HT}(p) \circ_{\mathcal{T}} w \succ u \circ_{\mathcal{T}} w \succeq u \circ w$.
Note that this proof uses the fact that the ordering $\succ$ on $\mathcal{M}$ is induced by the completion ordering $\succeq_T$ of the vector replacement system (Σ, T) presenting $\mathcal{M}$, as we need that the ordering is admissible on $\mathcal{T}$, i.e., $u \circ_{\mathcal{T}} v \succeq_T (u \circ_{\mathcal{T}} v)\downarrow_T = u \circ v$ for all $u, v \in \mathcal{M}$.
q.e.d.

Let us continue by taking a closer look at commutative reduction. An essential property in characterizing Gröbner bases, the translation lemma holds.

Lemma 4.5.16
Let F be a set of polynomials and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$.

1. *Let $p - q \longrightarrow^{\mathrm{c}}_{F} h$. Then there are $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}^{\mathrm{c}}_{F} p'$, $q \xrightarrow{*}^{\mathrm{c}}_{F} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{c}}_{F}$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}^{\mathrm{c}}_{F} g$ and $q \xrightarrow{*}^{\mathrm{c}}_{F} g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{c}}_{F} h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*, f \in F, w \in \mathcal{M}$ and $\mathsf{HT}(f) \circ_{\mathcal{T}} w = t$, i.e. $\alpha \cdot \mathsf{HC}(f)$ is the coefficient of t in $p - q$. We have to distinguish three cases:
   (a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$: Then we can eliminate the term t in the polynomials p respectively q by commutative reduction and get $p \longrightarrow^{\mathrm{c}}_{f} p - \alpha_1 \cdot f * w = p'$, $q \longrightarrow^{\mathrm{c}}_{f} q - \alpha_2 \cdot f * w = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f)$ and $\alpha_2 \cdot \mathsf{HC}(f)$ are the coefficients of t in p respectively q.
   (b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$: Then we can eliminate the term t in the polynomial p by commutative reduction and get $p \longrightarrow^{\mathrm{c}}_{f} p - \alpha \cdot f * w = p'$ and $q = q'$.
   (c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$: Then we can eliminate the term t in the polynomial q by commutative reduction and get $q \longrightarrow^{\mathrm{c}}_{f} q + \alpha \cdot f * w = q'$ and $p = p'$.

In all cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

2. We show our claim by induction on k, where $p - q \xrightarrow{k}{}^{\mathrm{c}}_F 0$. In the base case $k = 0$ there is nothing to show. Hence, let $p - q \longrightarrow^{\mathrm{c}}_F h \xrightarrow{k}{}^{\mathrm{c}}_F 0$. Then by (1) there are polynomials $p', q' \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{c}}_F p', q \xrightarrow{*}{}^{\mathrm{c}}_F q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \xrightarrow{k}{}^{\mathrm{c}}_F 0$ yields the existence of a polynomial $g \in \mathbf{K}[\mathcal{M}]$ such that $p \xrightarrow{*}{}^{\mathrm{c}}_F p' \xrightarrow{*}{}^{\mathrm{c}}_F g$ and $q \xrightarrow{*}{}^{\mathrm{c}}_F q' \xrightarrow{*}{}^{\mathrm{c}}_F g$.

q.e.d.

The following lemma shows that commutative reduction captures the ideal congruence when using free commutative standard bases of ideals. Reviewing example 4.5.5 we find that this is not true in general.

Lemma 4.5.17
Let F be a free commutative standard basis and p, q, h some polynomials in $\mathbf{K}[\mathcal{M}]$. Then

$$p \xleftrightarrow{*}{}^{\mathrm{c}}_F q \text{ if and only if } p - q \in \mathsf{ideal}(F).$$

Proof :
In order to prove our claim we have to show two subgoals. The inclusion $\xleftrightarrow{*}{}^{\mathrm{c}}_F \subseteq \equiv_{\mathsf{ideal}(F)}$ is an immediate consequence of the definition of commutative reduction and can be shown by induction as in lemma 4.2.11. To prove the converse inclusion $\equiv_{\mathsf{ideal}(F)} \subseteq \xleftrightarrow{*}{}^{\mathrm{c}}_F$ let us remember that $p \equiv_{\mathsf{ideal}(F)} q$ implies $p = q + \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$, where $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{M}$ and every multiple $f_j * w_j$ belongs to $\mathsf{ideal}(F)$. As F is a free commutative standard basis, by lemma 4.5.4 we can assume $\mathsf{HT}(f * w) = \mathsf{HT}(f) \circ_{\mathcal{T}} w$ for all polynomials occurring in the sum. Under these assumptions we can then show our claim straightforward as in lemma 4.2.11 by induction on m.

q.e.d.

Let us continue by defining Gröbner bases with respect to commutative reduction.

Definition 4.5.18
A set $G \subseteq \mathbf{K}[\mathcal{M}]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{c}}$ or a **commutative Gröbner basis**, if

(i) $\xleftrightarrow{*}{}^{\mathrm{c}}_G = \equiv_{\mathsf{ideal}(G)}$, and

(ii) $\longrightarrow^{\mathrm{c}}_G$ is confluent. $\diamond$

As in the previous section there is a natural connection between free commutative standard bases and commutative reduction.

Lemma 4.5.19
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{M}]$.

1. *Then $p \xrightarrow{*}{}^{\mathrm{c}}_{F} 0$ implies the existence of a free commutative standard representation for p.*

2. *In case p has a free commutative standard representation with respect to F, then p is commutatively reducible at its head monomial by F, i.e., p is commutatively top-reducible by F.*

3. *In case F is a free commutative standard basis, every polynomial $p \in \mathsf{ideal}(F)\backslash\{0\}$ is commutatively top-reducible to zero by F.*

Proof :

1. This follows directly by adding up the polynomials used in the reduction steps occurring in $p \xrightarrow{*}{}^{\mathrm{c}}_{F} 0$.

2. This is an immediate consequence of definition 4.5.2 as the existence of a polynomial f in F and an element $w \in \mathcal{M}$ with $\mathsf{HT}(f * w) = \mathsf{HT}(f) \circ_{\mathcal{T}} w = \mathsf{HT}(p)$ is guaranteed.

3. We show that every non-zero polynomial $p \in \mathsf{ideal}_r(F)\backslash\{0\}$ is top-reducible to zero using F by induction on $\mathsf{HT}(p)$. First let $\mathsf{HT}(p) = \min\{\mathsf{HT}(g) \mid g \in \mathsf{ideal}(F)\backslash\{0\}\}$. Then, as $p \in \mathsf{ideal}(F)$ and F is a free commutative standard basis, this gives us a representation $p = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$ and $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$ for all $1 \leq i \leq k$. Without loss of generality, let us assume $\mathsf{HT}(p) = \mathsf{HT}(f_1) \circ_{\mathcal{T}} w_1$. Hence, the polynomial p is commutatively reducible by f_1. Let $p \longrightarrow^{\mathrm{c}}_{f_1} q$, i.e., $q = p - \mathsf{HC}(p) \cdot \mathsf{HC}(f_1)^{-1} \cdot f_1 * w_1$, and by the definition of commutative reduction the term $\mathsf{HT}(p)$ is eliminated from p implying that $\mathsf{HT}(q) \prec \mathsf{HT}(p)$ as $q < p$. Now, since $\mathsf{HT}(p)$ was minimal among the head terms of the elements in the ideal generated by F, this implies $q = 0$, and, therefore, p is commutatively top-reducible to zero by f_1 in one step. On the other hand, in case $\mathsf{HT}(p) \succ \min\{\mathsf{HT}(g) | g \in \mathsf{ideal}(F)\backslash\{0\}\}$, by the same arguments used before we can commutatively reduce p to a polynomial q with $\mathsf{HT}(q) \prec \mathsf{HT}(p)$, and, thus, by our induction hypothesis we know that q is commutatively top-reducible to zero. Therefore, as the reduction step $p \longrightarrow^{\mathrm{c}}_{f_1} q$ takes place at the head term of p, the polynomial p is also commutatively top-reducible to zero.

q.e.d.

Indeed, free commutative standard bases and commutative Gröbner bases are equivalent.

Theorem 4.5.20
For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *F is a commutative Gröbner basis.*

2. *For all polynomials* $g \in \mathsf{ideal}(F)$ *we have* $g \xrightarrow{*}{}^{\mathrm{c}}_{F} 0$.

3. *F is a free commutative standard basis.*

Proof :
$1 \Longrightarrow 2$: By (i) of definition 4.5.18 we know that $g \in \mathsf{ideal}(F)$ implies $g \xleftrightarrow{*}{}^{\mathrm{c}}_{F} 0$ and since $\longrightarrow^{\mathrm{c}}_{F}$ is confluent and 0 is irreducible, $g \xrightarrow{*}{}^{\mathrm{c}}_{F} 0$ follows immediately.

$2 \Longrightarrow 3$: This follows directly by adding up the polynomials used in the reduction steps $g \xrightarrow{*}{}^{\mathrm{c}}_{F} 0$.

$3 \Longrightarrow 1$: In order to show that F is a commutative Gröbner basis we have to show two subgoals: $\xleftrightarrow{*}{}^{\mathrm{c}}_{F} = \equiv_{\mathsf{ideal}(F)}$ was already shown in lemma 4.5.17. It remains to show that $\longrightarrow^{\mathrm{c}}_{F}$ is confluent. Since $\longrightarrow^{\mathrm{c}}_{F}$ is Noetherian, we only have to prove local confluence. Suppose $g \longrightarrow^{\mathrm{c}}_{F} g_1, g \longrightarrow^{\mathrm{c}}_{F} g_2$ and $g_1 \neq g_2$. Then $g_1 - g_2 \in \mathsf{ideal}(F)$ and, therefore, is commutatively top-reducible to zero as a result of lemma 4.5.12. Thus lemma 4.5.16 provides the existence of a polynomial $h \in \mathbf{K}[\mathcal{M}]$ such that $g_1 \xrightarrow{*}{}^{\mathrm{c}}_{F} h$ and $g_2 \xrightarrow{*}{}^{\mathrm{c}}_{F} h$, i.e., $\longrightarrow^{\mathrm{c}}_{F}$ is confluent.

q.e.d.

Since in general $\xleftrightarrow{*}{}^{\mathrm{r}} \neq \xleftrightarrow{*}{}^{\mathrm{c}}$ and $\xleftrightarrow{*}{}^{\mathrm{s}} \neq \xleftrightarrow{*}{}^{\mathrm{c}}$ we again enrich our set of polynomials used for reduction to regain the desired expressiveness of strong reduction.

Definition 4.5.21
A set of polynomials $F \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}\}$ is called a **commutatively saturating set** for a non-zero polynomial $p \in \mathbf{K}[\mathcal{M}]$, if for all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$, with $\alpha \cdot p * w \neq 0$ we have $\alpha \cdot p * w \longrightarrow^{\mathrm{c}}_{F} 0$[32]. $\mathcal{SAT}_c(p)$ denotes the family of all commutatively saturating sets for p. We call a set $F \subseteq \mathbf{K}[\mathcal{M}]$ **commutatively saturated**, if for all $\alpha \in \mathbf{K}^*$, $f \in F$, $w \in \mathcal{M}$, we have $\alpha \cdot f * w \longrightarrow^{\mathrm{c}}_{F} 0$ in case $\alpha \cdot f * w \neq 0$. $\diamond$

Note that commutatively saturating sets are also saturating sets. Moreover, they give us additional information as they allow special representations of elements in the ideals they generate comparable to lemma 4.4.24 for prefix saturated sets.

Lemma 4.5.22
Let F be a commutatively saturated set of polynomials in $\mathbf{K}[\mathcal{M}]$. Then every non-zero polynomial g in $\mathsf{ideal}(F)$ has a representation $g = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, where $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{M}$, and $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ_T w_i$. $\square$

Notice that these representations need not be free commutative standard representations as we cannot conclude $\mathsf{HT}(g) \succeq \mathsf{HT}(f_i) \circ_T w_i$.

As in the case of prefix saturation combined with prefix saturation, commutative saturation enables us to do the same reduction steps we can do using strong reduction or right reduction combined with saturation (compare lemma 4.4.23).

[32]Since $\mathbf{K}$ is a field it is sufficient to demand $p * w \xrightarrow{\leq 1}{}^{\mathrm{c}}_{F} 0$ for all $w \in \mathcal{M}$.

Lemma 4.5.23
Let f, g, p be some polynomials in $\mathbf{K}[\mathcal{M}]$, $S \in \mathcal{SAT}(p)$, and $S_c \in \mathcal{SAT}_c(p)$. Then

$$f \longrightarrow^{\mathrm{r}}_{S} g \text{ if and only if } f \longrightarrow^{\mathrm{c}}_{S_c} g.$$

□

Further commutative reduction combined with commutative saturation is strong enough to capture the ideal congruence.

Lemma 4.5.24
Let F be a commutatively saturated set of polynomials and p, q some polynomials in $\mathbf{K}[\mathcal{M}]$. Then

$$p \overset{*}{\longleftrightarrow}^{\mathrm{c}}_{F} q \text{ if and only if } p - q \in \mathsf{ideal}(F).$$

Proof :
This lemma follows directly from theorem 4.3.28 and lemma 4.5.23.

q.e.d.

The existence of finite commutatively saturating sets is guaranteed by Dickson's lemma.

Lemma 4.5.25
Every commutatively saturating set for a polynomial contains a finite commutatively saturating set.

Proof :
For $p \in \mathbf{K}[\mathcal{M}]$ let S be an arbitrary saturating set. Then comparable to the constructive approach for saturating sets in definition 4.3.20 we can decompose S into sets S_t for $t \in \mathsf{T}(p)$ such that $S_t = \{q \in S \mid \mathsf{HT}(q) \text{ results from the term } t\}$. Further let $Z_t = \{\mathsf{HT}(q) \mid q \in S_t\} \subseteq \mathcal{M} \subseteq \mathcal{T}$. Then Z_t is a (possibly infinite) subset of $\mathcal{T}$ in the sense of Dickson's lemma and we can choose a finite subset D_t of Z_t such that for every $w \in Z_t$ there exist $u \in D_t$ and $v \in \mathcal{M} \subseteq \mathcal{T}$ such that $u \circ_{\mathcal{T}} v = w$. Now for every $t \in \mathsf{T}(p)$ we can associate every term $s \in D_t$ with a polynomial $q_s \in S_t$ such that $\mathsf{HT}(q_s) = s$. The union of all such polynomials then is a finite saturating set for p which obviously is a subset of S.

q.e.d.

The property of being commutatively saturated is decidable.

Lemma 4.5.26
It is decidable, whether a finite set $F \subseteq \mathbf{K}[\mathcal{M}]$ is commutatively saturated.

Proof :
We will show that the following procedure is correct:

Procedure: COMMUTATIVELY SATURATED CHECK

Given: A finite set $F \subseteq \mathbf{K}[\mathcal{M}]$, and (Σ, T_c) a convergent presentation of $\mathcal{M}$.
Find: *yes*, if F is commutatively saturated
no, otherwise.

answer := yes
for all $q \in F$ **do**
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{ w \in \mathcal{T} | \mathsf{LCM}(t, l) = t \circ_{\mathcal{T}} w = l \circ_{\mathcal{T}} u \neq t \circ_{\mathcal{T}} l$ for some rule $(l, r) \in T_c, u \in \mathcal{T} \}$ **do**
    % $C(t)$ contains special overlaps between t and left hand sides of rules in T
    % Multiplying t with terms in $C(t)$ leads to cancellation
    $q' := (q * w_1)$;
    if $q' \not\longrightarrow^{c}_{F} 0$ and $q' \neq 0$
      then answer := no;
    endif
  endfor
endfor

It remains to show that the answer of our procedure is "no" if and only if F is not commutatively saturated. Obviously, the answer "no" implies the existence of an element $w \in \mathcal{M}$ such that for some $f \in F$ with $f * w \neq 0$, $f * w \not\longrightarrow^{c}_{F} 0$. On the other hand let us assume that our procedure gives us "yes", but F is not commutatively saturated. Then there exists an element $w \in \mathcal{M}$ and a polynomial $f \in F$ such that $\mathsf{HT}(f) \circ_{\mathcal{T}} w$ is minimal according to our ordering on $\mathcal{T}$, $f * w \neq 0$ and $f * w \not\longrightarrow^{c}_{F} 0$. In case $w \in C(\mathsf{HT}(f))$ this would give us "no" contradicting our assumption. Therefore, let us assume $w \notin C(\mathsf{HT}(f))$. Furthermore, $\mathsf{HT}(f) \circ_{\mathcal{T}} w$ must be T-reducible as otherwise $f * w \longrightarrow^{c}_{f \in F} 0$. Let $w = w_1 \circ_{\mathcal{T}} w_2$ such that $\mathsf{HT}(f) \circ_{\mathcal{T}} w_1 = l \circ_{\mathcal{T}} v = \mathsf{LCM}(\mathsf{HT}(f), l)$ for some rule $(l, r) \in T$, i.e., $w_1 \in C(\mathsf{HT}(f))$. Now $f * w_1$ is considered by our procedure and since $w \succ w_1$ and the choice of w, f was minimal, we either get $f * w_1 = 0$ contradicting the fact that $f * w \neq 0$ or $f * w_1 \longrightarrow^{c}_{F} 0$. Furthermore, this gives us the existence of $f' \in F$ such that $\mathsf{HT}(f) \circ_{\mathcal{T}} w_1 \succ \mathsf{HT}(f * w_1) = \mathsf{HT}(f') \circ_{\mathcal{T}} z$ for some $z \in \mathcal{M}$. This implies $\mathsf{HT}(f) \circ_{\mathcal{T}} w = \mathsf{HT}(f) \circ_{\mathcal{T}} (w_1 \circ_{\mathcal{T}} w_2) = (\mathsf{HT}(f) \circ_{\mathcal{T}} w_1) \circ_{\mathcal{T}} w_2 \succ \mathsf{HT}(f * w_1) \circ_{\mathcal{T}} w_2 = (\mathsf{HT}(f') \circ_{\mathcal{T}} z) \circ_{\mathcal{T}} w_2 = \mathsf{HT}(f') \circ_{\mathcal{T}} (z \circ_{\mathcal{T}} w_2) \succeq \mathsf{HT}(f') \circ_{\mathcal{T}} (z \circ w_2)$ and gives us $f * w = \alpha \cdot f' * (z \circ w_2) \longrightarrow^{c}_{F} 0$ contradicting our assumption.
Further this procedure terminates, as the sets H and T are always finite.

q.e.d.

The next lemma states that minimal commutatively saturating sets exist.

Lemma 4.5.27
Let p be a polynomial in $\mathbf{K}[\mathcal{M}]$ and $S \in \mathcal{SAT}_c(p)$. Then if there is a polynomial $q \in S$ such that $q \longrightarrow^{c}_{S \backslash \{q\}} 0$, the set $S \backslash \{q\}$ is a commutatively saturating set for p.

Proof :
This is an immediate consequence as $p \longrightarrow^{c}_{q_1} 0$ and $q_1 \longrightarrow^{c}_{q_2} 0$ implies $p \longrightarrow^{c}_{q_2} 0$, i.e., item 3 of lemma 4.2.8 also holds for commutative reduction.

q.e.d.

We proceed to give a procedure, which actually computes a simplified commutatively saturating set for a polynomial p (compare the approach for prefix saturation using simplification on page 105). The idea is to compute overlaps of terms with rules in T_c using least common multiples in $\mathcal{T}$. In giving a procedure for prefix saturating a polynomial, prefixes were used to define a set of critical overlaps for a term t of the form $C(t) = \{w \in \Sigma^* \mid tw \equiv t_1 t_2 w \equiv t_1 l, t_2 \neq \lambda$ for some rule $(l,r) \in T\}$. Here we will look at the set $C(t) = \{w \in \mathcal{T} \mid \mathsf{LCM}(t,l) = t \circ_{\mathcal{T}} w = l \circ_{\mathcal{T}} u \neq t \circ_{\mathcal{T}} l$ for some rule $(l,r) \in T_c, u \in \mathcal{T}\}$ which corresponds to the overlaps between the term t and the rules in T_c in terms of semi-Thue systems modulo commutativity. Additionally, polynomials are removed from the computes set in case they are commutatively reducible to zero in one step by a polynomial computed later on.

Procedure: COMMUTATIVE SATURATION USING SIMPLIFICATION

Given: A polynomial $p \in \mathbf{K}[\mathcal{M}]$, and (Σ, T_c) a convergent presentation of $\mathcal{M}$.
Find: $S_c \in \mathcal{SAT}_c(p)$.

$S_0 := \{p\}$;
$H := \{p\}$;
$i := 0$;
while $H \neq \emptyset$ **do**
  $i := i + 1$;
  $S_i := S_{i-1}$;
  $q :=$ remove(H);
  % Remove an element from a set using a fair strategy
  $t := \mathsf{HT}(q)$;
  for all $w \in C(t) = \{\, w \in \mathcal{T} | \mathsf{LCM}(t,l) = t \circ_{\mathcal{T}} w = l \circ_{\mathcal{T}} u \neq t \circ_{\mathcal{T}} l$ for some rule $(l,r) \in T_c, u \in \mathcal{T}\}$ **do**
    % $C(t)$ contains special overlaps between t and left hand sides of rules in T
    $q' := (q * w_1)$;
    if $q' \not\longrightarrow^{c}_{S_c} 0$ and $q' \neq 0$
      then $S_i :=$ simplify$(S_i, q') \cup \{q'\}$;
        % Simplify removes elements s from S_i in case $s \longrightarrow^{c}_{q'} 0$
        $H := H \cup \{q'\}$;
    endif
  endfor
endwhile
$S_c := S_i$

Lemma 4.5.28
Procedure COMMUTATIVE SATURATION USING SIMPLIFICATION *is correct.*

Proof :
We will prove that for all $q \in S_c, w \in \mathcal{M}$ we have $q * w \longrightarrow^{c}_{S_c} 0$ in case $q * w \neq 0$. Let us assume this is not true. Then we can choose a counter-example $q * w$ such that $\mathsf{HT}(q) \circ_{\mathcal{T}} w$ is minimal (according to the ordering on $\mathcal{T}$) and $q * w \not\longrightarrow^{c}_{S_c} 0$. Then $\mathsf{HT}(q) \circ_{\mathcal{T}} w$ must be T-reducible, as otherwise $q * w \longrightarrow^{c}_{q} 0$ and $q \in S_c$. Let $w = w_1 \circ_{\mathcal{T}} w_2$ such that $w_1 \in \mathcal{M}$ causing $\mathsf{HT}(q) \circ w_1 \neq \mathsf{HT}(q) \circ_{\mathcal{T}} w_1 = l \circ_{\mathcal{T}} z = \mathsf{LCM}(\mathsf{HT}(q), l)$ for some $(l, r) \in T$, $z \in \mathcal{T}$. Since $q \in S_c$, the polynomial $q * w_1$ is considered during the computation of S_c[33]. We have to consider two cases. If $q * w_1 \in S_c$ then $q * w = (q * w_1) * w_2 \longrightarrow^{c}_{S_c} 0$ since $w_1 \in \mathcal{M}$ and $\mathsf{HT}(q) \circ_{\mathcal{T}} w \succ \mathsf{HT}(q * w_1) \circ_{\mathcal{T}} w_2$ contradicting our assumption. On the other hand, if $q * w_1 \notin S_c$ then for some iteration step i_q we have $q * w_1 \longrightarrow^{c}_{q' \in S_{i_q}} 0$ and first we show that even $q * w_1 \longrightarrow^{c}_{S_c} 0$ holds. This follows since the fact that $q \longrightarrow^{c}_{q_1} 0$ and $q_1 \longrightarrow^{c}_{q_2} 0$ implies $q \longrightarrow^{c}_{q_2} 0$ yields that $q * w_1 \longrightarrow^{c}_{S_i} 0$ implies $q * w_1 \longrightarrow^{c}_{S_{i+n}} 0$ for all $n \in \mathbf{N}$. Furthermore, as removing a polynomial s from a set S_i because of a polynomial q' we know $\mathsf{HT}(q') <_{\mathrm{tup}} \mathsf{HT}(s)$ and this cannot occur infinitely often, we would get $q * w_1 \longrightarrow^{c}_{S_c} 0$ contradicting our assumption. Thus we can assume $q * w_1 \longrightarrow^{c}_{S_c} 0$ and moreover, we know $w_1 \in \mathcal{M}$ and $\mathsf{HT}(q) \circ_{\mathcal{T}} w_1 \succ \mathsf{HT}(q * w_1) = \mathsf{HT}(q') \circ_{\mathcal{T}} z$ for some $z \in \mathcal{M}$. Further $q * w_1 = \alpha' \cdot q' * z$ and $\mathsf{HT}(q * w_1) = \mathsf{HT}(q') \circ_{\mathcal{T}} z$ give us $q * w = (q * w_1) * w_2 = (\alpha' \cdot q' * z) * w_2 = \alpha' \cdot q' * (z \circ w_2)$, and $\mathsf{HT}(q) \circ_{\mathcal{T}} w = \mathsf{HT}(q) \circ_{\mathcal{T}} (w_1 \circ_{\mathcal{T}} w_2) = (\mathsf{HT}(q) \circ_{\mathcal{T}} w_1) \circ_{\mathcal{T}} w_2 \succ (\mathsf{HT}(q') \circ_{\mathcal{T}} z) \circ_{\mathcal{T}} w_2 = \mathsf{HT}(q') \circ_{\mathcal{T}} (z \circ_{\mathcal{T}} w_2) \succeq \mathsf{HT}(q') \circ_{\mathcal{T}} (z \circ w_2)$. Therefore, $q * w = (\alpha' \cdot q' * z) * w_2 = \alpha' \cdot q' * (z \circ w_2) \longrightarrow^{c}_{S_c} 0$, contradicting our assumption.
q.e.d.

Lemma 4.5.29
Procedure COMMUTATIVE SATURATION USING SIMPLIFICATION *terminates.*

Proof :
This follows at once as the procedure is correct and by lemma 4.5.25 the constructed set must contain a finite commutatively saturated subset.
q.e.d.

Commutative saturation enriches a polynomial p by adding a set of polynomials $S \in \mathcal{SAT}_c(p)$ such that we can substitute a reduction step $q \longrightarrow^{(\mathrm{s,r})}_{p} q'$ by a commutative reduction step $q \longrightarrow^{c}_{p' \in S} q'$. This additional information can be combined with special s-polynomials to give a finite confluence test similar to the approach using prefix reduction.

Definition 4.5.30
Given two non-zero polynomials $p_1, p_2 \in \mathbf{K}[\mathcal{M}]$ such that $\mathsf{HT}(p_1) \circ_{\mathcal{T}} w_1 = \mathsf{HT}(p_2) \circ_{\mathcal{T}} w_2 = \mathsf{LCM}(\mathsf{HT}(p_1), \mathsf{HT}(p_2)) \in \mathcal{M}$ for some $w_1, w_2 \in \mathcal{M}$, then the **commutative s-polynomial** is defined as

$$\mathsf{spol}_c(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w_2. \qquad \diamond$$

[33]We can assume that the elements are removed from the set H using a fair strategy, e.g., first in first out.

Obviously this definition implies $\mathsf{HT}(\mathsf{spol}_c(p_1,p_2)) \prec \mathsf{LCM}(\mathsf{HT}(p_1),\mathsf{HT}(p_2))$. An s-polynomial is called non-trivial in case it is not zero. Notice that a finite set $F \subseteq \mathbf{K}[\mathcal{M}]$ only gives us finitely many commutative s-polynomials. A commutative s-polynomial for two polynomials p_1, p_2 corresponds to a term, namely $\mathsf{LCM}(\mathsf{HT}(p_1),\mathsf{HT}(p_2)) \in \mathcal{M}$, where both polynomials p_1 and p_2 can be applied to perform a commutative reduction step. As in the previous section (commutative) Gröbner bases cannot be characterized by such restricted s-polynomials alone. However, this can be done in case we have a commutatively saturated set.

Theorem 4.5.31
For a commutatively saturated set F of polynomials in $\mathbf{K}[\mathcal{M}]$, the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}{}^{\mathrm{c}}_F 0$.*
2. *For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}_c(f_k,f_l) \xrightarrow{*}{}^{\mathrm{c}}_F 0$.*

Proof :
$1 \Longrightarrow 2$: In case $\mathsf{HT}(f_k) \circ_{\mathcal{T}} w_k = \mathsf{HT}(f_l) \circ_{\mathcal{T}} w_l = \mathsf{LCM}(\mathsf{HT}(f_k),\mathsf{HT}(f_l)) \in \mathcal{M}$ for some elements $w_k, w_l \in \mathcal{M}$, then by definition 4.5.30 we get

$$\mathsf{spol}_c(f_k,f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * w_l \ \in \mathsf{ideal}(F),$$

and hence $\mathsf{spol}_c(f_k,f_l) \xrightarrow{*}{}^{\mathrm{c}}_F 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{c}}_F$-reducible to zero. Remember that for $h \in \mathsf{ideal}(F)$, $h \longrightarrow^{\mathrm{c}}_F h'$ implies $h' \in \mathsf{ideal}(F)$. As $\longrightarrow^{\mathrm{c}}_F$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{c}}_F$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{M}$. By lemma 4.5.22 we can assume $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$. This will be important to restrict ourselves to commutative s-polynomials in order to modify this representation of g. Depending on the above representation of g and a well-founded total ordering $\succeq$ on $\mathcal{M}$ we define $t = \max\{\mathsf{HT}(f_j) \circ_{\mathcal{T}} w_j \mid j \in \{1,\dots m\}\}$ and K is the number of polynomials $f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{c}}_F$-reducible. So by lemma 4.5.19 it is sufficient to show that g has a free commutative standard representation, as this implies that g is top-reducible using F. This will be done by induction on (t,K), where $(t',K') < (t,K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[34]. Now if $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[35] such that $\mathsf{HT}(f_k) \circ_{\mathcal{T}} w_k = \mathsf{HT}(f_l) \circ_{\mathcal{T}} w_l$. By definition 4.5.30 we have a commutative s-polynomial $\mathsf{spol}_c(f_k,f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * z_1 - \mathsf{HC}(f_l)^{-1} \cdot f_l * z_2$ and we further know $\mathsf{HT}(f_k) \circ_{\mathcal{T}} w_k = \mathsf{HT}(f_l) \circ_{\mathcal{T}} w_l = \mathsf{HT}(f_k) \circ_{\mathcal{T}} z_1 \circ_{\mathcal{T}} w = \mathsf{HT}(f_l) \circ_{\mathcal{T}} z_2 \circ_{\mathcal{T}} w$ for some

[34] Note that this ordering is well-founded since $\succ$ is and $K \in \mathbf{N}$.

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

$z_1, z_2, w \in \mathcal{M}$ such that $\mathsf{HT}(f_k) \circ_{\mathcal{T}} z_1 = \mathsf{HT}(f_l) \circ_{\mathcal{T}} z_2 = \mathsf{LCM}(\mathsf{HT}(f_k), \mathsf{HT}(f_l)) \in \mathcal{M}$. Note that as in the case of prefix reduction in theorem 4.4.35 we can localize ourselves to this part of the original overlap $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l$. We will now change our representation of g by using the additional information on this s-polynomial in such a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume $\mathsf{spol}_c(f_k, f_l) \neq 0$[36]. Hence, the reduction sequence $\mathsf{spol}_c(f_k, f_l) \xrightarrow{*}{}^{c}_{F} 0$ results in a free commutative standard representation of the form $\mathsf{spol}_c(f_k, f_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i$ such that $\delta_i \in \mathbf{K}^*, h_i \in F, v_i \in \mathcal{M}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_c(f_k, f_l))$. Then by lemma 4.5.15 we can conclude that t is a real bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * w$. Furthermore, we can assume that this representation is of the required form, as we can substitute all polynomials h_i, where $\mathsf{HT}(h_i * v_i * w_k) \neq \mathsf{HT}(h_i) \circ_{\mathcal{T}} (v_i \circ w)$ without increasing t or K. This gives us:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \;& \alpha_k \cdot f_k * w_k + \underbrace{\alpha'_l \cdot \beta_k \cdot f_k * w_k - \alpha'_l \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha'_l \cdot \beta_l \cdot f_l * w_l \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}_c(f_k, f_l) * w} \\
= \;& (\alpha_k + \alpha'_l \cdot \beta_k) \cdot f_k * w_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i * w) \qquad (4.4)
\end{aligned}$$

where $\beta_k = \mathsf{HC}(f_k)^{-1}$,$\beta_l = \mathsf{HC}(f_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (4.4) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

q.e.d.

Now theorem 4.5.31 gives rise to the following procedure that computes a Gröbner basis with respect to $\longrightarrow^{c}$ for a finitely generated ideal similar to procedure Prefix Gröbner Bases on page 110. The resulting set is additionally commutatively saturated.

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

Procedure: COMMUTATIVE GRÖBNER BASES

Given: A finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$.
Find: $\text{GB}_c(F)$, a commutative Gröbner basis of F.
Using: SAT_c a commutative saturating procedure for polynomials.

$G := \bigcup_{f \in F} \text{SAT}_c(f)$
$B := \{(q_1, q_2) \mid q_1, q_2 \in G\}$;
% B is used to check statement 2 of theorem 4.5.31
while $B \neq \emptyset$ **do**
  $(q_1, q_2) :=$ remove(B);
  % Remove an element from a set
  if $\mathsf{spol}_c(q_1, q_2)$ exists
    % Compute the s-polynomial if it is not trivial
    then $h :=$ normalform$(\mathsf{spol}_c(q_1, q_2), \longrightarrow^{c}_{G})$;
      % Compute a normal form using commutative reduction
      if $h \neq 0$
        % Statement 2 of theorem 4.5.31 does not hold
        then $G := G \cup \text{SAT}_c(h)$;
          % G is extended to achieve statement 2
          % G is commutatively saturated
          $B := B \cup \{(f, \tilde{h}) \mid f \in G, \tilde{h} \in \text{SAT}_c(h)\}$;
      endif
  endif
endwhile
$\text{GB}_c(F) := G$

Lemma 4.5.32
Procedure COMMUTATIVE GRÖBNER BASES *terminates.*

Proof :
New polynomials are only added in case an s-polynomial does not reduce to zero. Hence, if our procedure would not terminate there would be an infinite sequence of normal forms of s-polynomials added contradicting the fact that the set of head terms of these polynomials has a finite basis via $\circ_{\mathcal{T}}$ as a subset of $\mathcal{T}$ by Dickson's lemma and the ideal can be characterized by the head terms of the polynomials it contains as described in theorem 4.5.7.

q.e.d.

Lemma 4.5.33
Procedure COMMUTATIVE GRÖBNER BASES *is correct.*

Proof :
This follows immediately from theorem 4.5.31.

q.e.d.

The sets characterized in theorem 4.5.31 are commutative Gröbner bases and hence right Gröbner bases, but they are required to be commutatively saturated. Reviewing example 4.5.5 we see that there exist right Gröbner bases in commutative monoid rings which are not commutatively saturated.

Example 4.5.34
Let $\Sigma = \{a, b\}$ and $T_c = \{a^2 \longrightarrow \lambda, b^2 \longrightarrow \lambda\}$ be a presentation of a commutative monoid $\mathcal{M}$ (which is in fact a group) with a length-lexicographical ordering induced by $a \succ b$.
Then the set $\{ab+\lambda\} \subseteq \mathbf{Q}[\mathcal{M}]$ itself is a right Gröbner basis, but neither commutatively saturated nor a commutative Gröbner basis. We have $a + b \in \mathsf{ideal}(ab + \lambda)$ but $a + b \not\longrightarrow^{c}_{ab+\lambda} 0$. ◇

Note that a commutative Gröbner basis need not be commutatively saturated.

Example 4.5.35
Let $\Sigma = \{a, b, c, d, e\}$ and $T_c = \{ac \longrightarrow d, bc \longrightarrow e\}$ be a presentation of a commutative monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c \succ d \succ e$.
Then the set $F = \{a + b, d + \lambda, e - \lambda\}$ is a commutative Gröbner basis in $\mathbf{Q}[\mathcal{M}]$. This can be seen by studying the right ideal generated by F, $\mathsf{ideal}(F) = \{\alpha_1 \cdot (a + b) * w_1 + \alpha_2 \cdot (d - \lambda) * w_2 + \alpha_3 \cdot (e - \lambda) * w_3 + \alpha_4 \cdot (d + e) * w_4 | \alpha_i \in \mathbf{Q}, w_i \in \mathcal{M}, w_1 \neq c \circ_T w'\}$.
But F is not commutatively saturated, as $(a + b) * c = d + e \not\longrightarrow^{c}_{F} 0$. We only have $d + e \stackrel{2}{\longrightarrow}{}^{c}_{F} 0$. ◇

Next we will give a characterization of commutative Gröbner bases as free commutative standard bases without demanding that the set of polynomials is commutatively saturated. This is important as interreducing a set of commutatively saturated polynomials destroys this property. But interreducing a free commutative standard basis again gives us a free commutative standard basis. Remember that this is also true for prefix standard bases but not for stable standard bases in general.

Theorem 4.5.36
For a set F of polynomials in $\mathbf{K}[\mathcal{M}]$, equivalent are:

1. *Every polynomial $g \in \mathsf{ideal}(F)$ has a free commutative standard representation.*
2. (a) *For all polynomials $f \in F$ and all elements $w \in \mathcal{M}$, the polynomial $f * w$ has a free commutative standard representation.*
   (b) *For all polynomials $f_k, f_l \in F$ the non-trivial commutative s-polynomials have free commutative standard representations.*

Proof :
$1 \Longrightarrow 2$: This follows immediately.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}(F)\backslash\{0\}$ has a free commutative standard representation. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be an arbitrary representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{M}$. By our assumption and lemma 4.5.3 we can assume $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$ as $f_i \in F$ and every $f_i * w_i$ has a free commutative standard representation[37]. Now using statement (a) and (b) we can show as in theorem 4.5.31 how the representation of g can be transformed into a free commutative standard representation.

q.e.d.

Note that this theorem gives us a stronger characterization of commutative Gröbner bases, as it does not require them to be commutatively saturated.

Remark 4.5.37
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$.

1. If F is commutatively saturated, then for every polynomial $f \in F$ and every element $w \in \mathcal{M}$ the polynomial $f * w$ has a free commutative standard representation. This follows immediately, since $f * w \longrightarrow^{\mathrm{c}}_{F} 0$ implies that there exists a polynomial $f' \in F$ such that $f * w \longrightarrow^{\mathrm{c}}_{f'} 0$ and $\mathsf{HT}(f * w) = \mathsf{HT}(f') \circ_{\mathcal{T}} u$ for some $u \in \mathcal{M}$. Note that F need not be a free commutative standard basis.

2. On the other hand, if for all polynomials $f \in F$ and all elements $w \in \mathcal{M}$ the polynomial $f * w$ has a free commutative standard representation, this need not imply that F is commutatively saturated. To see this, let us review example 4.5.35
Let $\Sigma = \{a, b, c, d, e\}$ and $T_c = \{ac \longrightarrow d, bc \longrightarrow e\}$ be a semi-Thue system modulo commutativity presenting a commutative monoid $\mathcal{M}$ with a length-lexicographical ordering induced by $a \succ b \succ c \succ d \succ e$.
Then for every polynomials f in the set $F = \{a+b, d+\lambda, e-\lambda\}$ and every element $w \in \mathcal{M}$ the multiple $f * w$ has a free commutative standard representation. For the elements $w \in \mathcal{M}$ where $(a+b) * w = a \circ_{\mathcal{T}} w + b \circ_{\mathcal{T}} w$, $(d+\lambda) * w = d \circ_{\mathcal{T}} w + w$ and $(e - \lambda) * w = e \circ_{\mathcal{T}} w - w$, these are free commutative standard representations. It remains to check the case $(a + b) * (c \circ_{\mathcal{T}} w) = d \circ_{\mathcal{T}} w + e \circ_{\mathcal{T}} w$. Since $d + e \longrightarrow^{\mathrm{c}}_{d+\lambda} e - \lambda \longrightarrow^{\mathrm{c}}_{e-\lambda} 0$, we have a free commutative standard representation $d \circ_{\mathcal{T}} w + e \circ_{\mathcal{T}} w = (d+\lambda) * w + (e-\lambda) * w$, but $d \circ_{\mathcal{T}} w + e \circ_{\mathcal{T}} w$ does not commutatively reduce to zero using F in *one* step. We only have $(d + e) * w \xrightarrow{2}{}^{\mathrm{c}}_{F} 0$. $\diamond$

Definition 4.5.38
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ **weakly commutatively saturated**, if for all $f \in F$ and all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$ we have $\alpha \cdot f * w \xrightarrow{*}{}^{\mathrm{c}}_{F} 0$. $\diamond$

[37] Note that these free commutative standard representations do not yield a free commutative standard representation for the polynomial g, as $\mathsf{HT}(g) \prec \mathsf{HT}(f_i) \circ_{\mathcal{T}} w_i$ is possible.

If a set of polynomials F is weakly commutatively saturated this implies that for all $f \in F$ and all $w \in \mathcal{M}$ the polynomial $f * w$, in case it is non-zero, has a free commutative standard representation. Thus we can give the following procedure to compute reduced commutative Gröbner bases where weak saturation is ensured by the use of a saturating procedure for polynomials.

Procedure: Reduced Commutative Gröbner Bases

Given: A finite set $F \subseteq \mathbf{K}[\mathcal{M}]$.
Find: $\text{GB}(F)$, a commutative Gröbner basis of F.
Using: A procedure SAT_c for computing commutatively saturating sets.
$G_0 := \emptyset$;
$S_0 := F$;
$i := 0$;
while $S_i \neq \emptyset$ do
  $i := i + 1$;
  $q_i := \text{remove}(S_{i-1})$;
  % Remove an element using a fair strategy
  $q_i' := \text{normalform}(q_i, \longrightarrow^{\text{c}}_{G_{i-1}})$;
  % Compute a normal form using commutative reduction
  if $q_i' \neq 0$
    % Statement 2 of theorem 4.5.36 does not hold
    then $H_i := \{g \in G_{i-1} \mid \mathsf{HT}(g) \text{ is commutatively reducible using } q_i'\}$;
      % These polynomials would have new head terms after commutative
      % reduction using q_i'
      $G_i := \text{reduce}((G_{i-1} \backslash H_i) \cup \{q_i'\})$;
      % $\text{reduce}(F) = \{\text{normalform}(f, \longrightarrow^{\text{c}}_{F\backslash\{f\}}) | f \in F\}$[38]
      % No head term of a polynomial in G_i is commutatively reducible by the
      % other polynomials in G_i
      $S_i := S_{i-1} \cup H_i \cup \bigcup_{g \in (G_i \backslash G_{i-1})} (\text{SAT}_c(g) \backslash \{g\})$
        $\cup \{\mathsf{spol}_c(f, g) \mid f \in G_i, g \in G_i \backslash G_{i-1}\}$;
    else $G_i := G_{i-1}$;
      $S_i := S_{i-1}$;
  endif
endwhile
$\text{GB}(F) := G_i$

The sets S_i will contain saturating sets and s-polynomials corresponding to polynomials added to some set G_j. Hence, in general this set will contain polynomials that are no longer necessary, e.g. in case a polynomial is removed from a set G_j neither its s-polynomials nor all saturating polynomials need to be considered. This is due to the fact that the conditions named in theorem 4.5.36 must hold for the final set G_k only. Hence it is possible to develop marking strategies in order to keep the sets S_i smaller.

The following lemmata ensure the correctness of our procedure.

[38] Notice that only the reducts of the polynomials are touched in this procedure.

Lemma 4.5.39
Let F be a set of polynomials in $\mathbf{K}[\mathcal{M}]$ and G_i, S_i, $i \in \mathbf{N}$ the respective sets in procedure Reduced Commutative Gröbner Bases. *Then we have*

$$\mathsf{ideal}(F) = \mathsf{ideal}(G_i \cup S_i).$$

Proof :
For $i = 0$ we have $G_0 \cup S_0 = F$ and hence $\mathsf{ideal}(F) = \mathsf{ideal}(G_0 \cup S_0)$. For $i > 0$ let G_{i-1}, S_{i-1} be the respective sets before entering the **while** loop for its i-th iteration. Further let q_i be the polynomial chosen from S_{i-1} and q_i' a normal from of q_i with respect to commutative reduction using G_{i-1}. Then in case $q_i' = 0$ we know $q_i \in \mathsf{ideal}(G_{i-1})$ and thus as $G_i = G_{i-1}$ and $S_i = S_{i-1}\backslash\{q_i\}$ we can conclude

$$\mathsf{ideal}(G_i \cup S_i) = \mathsf{ideal}(G_{i-1} \cup S_{i-1}) = \mathsf{ideal}(F).$$

In case $q_i' \neq 0$, we know $\mathsf{ideal}(\text{reduce}((G_{i-1}\backslash H_i) \cup \{q_i'\})) = \mathsf{ideal}((G_{i-1}\backslash H_i) \cup \{q_i'\})$, $\mathsf{ideal}(G_{i-1} \cup \{q_i'\} \cup (S_{i-1}\backslash\{q_i\})) = \mathsf{ideal}(G_{i-1} \cup S_{i-1})$ and $\mathsf{ideal}(\bigcup_{g\in(G_i\backslash G_{i-1})}(\textsc{Sat}_c(g)\backslash\{g\}) \cup \{\mathsf{spol}_c(f,g) \mid f \in G_i, g \in G_i\backslash G_{i-1}\}) \subseteq \mathsf{ideal}(G_i)$.
Abbreviating $\bigcup_{g\in(G_i\backslash G_{i-1})}(\textsc{Sat}_c(g)\backslash\{g\})$ by S_c we can conclude

$$\begin{aligned}
& \mathsf{ideal}(G_i \cup S_i) \\
= \;& \mathsf{ideal}(G_i \cup (S_{i-1}\backslash\{q_i\}) \cup H_i \cup S_c \cup \{\mathsf{spol}_c(f,g) \mid f \in G_i, g \in G_i\backslash G_{i-1}\}) \\
= \;& \mathsf{ideal}_r(G_i \cup (S_{i-1}\backslash\{q_i\}) \cup H_i) \\
= \;& \mathsf{ideal}_r(\text{reduce}((G_{i-1}\backslash H_i) \cup \{q_i'\}) \cup (S_{i-1}\backslash\{q_i\}) \cup H_i) \\
= \;& \mathsf{ideal}((G_{i-1}\backslash H_i) \cup \{q_i'\} \cup (S_{i-1}\backslash\{q_i\}) \cup H_i) \\
= \;& \mathsf{ideal}(G_{i-1} \cup \{q_i'\} \cup (S_{i-1}\backslash\{q_i\})) \\
= \;& \mathsf{ideal}(G_{i-1} \cup S_{i-1}) \\
= \;& \mathsf{ideal}_r(F).
\end{aligned}$$

q.e.d.

Remark 4.5.40
As in the case of procedure Reduced Prefix Gröbner Bases on page 114 the head terms of the polynomials in the sets G_i fulfill that every term that had a divisor in a set $\mathsf{HT}(G_k)$ will then also have a divisor in each set $\mathsf{HT}(G_{k+n})$, $n \in \mathbf{N}$. Hence, as the polynomials added are always in normal form and the sets $\mathsf{HT}(G_i)$ can be regarded as subsets of $\mathcal{T}$, Dickson's lemma yields termination. $\diamond$

Theorem 4.5.41
Let G be the set generated by procedure Reduced Commutative Gröbner Bases *on a finite input $F \subseteq \mathbf{K}[\mathcal{M}]$. Then the following statements hold:*

1. $\mathsf{ideal}(G) = \mathsf{ideal}(F)$.

2. *For all polynomials $f \in G$ and all elements $w \in \mathcal{M}$, the polynomial $f * w$ has a free commutative standard representation in case it is non-zero.*

3. *For all polynomials $f_k, f_l \in F$ the non-trivial commutative s-polynomials have free commutative standard representations.*

4. *G is a reduced commutative Gröbner basis.*

Proof :
Since procedure Reduced Commutative Gröbner Bases terminates we have $G = G_k$ for some $k \in \mathbf{N}$ and $S_k = \emptyset$. Now as by lemma 4.5.39 we have $\mathsf{ideal}(F) = \mathsf{ideal}(G_i \cup S_i)$ for all $i \in \mathbf{N}$, this implies $\mathsf{ideal}(F) = \mathsf{ideal}(G)$. Since according to our construction all s-polynomials corresponding to polynomials in G are not commutatively reducible to zero, it remains to show that for all $f \in G$, $w \in \mathcal{M}$ the right multiple $f * w$ has a free commutative standard representation with respect to G. We will first show that for all $i \leq k$, $f \in S_i \cup G_i$ implies that f has a free commutative standard representation with respect to G. This can be done by induction on j where $i = k - j$. The case $j = 0$ is trivial, as this implies $S_k = 0$ and every $f \in G_k$ has a free commutative standard representation with respect to $G = G_k$. Hence let $f \in S_{k-(j+1)} \cup G_{k-(j+1)}$ and suppose $f \notin S_{k-j} \cup G_{k-j}$, as otherwise we are already done. In case $f \in G_{k-(j+1)}$, as $f \notin G_{k-j}$, f must be commutatively reducible by q'_{k-j}. Then either $f \in S_{k-j}$ if $\mathsf{HT}(f)$ is commutatively reducible by q'_{k-j} and our induction hypothesis then yields the existence of a free commutative standard representation for f. Or f is the result of reduction during the computation of the set $G_{k-j} = \mathrm{reduce}((G_{k-(j+1)} \backslash H_{k-j}) \cup \{q'_{k-j}\})$. But then by lemma 4.5.12, f has a free commutative standard representation with respect to G_{k-j} yielding the existence of a free commutative standard representation with respect to G, as every polynomial in G_{k-j} has one. In case $f \in S_{k-(j+1)}$, as $f \notin S_{k-j}$, f is chosen to compute the polynomial $q'_{k-j} = \mathrm{normalform}(f, \longrightarrow^{\mathrm{c}}_{G_{k-j+1}})$. Now in case $q'_{k-j} = 0$ we have $G_{k-(j+1)} = G_{k-j}$ and hence f has a free commutative standard representation with respect to G_{k-j}. Furthermore, as every polynomial in G_{k-j} by induction hypothesis has a free commutative standard representation with respect to G, by lemma 4.5.12 we are done. If $q'_{k-j} \neq 0$ we get that f has a free commutative standard representation with respect to $G_{k-(j+1)} \cup \{q'_{k-j}\}$ and even with respect to $G_{k-j} = \mathrm{reduce}((G_{k-(j+1)} \backslash H_{k-j}) \cup \{q'_{k-j}\})$. Again by the induction hypothesis and by lemma 4.5.12, f has a free commutative standard representation with respect to G.
Now let us return to our initial goal, to prove that for all polynomials $f \in G$ and all elements $w \in \mathcal{M}$, the polynomial $f * w$ has a free commutative standard representation in case it is non-zero. Since $f \in G$, the polynomials in $\textsc{Sat}_c(f) \backslash \{f\}$ have been added to some set S_i, i.e., there exists a polynomial $f' \in S_i \cup G_i$ such that $f * w \longrightarrow^{\mathrm{c}}_{f'} 0$ and f' has a free commutative standard representation. Then by lemma 4.5.12 we can conclude that $f * w$ also has a free commutative standard representation.
By construction, G is a reduced set of polynomials and by theorem 4.5.36 we can

conclude that G is a reduced commutative Gröbner basis.

q.e.d.

We end this section by sketching how Buchberger's algorithm can be lifted to quotient rings of polynomial rings and how these quotients are related to finitely generated commutative monoid rings. The ideas are mainly the same as stated by Deiß in [De89]. Let us start by recalling Buchberger's definition of reduction for a polynomial ring $\mathbf{K}[X_1, \ldots, X_n]$. Remember that $p \longrightarrow^{\mathrm{b}}_{f} q$ at a monomial $\alpha \cdot t$, if $\mathsf{HT}(f) \circ_{\mathcal{T}} u = t$ for some $u \in \mathcal{T}$, and $q = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f * u$.

Henceforth we will assume that our finitely generated commutative monoid $\mathcal{M}$ is presented by a finite convergent semi-Thue system modulo commutativity $T_c \subseteq \mathcal{T} \times \mathcal{T}$ where $\mathcal{T}$ is again the free commutative monoid generated now by an alphabet $\Sigma = \{X_1, \ldots, X_n\}$ to show the connection to the ordinary polynomial ring. Then we can consider the set R as a set of polynomials $P_{T_c} = \{l - r | (l, r) \in T_c\}$. Then P_{T_c} is a Gröbner basis with respect to the well-founded admissible completion ordering $\succeq$ on $\mathcal{T}$ related to the presentation (Σ, T_c).

We can show that in this context the monoid ring $\mathbf{K}[\mathcal{M}]$ is in fact isomorphic to a quotient of the ordinary polynomial ring $\mathbf{K}[X_1, \ldots, X_n]$.

Lemma 4.5.42
Let $\mathcal{M}$ be a commutative monoid presented by (Σ, T_c). Then $\mathbf{K}[\mathcal{M}]$ is isomorphic to $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$.

Proof :
Let $\varphi : \mathbf{K}[X_1, \ldots, X_n] \longrightarrow \mathbf{K}[\mathcal{M}]$ be the natural ring homomorphisms defined by setting $\varphi(\sum_{i=1}^{k} \alpha_i \cdot w_i) = \sum_{i=1}^{k} \alpha_i \cdot [w_i]_{\mathcal{M}}$ with $\alpha_i \in \mathbf{K}$, $w_i \in \mathcal{T}$. Then as in lemma 4.4.51 one can show that the kernel of φ is an ideal in $\mathbf{K}[X_1, \ldots, X_n]$, namely $\mathsf{ideal}^{\mathbf{K}[X_1,\ldots,X_n]}(P_{T_c})$, and hence $\mathbf{K}[\mathcal{M}]$ is isomorphic to the ring $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}^{\mathbf{K}[X_1,\ldots,X_n]}(P_{T_c})$.

q.e.d.

Now let us state how computation in our quotient structure is done. For a polynomial $p = \sum_{i=1}^{m} \alpha_i \cdot t_i \in \mathbf{K}[X_1, \ldots, X_n]$ we define

$$[p]_{\mathsf{ideal}(P_{T_c})} = \sum_{i=1}^{m} \alpha_i \cdot [t_i[_{\mathcal{M}} = \sum_{i=1}^{m} \alpha_i \cdot t_i {\downarrow}_{P_{T_c}}$$

and we will write p instead of $[p]_{\mathsf{ideal}(P_{T_c})}$ to denote elements of $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ or $p{\downarrow}_{P_{T_c}}$ if we want to turn a polynomial in $\mathbf{K}[X_1, \ldots, X_n]$ into an element of the quotient.

Definition 4.5.43
Let p, q be two polynomials in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$. Then we can define **addition** and **multiplication** as follows:

1. $p \oplus q = [p +_{\mathbf{K}[X_1,\ldots,X_n]} q]_{\mathsf{ideal}(P_{T_c})} = (p +_{\mathbf{K}[X_1,\ldots,X_n]} q){\downarrow}_{P_{T_c}}$

2. $p \otimes q = [p *_{\mathbf{K}[X_1,\ldots,X_n]} q]_{\mathsf{ideal}(P_{T_c})} = (p *_{\mathbf{K}[X_1,\ldots,X_n]} q)\downarrow_{P_{T_c}}$

such that $+_{\mathbf{K}[X_1,\ldots,X_n]}$ and $*_{\mathbf{K}[X_1,\ldots,X_n]}$ are the corresponding ring operations in the polynomial ring $\mathbf{K}[X_1,\ldots,X_n]$. $\diamond$

Then $\mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})$ together with $\oplus$ and $\otimes$ is a commutative ring with unit. We will now introduce quotient reduction to this structure by lifting Buchberger's reduction.

Definition 4.5.44
Let p, f be two non-zero polynomials in $\mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})$. Then we set $p \Longrightarrow_f q$ at a monomial $\alpha \cdot t$ of p if there exists a polynomial q' in $\mathbf{K}[X_1,\ldots,X_n]$ such that $p \longrightarrow^{\mathrm{b}}_f q'$ at $\alpha \cdot t$ and $q = q'\downarrow_{P_{T_c}}$. We can define $\stackrel{*}{\Longrightarrow}$, $\stackrel{+}{\Longrightarrow}$, and $\stackrel{n}{\Longrightarrow}$ as usual. Reduction by a set $F \subseteq \mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})$ is denoted by $p \Longrightarrow_F q$ and stands for $p \Longrightarrow_f q$ for some $f \in F$, also written as $p \Longrightarrow_{f \in F} q$. $\diamond$

For this reduction we can now state:

Lemma 4.5.45
Let F be a set of polynomials and p, q some polynomials in $\mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})$.

1. $\Longrightarrow_F \subseteq \stackrel{*}{\longrightarrow}^{\mathrm{b}}_{F \cup P_{T_c}}$, *i.e., reduction in the quotient can be simulated by reduction in the polynomial ring using additional polynomials.*

2. $p \Longrightarrow_F q$ *implies* $p > q$.

3. $\Longrightarrow_F$ *is Noetherian.*

Proof :

1. This follows by the definition of reduction, since $p \Longrightarrow_f q$ can be simulated by $p \longrightarrow^{\mathrm{b}}_f q' \stackrel{*}{\longrightarrow}^{\mathrm{b}}_{P_{T_c}} q$.

2. This follows immediately as Buchberger's reduction already has this property.

3. This follows from the fact that Buchberger's reduction is Noetherian.

q.e.d.

But although $\mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})$ still is a Noetherian ring, many other properties of reduction in $\mathbf{K}[X_1,\ldots,X_n]$ are lost as for example the quotient may contain zero-divisors.

Lemma 4.5.46
Let $p, q, h \in \mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})$ and $h \neq 0$.

1. $q < p$ *no longer implies* $q \otimes h < p \otimes h$.

2. $p \Longrightarrow_p 0$ *no longer implies* $p \otimes h \Longrightarrow_p 0$.

Example 4.5.47
Let $\Sigma = \{X_1\}$ and $P_T = \{X_1^2 - 1\}$ be a presentation of a commutative monoid.
Then $p = X_1$, $q = 1$ and $h = X_1$ gives us an appropriate counter-example, as we have $q < p$, but $q \otimes h = X_1 > p \otimes h = 1$, and $p \otimes h = 1$ cannot be quotient reduced to zero by p. $\diamond$

In the polynomial ring a basis of an ideal is called a Gröbner basis if Buchberger's reduction using it is confluent. We can easily extend this definition to our quotient structure.

Definition 4.5.48
A set of polynomials $G \subseteq \mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ is said to be a **Gröbner basis** with respect to $\Longrightarrow$, if

1. $\overset{*}{\Longleftrightarrow}_G \; = \; \equiv_{\mathsf{ideal}(G)}$, and
2. $\Longrightarrow_G$ is confluent. $\diamond$

Unfortunately, a polynomial alone is no longer a Gröbner basis, as in example 4.5.47 the set $\{p\}$ is no Gröbner basis. This is due to the fact that reduction in the quotient $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ no longer captures the ideal congruence. In our example we have $X_1 \equiv_{\mathsf{ideal}(p)} 1$ but $X_1 \overset{*}{\not\Longleftrightarrow}_p 1$.

In order to describe Gröbner bases, let us continue by giving a sufficient condition for confluence.

Lemma 4.5.49
Let P_{T_c} be a Gröbner basis in $\mathbf{K}[X_1, \ldots, X_n]$, $F \subseteq \mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$. Then if $\longrightarrow^{\mathrm{b}}_{F \cup P_{T_c}}$ is confluent on $\mathbf{K}[X_1, \ldots, X_n]$, $\Longrightarrow_F$ is confluent on $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$.

Proof :
Suppose there exist $f, h_1, h_2 \in \mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ such that we get $f \Longrightarrow_F h_1$ and $f \Longrightarrow_F h_2$. Then we can view these polynomials as elements of $\mathbf{K}[X_1, \ldots, X_n]$ and substitute $\Longrightarrow_F$ by $\overset{*}{\longrightarrow}^{\mathrm{b}}_{F \cup P_{T_c}}$ giving us $f \overset{*}{\longrightarrow}^{\mathrm{b}}_{F \cup P_{T_c}} h_1$ and $f \overset{*}{\longrightarrow}^{\mathrm{b}}_{F \cup P_{T_c}} h_2$. Hence, as $\longrightarrow^{\mathrm{b}}_{F \cup P_{T_c}}$ is confluent, there exists a polynomial $g \in \mathbf{K}[X_1, \ldots, X_n]$ such that $h_1 \overset{*}{\longrightarrow}^{\mathrm{b}}_{F \cup P_{T_c}} g$ and $h_2 \overset{*}{\longrightarrow}^{\mathrm{b}}_{F \cup P_{T_c}} g$. Since $\longrightarrow^{\mathrm{b}}_{F \cup P_{T_c}}$ is convergent we can use the following reduction strategy:

1. Do as many reduction steps as possible using P_{T_c}.
2. If possible apply one reduction step using F and return to 1.

We stop as soon as no more reduction steps are possible. Note that in this fashion we can combine reduction steps as required in the definition of reduction $\Longrightarrow_F$. This gives us that $h_1 \stackrel{*}{\Longrightarrow}_F \tilde{g}$ and $h_2 \stackrel{*}{\Longrightarrow}_F \tilde{g}$, where $\tilde{g} = g{\downarrow}_{P_{T_c}}$.

q.e.d.

The converse is not true as in example 4.5.47, $\Longrightarrow_{X_1}$ is confluent on $\mathbf{K}[X_1]/\mathsf{ideal}(X_1^2 - 1)$, but $\longrightarrow^{\mathrm{b}}_{\{X_1\} \cup \{X_1^2 - 1\}}$ is not confluent on $\mathbf{K}[X_1]$.
In order to use this lemma to sketch how a Gröbner basis with respect to quotient reduction can be computed, we use Buchberger's s-polynomials. Remember that the s-polynomial for two polynomials $p, q \in \mathbf{K}[X_1, \ldots, X_n]$ is defined as $\mathsf{spol}(p, q) = \mathsf{HC}(p)^{-1} \cdot p * u - \mathsf{HC}(q)^{-1} \cdot q * v$, where $\mathsf{LCM}(\mathsf{HT}(p), \mathsf{HT}(q)) = \mathsf{HT}(p) \circ_T u = \mathsf{HT}(q) \circ_T v$. We can thus compute an (even reduced) Gröbner basis by modifying Buchberger's algorithm as follows:

Compute the (reduced) Gröbner basis G' of $F \cup P_{T_c}$ in $\mathbf{K}[X_1, \ldots, X_n]$ with respect to Buchberger's reduction without changing the polynomials in P_{T_c}. Then the set $G := G' \backslash P_T$ is the reduced Gröbner basis of F in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$.

Computing the Gröbner basis of $F \cup P_{T_c}$ three kinds of s-polynomials can arise:

1. $f, g \in P_{T_c}$: Then the corresponding s-polynomial can be omitted, as P_T is already a Gröbner basis.
2. $f, g \in F$: Then the s-polynomial corresponds to the commutative s-polynomial as defined in 4.5.30.
3. $f \in F$, $g \in P_{T_c}$: Then the s-polynomial corresponds to the process of saturating f, in particular to the step of overlapping the head term of f with the rule $l \longrightarrow r$ where $g = l - r$ (compare procedure COMMUTATIVE SATURATION on page 139).

Thus we have a characterization of Gröbner bases in the quotient structure as follows:

Theorem 4.5.50
Let $P_{T_c} \subseteq \mathbf{K}[X_1, \ldots, X_n]$ be a reduced Gröbner basis in $\mathbf{K}[X_1, \ldots, X_n]$ and F a set of polynomials in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$. Then the following statements are equivalent:

1. *F is a Gröbner basis in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$.*
2. *(a) For all $f, g \in F$ we have $(\mathsf{spol}(f, g)){\downarrow}_{P_{T_c}} \stackrel{*}{\Longrightarrow}_F 0$, and*
   (b) for all $f \in F$, $g \in P_{T_c}$ we have $(\mathsf{spol}(f, g)){\downarrow}_{P_{T_c}} \stackrel{*}{\Longrightarrow}_F 0$.

Proof :
$1 \Longrightarrow 2$: This follows immediately as all s-polynomials lie in $\mathsf{ideal}^{\mathbf{K}[X_1,\ldots,X_n]/\mathsf{ideal}(P_{T_c})}(F)$ and therefore are congruent to zero. Thus the confluence of F implies that they can be reduced to zero using F.

$2 \Longrightarrow 1$: The statements (a) and (b) imply that $F \cup P_{T_c}$ is a Gröbner basis in the polynomial ring $\mathbf{K}[X_1, \ldots, X_n]$, i.e., $\longrightarrow^{\mathrm{b}}_{F \cup P_{T_c}}$ is confluent. Hence, by lemma 4.5.49

$\Longrightarrow_F$ is also confluent.
It remains to show that $\overset{*}{\Longleftrightarrow}_F = \equiv_{\mathsf{ideal}(F)}$. Obviously, $\overset{*}{\Longleftrightarrow}_F \subseteq \equiv_{\mathsf{ideal}(F)}$. On the other hand let p and q be polynomials in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$. Then $p \equiv_{\mathsf{ideal}(F)} q$ in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ implies $p \equiv_{\mathsf{ideal}(F \cup P_{T_c})} q$ in $\mathbf{K}[X_1, \ldots, X_n]$. Further, as $F \cup P_{T_c}$ is a Gröbner basis in $\mathbf{K}[X_1, \ldots, X_n]$, we know $\equiv_{\mathsf{ideal}(F \cup P_{T_c})} = \overset{*}{\longleftrightarrow}{}^{\mathrm{b}}_{F \cup P_{T_c}}$, and as $\longrightarrow^{\mathrm{b}}_{F \cup P_{T_c}}$ is confluent, $p \overset{*}{\longleftrightarrow}{}^{\mathrm{b}}_{F \cup P_{T_c}} q$ implies $p \downarrow_{F \cup P_{T_c}} q$. Thus, as in lemma 4.5.49, we can conclude $p \Downarrow_F q$ giving us $p \overset{*}{\Longleftrightarrow}_F q$.
This completes the proof that F is a Gröbner basis in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$.

q.e.d.

We will close this section by comparing the reduction introduced here for a quotient structure to right and commutative reduction in the corresponding commutative monoid ring. For a polynomial $p \in \mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ let $\tilde{p}$ be the corresponding polynomial in the monoid ring $\mathbf{K}[\mathcal{M}]$.

Lemma 4.5.51
Let p, q, f be some polynomials in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ and let $\tilde{p}, \tilde{q}, \tilde{f}$ be the corresponding polynomials in $\mathbf{K}[\mathcal{M}]$. Then $p \Longrightarrow_f q$ if and only if $\tilde{p} \longrightarrow^{\mathrm{c}}_{\tilde{f}} \tilde{q}$.

Proof :
Before entering the proof of our claim let us first take a closer look at reduction in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$. If $p \Longrightarrow_f q$ at a monomial $\alpha \cdot t$ with $t = \mathsf{HT}(f) \circ_{\mathcal{T}} u$, then we can express this reduction step by $p \longrightarrow^{\mathrm{b}}_f q' \overset{*}{\longrightarrow}{}^{\mathrm{b}}_{P_{T_c}} q$ and we have $q' = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f *_{\mathbf{K}[X_1,\ldots,X_n]} u$ and $q = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot f \otimes u$. In this context it is easy to see that $p \Longrightarrow_f q$ implies $\tilde{p} \longrightarrow^{\mathrm{c}}_{\tilde{f}} \tilde{q}$. On the other hand, commutative reduction requires that the head term of the polynomial is a divisor with respect to $\circ_{\mathcal{T}}$ of the term to be reduced, i.e., for T_c the term corresponding to t in $\tilde{p}$ we get $T_c = \mathsf{HT}(\tilde{f}) \circ_{\mathcal{T}} \tilde{u}$ and $\tilde{q} = \tilde{p} - \alpha \cdot \mathsf{HC}(\tilde{f})^{-1} \cdot \tilde{f} *_{\mathbf{K}[\mathcal{M}]} \tilde{u}$. Hence, a commutative reduction step in our monoid ring can be split into first doing one step using Buchberger's reduction and then normalizing the new monomials using P_{T_c}.

q.e.d.

Corollary 4.5.52
Let $G \subseteq \mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ and let $\tilde{G}$ be the corresponding set in $\mathbf{K}[\mathcal{M}]$. Then G is a Gröbner basis with respect to $\Longrightarrow$ if and only if $\tilde{G}$ is a Gröbner basis with respect to $\longrightarrow^{\mathrm{c}}$. □

Obviously, then $\Longrightarrow$ must be weaker than $\longrightarrow^{\mathrm{r}}$.

Corollary 4.5.53
Let p, q, f be some polynomials in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ and let $\tilde{p}, \tilde{q}, \tilde{f}$ be the corresponding polynomials in $\mathbf{K}[\mathcal{M}]$. Then $p \Longrightarrow_f q$ implies $\tilde{p} \longrightarrow^{\mathrm{r}}_{\tilde{f}} \tilde{q}$ but not vice versa.

Example 4.5.54
Let $\Sigma = \{X_1, X_2\}$ and $T_c = \{X_1^2 \longrightarrow \lambda, X_2^2 \longrightarrow \lambda\}$ be a presentation of a commutative group $\mathcal{G}$ with a length-lexicographical ordering induced by $X_1 \succ X_2$. Further let $\tilde{p} = X_2$ and $\tilde{f} = X_1X_2$ be polynomials in $\mathbf{K}[\mathcal{G}]$.
Then $\tilde{p} \longrightarrow^{\mathrm{r}}_{\tilde{f}} 0$, but for the corresponding polynomials p, f in $\mathbf{K}[X_1, \ldots, X_n]/\mathsf{ideal}(P_{T_c})$ we have $p \not\Longrightarrow_f$, as $X_1 \not\longrightarrow^{\mathrm{b}}_{X_1X_2}$. Note that the set $\{\tilde{f}\}$ itself is a Gröbner basis with respect to $\longrightarrow^{\mathrm{r}}$ but not with respect to $\longrightarrow^{\mathrm{c}}$, nor is $\{f\}$ a Gröbner basis with respect to $\Longrightarrow$. $\diamond$

Chapter 5

Group Rings

Longum iter est per praecepta,
Breve et efficax per exempla.

SENECA

In this chapter we want to apply the ideas of reduction developed in the previous chapter to group rings. In groups many problems have easy solutions due to the existence of inverses, e.g., the solvability of equations. Additional information provided by the presentations for different classes of groups is incorporated to give improved and terminating procedures to compute Gröbner bases for finitely generated right ideals.

Section 5.1: Similar to the equivalence of certain restricted versions of the word problem for semi-Thue systems to restricted versions of the ideal congruence problem for free monoid respectively group rings in section 3.2, we show that the subgroup problem is equivalent to a restricted version of the right ideal membership problem in a group ring. Thus only groups having solvable subgroup problem are candidates for allowing the computation of finite right Gröbner bases.

Section 5.2: The results on prefix reduction can be used to give a terminating procedure to compute finite reduced prefix Gröbner bases for finitely generated right ideals in free group rings.

Section 5.3: Similar ideas as in the case of free groups can be carried over to the class of plain groups and a procedure is provided to compute finite reduced prefix Gröbner bases for finitely generated right ideals.

Section 5.4: The results on free groups are combined with special presentations of context-free groups to give a procedure to compute finite reduced prefix Gröbner bases for finitely generated right ideals.

Section 5.5: The ideas of commutative reduction are generalized to the case of nilpotent groups resulting in the definition of quasi-commutative reduction. We give a terminating procedure to compute Gröbner bases for finitely generated right ideals in torsion-free nilpotent group rings and show how these ideas can be generalized for nilpotent group rings in a construction similar to context-free groups.

5.1 The Subgroup Problem

In section 3.2 we have shown that the word problem for group presentations is equivalent to a restricted version of the ideal membership problem for a free group ring. We will now show that a similar equivalence holds for the right ideal membership problem in group rings.

Definition 5.1.1
Given a subset S of a group $\mathcal{G}$ let $\langle S \rangle$ denote the subgroup generated by S. The **generalized word problem** or **subgroup problem** is then to determine, given an element $w \in \mathcal{G}$, whether $w \in \langle S \rangle$. $\diamond$

The word problem for a group $\mathcal{G}$ is just the generalized word problem for the trivial subgroup in $\mathcal{G}$. Thus the existence of a group with undecidable word problem yields undecidability for the subgroup problem. On the other hand, decidable word problem for a subgroup does not imply decidable generalized word problem.

The next theorem states that the subgroup problem for a group is equivalent to a special instance of the right membership problem in the corresponding group ring.

Theorem 5.1.2
Let S be a finite subset of $\mathcal{G}$ and $\mathbf{K}[\mathcal{G}]$ the group ring corresponding to $\mathcal{G}$. Further let $P_S = \{s - 1 \mid s \in S\}$ be a set of polynomials associated to S[1]. Then the following statements are equivalent:

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

Proof :
$1 \Longrightarrow 2$: Let $w = u_1 \circ \ldots \circ u_k \in \langle S \rangle$, i.e., $u_1, \ldots, u_k \in S \cup \{\mathsf{inv}(s) | s \in S\}$. We show $w - 1 \in \mathsf{ideal}_r(P_S)$ by induction on k. In the base case $k = 0$ there is nothing to show, as $w = \lambda \in \langle S \rangle$ and $0 \in \mathsf{ideal}_r(P_S)$. Hence, suppose $w = u_1 \circ \ldots \circ u_{k+1}$ and $u_1 \circ \ldots \circ u_k - 1 \in \mathsf{ideal}_r(P_S)$. Then $(u_1 \circ \ldots \circ u_k - 1) * u_{k+1} \in \mathsf{ideal}_r(P_S)$ and, since $u_{k+1} - 1 \in \mathsf{ideal}_r(P_S)$[2], we get $(u_1 \circ \ldots \circ u_k - 1) * u_{k+1} + (u_{k+1} - 1) = w - 1 \in \mathsf{ideal}_r(P_S)$.

$2 \Longrightarrow 1$: We have to show that $w - 1 \in \mathsf{ideal}_r(P_T)$ implies $w \in \langle S \rangle$. We know $w - 1 = \sum_{j=1}^{n} \alpha_j \cdot (u_j - 1) * x_j$, where $\alpha_j \in \mathbf{K}^*$, $u_j \in S \cup \{\mathsf{inv}(s) | s \in S\}$, $x_j \in \mathcal{G}$. Therefore, by showing the following stronger result we are done: A representation $w - 1 = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w'_j)$, $\alpha_j \in \mathbf{K}^*$,$w_j \neq w'_j$ and $w_j \circ \mathsf{inv}(w'_j) \in \langle S \rangle$ implies $w \in \langle S \rangle$. Now,

[1] Note that we use $1 = 1 \cdot \lambda = \lambda$.

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

let $w - 1 = \sum_{j=1}^{m} p_j$ be such a representation and $\succeq$ be an arbitrary total well-founded ordering on $\mathcal{G}$. Depending on this representation and $\succeq$ we define $t = \max\{w_j, w'_j \mid j = 1, \dots m\}$ and K is the number of polynomials p_j containing t as a term. We will show our claim by induction on (m, K), where $(m', K') < (m, K)$ if and only if $m' < m$ or ($m' = m$ and $K' < K$). In case $m = 0$, $w - 1 = 0$ implies $w = 1$ and hence $w \in \langle S \rangle$. Thus let us assume $m > 0$.
In case $K = 1$, let p_k be the polynomial containing t. As we either have $p_k = \alpha_k \cdot (t - w'_k)$ or $p_k = \alpha_k \cdot (w_k - t)$, where $\alpha_k \in \{1, -1\}$, without loss of generality we can assume $p_k = t - w'_k$. Using p_k we can decrease m by subtracting p_k from $w - 1$ giving us $w'_k - 1 = \sum_{j=1, j \neq k}^{m} p_j$. Since $t \circ \mathsf{inv}(w'_k) \in \langle S \rangle$ and our induction hypothesis yields $w'_k \in \langle S \rangle$, we can conclude $w = t = (t \circ \mathsf{inv}(w'_k)) \circ w'_k \in \langle S \rangle$.
In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w'_k)$ and $p_l = \alpha_l \cdot (t - w'_l)$. If then $w'_k = w'_l$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

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

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \neq w'_l$ and $w'_k \circ \mathsf{inv}(w'_l) \in \langle S \rangle$, since $w'_k \circ \mathsf{inv}(t), t \circ \mathsf{inv}(w'_l) \in \langle S \rangle$ and $w'_k \circ \mathsf{inv}(w'_l) = w'_k \circ \mathsf{inv}(t) \circ t \circ \mathsf{inv}(w'_l)$. In case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p'_k does not contain t, i.e., if m is not decreased K is.
q.e.d.

This theorem implies that we can only expect group rings over groups with solvable generalized word problem to allow solvable membership problem for right ideals. On the other hand, solvable subgroup problem only implies the solvability of a restricted version of the right ideal membership problem.

The usage of right ideals corresponds to the fact that the set $S \subseteq \mathcal{G}$ induces a left congruence, namely $u \sim_S v$ if and only if $\langle S \rangle\, u =_{\mathcal{G}} \langle S \rangle\, v$. Different methods to express this left congruence by reduction methods in order to solve the subgroup problem can be found in the literature. For free groups there is Nielsen's approach known as Nielsen reduction (compare [LySch77, AvMa84]). Kuhn and Madlener have developed prefix reduction methods and applied them successfully to the class of plain groups (see [KuMa89]). Wißmann solved the subgroup problem for the class of polycyclic groups (compare [Wi84, Wi89]) and Cremanns and Otto successfully treated the class of context-free groups (see [CrOt94]).

We move on now to study the right ideal membership problem in special classes of groups.

5.2 Free Groups

In group theory a particularly important role is played by groups that are free in the class of all groups which themselves are rather simple groups. In this section we state how the ideas of prefix reduction can be applied to give a completion algorithm for finitely generated free group rings.

Let $\mathcal{F}$ be a free group generated by a finite set $X = \{x_1, \ldots, x_n\}$. Then $\Sigma = X \cup X^{-1}$ and $T = \{xx^{-1} \longrightarrow \lambda, x^{-1}x \longrightarrow \lambda \mid x \in X\}$ is a presentation of $\mathcal{F}$ with $x_1^{-1} \succ x_1 \succ \ldots \succ x_n^{-1} \succ x_n$ inducing a length-lexicographical ordering on $\mathcal{F}$. Note that (Σ, T) then is a convergent 2-monadic monoid presentation of $\mathcal{F}$. We call x^{-1} the formal inverse of $x \in X$ and we will allow the following notations for such $x \in X$: $\mathsf{inv}(x) = x^{-1}$ and $\mathsf{inv}(x^{-1}) = x$. This can be extended to Σ^* by setting $\mathsf{inv}(\lambda) = \lambda$, $\mathsf{inv}(wx) = x^{-1}\mathsf{inv}(w)$ and $\mathsf{inv}(wx^{-1}) = x\mathsf{inv}(w)$ for $wx, wx^{-1} \in \Sigma^*$.

Let us start with some technical notions for polynomials in $\mathbf{K}[\mathcal{F}]$ which will allow an immediate characterization of saturating sets for polynomials. Note that the ideas used in the following definition for special instances can be compared to isolating prefixes as it is done in Nielsen's approach to solve the generalized word problem in free groups.

Definition 5.2.1
For a polynomial $p \in \mathbf{K}[\mathcal{F}]$ which has more than one monomial, we define

$$\begin{aligned}\sigma_1(p) &= \max\{u \in \mathcal{F} \mid \mathsf{inv}(u) \text{ is a suffix of } \mathsf{HT}(p) \text{ and } \mathsf{HT}(p * u) = \mathsf{HT}(p) \circ u\},\\ \sigma_2(p) &= \min\{u \in \mathcal{F} \mid \mathsf{inv}(u) \text{ is a suffix of } \mathsf{HT}(p) \text{ and } \mathsf{HT}(p * u) \neq \mathsf{HT}(p) \circ u\}.\end{aligned}$$

Then we can set $\mathsf{can}(p) = p * \sigma_1(p)$ and $\mathsf{acan}(p) = p * \sigma_2(p)$. For a polynomial $\alpha \cdot t \in \mathbf{K}[\mathcal{F}]$ we set $\sigma_1(p) = \sigma_2(p) = \mathsf{inv}(t)$ and $\mathsf{can}(p) = \mathsf{acan}(p) = \lambda$. $\diamond$

The polynomials $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ will often be called "mates" of each other. Note that $\sigma_1(p)$ is a prefix of $\sigma_2(p)$ and in case p contains more than one monomial we have $\sigma_2(p) \equiv \sigma_1(p)a$ where $a = \mathsf{inv}(\ell(\mathsf{HT}(p * \sigma_1(p))))$, i.e., a is the inverse of the last letter of the head term of the polynomial $\mathsf{can}(p)$. Hence $|\sigma_2(p)| = |\sigma_1(p)| + 1$ holds.

Example 5.2.2
Let $\Sigma = \{x, x^{-1}\}$ and $\mathcal{F}$ the free group generated by x.
Then for the polynomial $p = x^4 + x^2 + \lambda \in \mathbf{Q}[\mathcal{F}]$ we get $\sigma_1(p) = x^{-1}$, $\sigma_2(p) = x^{-2}$, $\mathsf{can}(p) = p * \sigma_1(p) = \underline{x^3} + x + x^{-1}$, and $\mathsf{acan}(p) = p * \sigma_2(p) = x^2 + \lambda + \underline{x^{-2}}$. $\diamond$

Notice that $\mathsf{HT}(p * \sigma_1(p))$ is a prefix of $\mathsf{HT}(p)$ and hence $p * \sigma_1(p) \leq p$. Furthermore, in case $p \neq \alpha \cdot t$, we get $p = \mathsf{can}(p) * \mathsf{inv}(\sigma_1(p)) = \mathsf{acan}(p) * \mathsf{inv}(\sigma_2(p))$ yielding $\mathsf{ideal}_r(p) = \mathsf{ideal}_r(\mathsf{can}(p)) = \mathsf{ideal}_r(\mathsf{acan}(p))$.

Next let us take a closer look at the special forms $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ of a polynomial p and their head terms respectively the last letters of their head terms. Let us associate a pair of terms (t_1^p, t_2^p) to p such that $t_1^p = \min\{\mathsf{HT}(\mathsf{can}(p)), \mathsf{HT}(\mathsf{acan}(p))\}$, $t_2^p = \max\{\mathsf{HT}(\mathsf{can}(p)), \mathsf{HT}(\mathsf{acan}(p))\}$ and set $q_i \in \{\mathsf{can}(p), \mathsf{acan}(p)\}$ such that $\mathsf{HT}(q_i) = t_i^p$. Then the following lemma holds.

Lemma 5.2.3
Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{F}]$ with more than one monomial, and (t_1^p, t_2^p), q_1, q_2 as described above. Then the following statements hold:

1. $|t_2^p| - |t_1^p| \leq 1$.
2. *For all terms $t' \in \mathsf{T}(q_2)$ with $|t'| = |t_2^p|$ we have $\ell(t') = \ell(t_2^p) = \mathsf{inv}(\ell(t_1^p))$.*
3. $q_1 * \mathsf{inv}(\ell(t_1^p)) = q_2$ *and* $q_2 * \mathsf{inv}(\ell(t_2^p)) = q_1$.

Proof :
Let $\mathsf{HT}(\mathsf{can}(p)) = \mathsf{HT}(p * \sigma_1(p)) = t$ and as $\sigma_2(p) \equiv \sigma_1(p)a$ for some $a \in \Sigma$ we get $\mathsf{HT}(\mathsf{acan}(p)) = \mathsf{HT}(p * \sigma_2(p)) = \mathsf{HT}(p * \sigma_1(p) * a) = s \circ a \succ t \circ a$ for some $s \in \mathsf{T}(\mathsf{can}(p))$. Then $s \prec t$ and $s \circ a \succ t \circ a$ implies $s \circ a \equiv sa$ and $|t \circ a| < |t|$. Hence either $|sa| = |t|$ or $|sa| = |t| + 1$, and hence, as $t_1^p, t_2^p \in \{sa, t\}$ we get $|t_2^p| - |t_1^p| \leq 1$.
To see that for all $t' \in \mathsf{T}(q_2)$ with $|t'| = |t_2^p|$ the last letters coincide with $\ell(t_2^p)$, let us take a closer look at the terms t_1^p and t_2^p respectively the terms in q_1 and q_2. We know $t_1^p \preceq t_2^p \equiv ub$ for some $u \in \mathcal{F}$, $b \in \Sigma$ and $t_2^p = v \circ c$ for some $v \in \mathsf{T}(q_1)$, $c \in \Sigma$, i.e., $v \preceq t_1^p$, but $ub \equiv v \circ c \succ t_1^p \circ c$. Hence for the last letter of t_1^p, $\ell(t_1^p) = \mathsf{inv}(c)$ must hold. On the other hand, $\ell(v) = \mathsf{inv}(c)$ is not possible, implying $ub \equiv vc$ and in particular $b = c$ and $u \in \mathsf{T}(q_1)$. It remains to study those terms $v' \in \mathsf{T}(q_1)$ with $|v' \circ b| = |t_2^p|$. In distinguishing the four possible cases we find that for the cases $|t_2^p| = |t_1^p| > |v'|$ and $|t_2^p| > |t_1^p| = |v'|$ we have $v' \circ b \equiv v'b$, and for the cases $|t_2^p| = |t_1^p| = |v'|$ and $|t_2^p| > |t_1^p| > |v'|$ either $|v' \circ b| = |t_2^p| + 1$ respectively $|v' \circ b| = |t_2^p| - 1$ or $|v' \circ b| \leq |t_2^p| - 1$ gives us a contradiction to $|v' \circ b| = |t_2^p|$.
Finally, since $\ell(t_1^p) = \mathsf{inv}(b)$ and $\ell(t_2^p) = b$, $q_1 \circ b = q_2$ and $q_2 * \mathsf{inv}(b) = q_1$ follows immediately. Furthermore, since $t_1^p, t_2^p \in \{sa, t\}$, this implies $b \in \{a, \mathsf{inv}(a)\}$.

q.e.d.

Corollary 5.2.4
Let p be a polynomial in $\mathbf{K}[\mathcal{F}]$ containing more than one monomial. Then neither $\mathsf{HT}(\mathsf{can}(p))$ nor $\mathsf{HT}(\mathsf{acan}(p))$ are prefixes of one another. In particular we get $\mathsf{can}(p) = \mathsf{acan}(p)$ if and only if $p = \alpha \cdot t$ for some $\alpha \in \mathbf{K}^*$, $t \in \mathcal{F}$.

Proof :
Let $\mathsf{HT}(\mathsf{can}(p)) \equiv ta$ for some $a \in \Sigma$ and by lemma 5.2.3 $\mathsf{HT}(\mathsf{acan}(p)) \equiv s\mathsf{inv}(a)$ for some $s \in \mathsf{T}(\mathsf{can}(p))$. Now suppose ta is a prefix of $s\mathsf{inv}(a)$. Then, as $||\mathsf{HT}(\mathsf{acan}(p))| - |\mathsf{HT}(\mathsf{can}(p))|| \leq 1$ and $a \neq \mathsf{inv}(a)$, we get $s \equiv ta$ contradicting the fact that $s \circ \mathsf{inv}(a) \equiv s\mathsf{inv}(a)$. Likewise, if $s\mathsf{inv}(a)$ were a prefix of ta we would get $t \equiv s\mathsf{inv}(a)$ contradicting that $ta \in \mathcal{F}$.
In particular $\mathsf{can}(p) = \mathsf{acan}(p)$ implies $\mathsf{HT}(\mathsf{can}(p)) = \mathsf{HT}(\mathsf{acan}(p))$, and this is only possible in case $p = \alpha \cdot t$ for some $\alpha \in \mathbf{K}^*$, $t \in \mathcal{F}$ and $\mathsf{can}(p) = \mathsf{acan}(p) = \lambda$.

q.e.d.

Lemma 5.2.5
Let p be a polynomial in $\mathbf{K}[\mathcal{F}]$ containing more than one monomial. Then the following statements hold:

1. $\mathsf{can}(\mathsf{can}(p)) = \mathsf{can}(p)$.
2. $\mathsf{acan}(\mathsf{can}(p)) = \mathsf{acan}(p)$.
3. $\mathsf{can}(\mathsf{acan}(p)) = \mathsf{acan}(p)$.
4. $\mathsf{acan}(\mathsf{acan}(p)) = \mathsf{can}(p)$.

Proof :
Note that $\sigma_1(\mathsf{can}(p)) = \lambda$ and $\sigma_2(\mathsf{can}(p)) = \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p)))) = \ell(\mathsf{HT}(\mathsf{acan}(p)))$. Therefore, we get $\mathsf{can}(\mathsf{can}(p)) = \mathsf{can}(p) * \sigma_1(\mathsf{can}(p)) = \mathsf{can}(p)$ and $\mathsf{acan}(\mathsf{can}(p) = \mathsf{can}(p) * \sigma_2(\mathsf{can}(p)) = \mathsf{acan}(p)$. On the other hand we find $\sigma_1(\mathsf{acan}(p)) = \lambda$ and $\sigma_2(\mathsf{acan}(p)) = \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{acan}(p)))) = \ell(\mathsf{HT}(\mathsf{can}(p)))$. Thus, $\mathsf{can}(\mathsf{acan}(p)) = \mathsf{acan}(p) * \sigma_1(\mathsf{acan}(p)) = \mathsf{acan}(p)$ and $\mathsf{acan}(\mathsf{acan}(p)) = \mathsf{acan}(p) * \sigma_2(\mathsf{acan}(p)) = \mathsf{can}(p)$.

q.e.d.

We can specify prefix saturating sets for polynomials in $\mathbf{K}[\mathcal{F}]$ in terms of the polynomials defined in definition 5.2.1.

Lemma 5.2.6
If a polynomial $p \in \mathbf{K}[\mathcal{F}]$ contains more than one monomial, the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ is a prefix saturating set for p. In particular, we find $\mathcal{SAT}_p(p) = \mathcal{SAT}_p(\mathsf{can}(p)) = \mathcal{SAT}_p(\mathsf{acan}(p))$.

Proof :
We can use procedure PREFIX SATURATED CHECK on page 4.4 to show that the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ is a prefix saturating set for a polynomial p. For the polynomials $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ we get the corresponding sets $C(\mathsf{HT}(\mathsf{can}(p))) = \{\mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p))))\}$ respectively $C(\mathsf{HT}(\mathsf{acan}(p))) = \{\mathsf{inv}(\ell(\mathsf{HT}(\mathsf{acan}(p))))\}$. Now by lemma 5.2.3 we know $\mathsf{can}(p) * \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{can}(p)))) = \mathsf{acan}(p)$ and $\mathsf{acan}(p) * \mathsf{inv}(\ell(\mathsf{HT}(\mathsf{acan}(p)))) = \mathsf{can}(p)$ and hence the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ is prefix saturated. Furthermore, as it is a subset of $\{p * w \mid w \in \mathcal{F}\}$ it is also a prefix saturating set for p.

q.e.d.

Remark 5.2.7
For a non-zero polynomial p in $\mathbf{K}[\mathcal{F}]$ the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ even is a prefix Gröbner basis of the right ideal generated by p. In case $p = \alpha \cdot t \in \mathbf{K}[\mathcal{F}]$ this is true as the set $\{\lambda\}$ is a prefix Gröbner basis for $\mathsf{ideal}_r(p) = \mathbf{K}[\mathcal{F}]$. If p contains more than one monomial, the head terms of the polynomials $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ are no prefixes of each other and this set is prefix saturated. As $\mathsf{ideal}_r(p) = \mathsf{ideal}_r(\mathsf{can}(p)) = \mathsf{ideal}_r(\mathsf{acan}(p))$, theorem 4.4.35 implies that $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ is a prefix Gröbner basis. $\diamond$

Now we can give a completion procedure for $\mathbf{K}[\mathcal{F}]$ by modifying procedure REDUCED PREFIX GRÖBNER BASES (see page 114) in specifying the saturating procedure for polynomials. It remains to show that finite reduced prefix Gröbner basis exist, as then this procedure will compute them. This will be done for the more general case of plain groups in the next section. In section 4.4 we mentioned that the sets S_i in procedure REDUCED PREFIX GRÖBNER BASES in general contain unnecessary polynomials. Therefore, we next provide a procedure using additional information to prevent this overhead. The idea is to use prefix reduction at head terms (this is comparable to the step of computing prefix s-polynomials) combined with saturating polynomials and to remove not only *one* polynomial from the set G_i for reduction, but also its corresponding "mate", i.e., we remove not only a polynomial q from G_i but the set $\{\mathsf{can}(q), \mathsf{acan}(q)\}$[3]. Hence the sets G_i contain at most $2 \cdot |F|$ polynomials. This algorithm can be compared to the results of Rosenmann's approach to free group rings in [Ro93]. The procedure will use the definitions of the special terms t_1^q and t_2^q introduced for polynomials q on page 158. Given two polynomials q, q' we define the following tuple ordering on the accompanying terms which is well-founded: $(t_1^q, t_2^q) \succ (t_1^{q'}, t_2^{q'})$ if and only if $t_1^q \succ t_1^{q'}$ or ($t_1^q = t_1^{q'}$ and $t_2^q \succ t_2^{q'}$).

Procedure: COMPLETION IN FREE GROUP RINGS

Given: A finite set $F \subseteq \mathbf{K}[\mathcal{F}]$.
Find: $\textsc{Gb}(F)$, a prefix Gröbner basis of F.

$i := 0$;
$G_0 := \{\mathsf{can}(f), \mathsf{acan}(f) \mid f \in F\}$;
% $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_0)$ and G_0 is prefix saturated
while there exists $q \in G_i$ such that $\mathsf{HT}(q)$ is prefix reducible by $g' \in G_i \backslash \{q\}$ with
  $(t_1^{g'}, t_2^{g'}) \preceq (t_1^q, t_2^q)$ **do**
  $i := i + 1$;
  $G_i := G_{i-1} \backslash \{\mathsf{can}(q), \mathsf{acan}(q)\}$;
  $G' := \{g \in G_i \mid (t_1^g, t_2^g) \preceq (t_1^q, t_2^q)\}$;
  $q' :=$ headnormalform$(q, \longrightarrow^{\mathrm{p}}_{G'})$;
  % Compute a normalform of a polynomial allowing only reduction steps at the
  % respective head terms
  if $|\mathsf{T}(q')| = 1$ % The right ideal generated by F is trivial
    then $G_i := \{\lambda\}$;
    else **if** $q' \neq 0$
        then $G_i := G_i \cup \{\mathsf{can}(q'), \mathsf{acan}(q')\}$;
          % $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_i)$ and G_i is prefix saturated
      endif
  endif
endwhile
$G := G_i$

---

[3] Note that by construction we will have $q \in \{\mathsf{can}(q), \mathsf{acan}(q)\}$.

Notice that we always have $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_i)$ and for the prefix reduced set $\tilde{G} = \{\text{normalform}(g, G\backslash\{g\}) \mid g \in G\}$ we again have $\mathsf{ideal}_r(G) = \mathsf{ideal}_r(\tilde{G})$. Furthermore, $\mathsf{HT}(G) = \mathsf{HT}(\tilde{G})$ holds since by construction no term in $\mathsf{HT}(G)$ is prefix of another term in $\mathsf{HT}(G)$. Thus $\tilde{G}$ is a reduced prefix Gröbner basis of $\mathsf{ideal}_r(G)$.

Theorem 5.2.8
Procedure COMPLETION IN FREE GROUP RINGS *is totally correct.*

Proof :
In case the procedure terminates, correctness follows at once from the fact that the final set G_k is a prefix Gröbner basis of $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_k)$, as it is prefix saturated by construction and no prefix s-polynomials exist. To see the latter, let us assume that although no polynomial $q \in G_k$ exists such that $\mathsf{HT}(q)$ is prefix reducible by a polynomial $g' \in G_k\backslash\{q\}$ with $(t_1^{g'}, t_2^{g'}) \preceq (t_1^q, t_2^q)$, there exist $g, g' \in G_k$ such that $\mathsf{HT}(g) \equiv \mathsf{HT}(g')u$ for some $u \in \mathcal{F}$. Then $(t_1^{g'}, t_2^{g'}) \succ (t_1^g, t_2^g)$, i.e., $t_1^{g'} \succ t_1^g$ or ($t_1^{g'} = t_1^g$ and $t_2^{g'} \succ t_2^g$), must hold. The case $u = \lambda$ is not possible as then the **while loop** would have to be executed using $q = g'$ contradicting our assumption. Now let us distinguish the possible cases. If $\mathsf{HT}(g) = t_1^g$ we get $t_1^g = \mathsf{HT}(g) \succ \mathsf{HT}(g') \succeq t_1^{g'}$ contradicting the fact that $t_1^{g'} \succeq t_1^g$ holds. It remains to look at the case $\mathsf{HT}(g) = t_2^g$. Now, if $|u| > 1$, this immediately implies $|t_1^g| \geq |t_2^g| - 1 > |\mathsf{HT}(g')|$ giving us $t_1^g \succ \mathsf{HT}(g') \succeq t_1^{g'}$ contradicting $t_1^{g'} \succeq t_1^g$. Hence we can assume $\mathsf{HT}(g) = t_2^g \equiv \mathsf{HT}(g')a$ for some $a \in \Sigma$. By lemma 5.2.3 we know $\mathsf{HT}(g * \mathsf{inv}(a)) = t_1^g \succ t_2^g * \mathsf{inv}(a) = \mathsf{HT}(g')$ and again $t_1^g \succ \mathsf{HT}(g') \succeq t_1^{g'}$ contradicts the assumption that $t_1^{g'} \succeq t_1^g$.
It remains to show that the procedure does indeed terminate. This is not trivial, as we either remove a pair of polynomials or replace a pair of polynomials by another pair of polynomials. We will use the technique of multisets. Let $C_i = \{\{(t_1^g, t_2^g) | g \in G_i\}\}$ be a multiset of pairs of terms and set $C_i = \{\{(\lambda, \lambda)\}\}$ in case $G_i = \{\lambda\}$. We will show that for all computed sets G_i we have $C_{i+1} \ll C_i$ according to the well-founded tuple-ordering $(t_1^g, t_2^g) \succ (t_1^{g'}, t_2^{g'})$ if and only if $t_1^g \succ t_1^{g'}$ or ($t_1^g = t_1^{g'}$ and $t_2^g \succ t_2^{g'}$)[4]. In case $G_{i+1} = \{\lambda\}$ or the respective polynomial q in the algorithm prefix reduces to zero we are done. Hence it remains to show that in case $p_1 \longrightarrow_g^{\mathrm{p}} p_2 = p_1 - \alpha \cdot g * w \neq 0$ at $\mathsf{HT}(p_1)$ and for some polynomial q we have $(t_1^g, t_2^g) \preceq (t_1^q, t_1^q)$, $(t_1^{p_1}, t_2^{p_1}) \preceq (t_1^q, t_2^q)$ then this implies $(t_1^{p_2}, t_2^{p_2}) \prec (t_1^q, t_2^q)$. For the polynomial q chosen by our procedure and $q' =$ headnormalform$(q, \longrightarrow_{G'}^{\mathrm{p}})$ this then implies $(t_1^q, t_2^q) \succ (t_1^{q'}, t_2^{q'})$. We show our claim by distinguishing the possible cases. In case $\mathsf{HT}(p_1) = t_1^{p_1}$ we find $\mathsf{HT}(p_1) \succ \mathsf{HT}(p_2) \succeq t_1^{p_2}$ immediately implies $t_1^{p_1} \succ t_1^{p_2}$. Hence let us assume $\mathsf{HT}(p_1) = t_2^{p_1} \equiv ta$ for some $t \in \mathcal{F}$, $a \in \Sigma$. Then by lemma 5.2.3 for all $s \in \mathsf{T}(p_1)$ with $|s| = |t_2^{p_1}|$ we have $\ell(s) = a$. Let us take a closer look at $p_2 = p_1 - \alpha \cdot g * w$.
In case $w = \lambda$ we get $\mathsf{HT}(p_1) = \mathsf{HT}(g)$. Then if $t_1^g = \mathsf{HT}(g)$, since $t_1^g \preceq t_1^q$ we get $t_1^q \succeq t_1^g = \mathsf{HT}(g) = t_2^{p_1} = \mathsf{HT}(p_1) \succ \mathsf{HT}(p_2) \succeq t_1^{p_2}$. Hence it remains to look at

[4] This induces a well-founded multiset ordering.

$\mathsf{HT}(g) = t_2^g$ and since $w = \lambda$ we know $t_2^g \equiv ta \equiv t_1^{p_1}$ and this implies that as for all $s \in \mathsf{T}(p_1)$, for all $s' \in \mathsf{T}(g)$ with $|s'| = |t_2^g|$ we have $\ell(s') = a$. Furthermore, for all $s \in \mathsf{T}(p_1)$ and for all $s' \in \mathsf{T}(g)$ we have $s \circ \mathsf{inv}(a) \preceq t_1^{p_1} \preceq t_1^q$ and $s' \circ \mathsf{inv}(a) \preceq t_1^g \preceq t_1^q$. Thus we have $t_1^{p_2} \preceq \mathsf{HT}(p_2 * \mathsf{inv}(a)) \preceq t_1^q$ and in case $\mathsf{HT}(p_2 * \mathsf{inv}(a)) = t_1^{p_2} = t_1^q$ we find that either $t_1^{p_1} = t_1^q$ or $t_1^g = t_1^q$ and hence $t_2^{p_2} \preceq \mathsf{HT}(p_2) \prec \mathsf{HT}(p_1) = t_2^{p_1} = t_2^g \preceq t_2^q$.
In case $w \equiv ua$ for all $s \in \mathsf{T}(\mathsf{RED}(g * u))$ we have $s \prec \mathsf{HT}(g)u \equiv t \prec \mathsf{HT}(p_1 * \mathsf{inv}(a)) = t_1^{p_1} \preceq t_1^q$. Thus we get $t_1^{p_2} \preceq \mathsf{HT}(p_2 * \mathsf{inv}(a)) = \mathsf{HT}(p_1 * \mathsf{inv}(a) - \alpha \cdot g * u) = t_1^{p_1} \preceq t_1^q$ and in case $t_1^{p_2} = t_1^{p_1} = t_1^q$ we know, $t_1^{p_2} = \mathsf{HT}(p_2 * \mathsf{inv}(a))$, i.e., $t_2^{p_2} \preceq \mathsf{HT}(p_2) \prec \mathsf{HT}(p_1) = t_2^{p_1} \preceq t_2^q$.

q.e.d.

We will end this section by showing how a special case of our approach can be compared to the Nielsen method to solve the subgroup problem in free groups.

Let us start by giving a short description of this method, which can e.g. be found in [LySch77]. Let $\mathcal{F}$ be a free group with basis X. We call a word $w \equiv w_1 \ldots w_k$, $w_i \in \mathcal{F}$, **reduced**, in case $w = w_1 \circ \ldots \circ w_k$, i.e., $|w| = \sum_{i=1}^k |w_i|$. Subsets of $\mathcal{F}$ are written as $U = \{u_i \mid i \in \mathbf{N}\}$ or $U = \{u_1, \ldots, u_n\}$ depending on whether they are finite or not. Then we can define **elementary Nielsen transformations** on a set U as follows:

(T1) Replace some $u_i \in U$ by $\mathsf{inv}(u_i)$.

(T2) Replace some $u_i \in U$ by $u_i \circ u_j$ where $j \neq i$.

(T3) Delete some $u_i \in U$ where $u_i = \lambda$.

In all three cases it is understood that the u_l remain unchanged for $l \neq i$. A product of such elementary transformations is called a **Nielsen transformation**.

Lemma 5.2.9
If a subset U of $\mathcal{F}$ is carried into a set U' by a Nielsen transformation, then U and U' generate the same subgroup. □

We call a set U **Nielsen reduced**, if for all $v_1, v_2, v_3 \in U \cup \{\mathsf{inv}(u_i) | u_i \in U\}$ the following conditions hold:

(N0) $v_1 \neq \lambda$;

(N1) $v_1 \circ v_2 \neq \lambda$ implies $|v_1 \circ v_2| \geq \max\{|v_1|, |v_2|\}$;

(N2) $v_1 \circ v_2 \neq \lambda$ and $v_2 \circ v_3 \neq \lambda$ imply $|v_1 \circ v_2 \circ v_3| > |v_1| - |v_2| + |v_3|$.

Nielsen reduced sets play an important role, as they are free generating systems for the subgroup they generate. The following theorem due to Ziechang states that freely reducing a product of elements of a Nielsen reduced set cannot result in arbitrary cancellations on the elements involved.

Theorem 5.2.10
Let U be a Nielsen reduced set. Then for every $u \in U \cup \{\mathsf{inv}(u) \mid u \in U\}$ there are words $a(u)$ and $m(u)$ with $m(u) \neq \lambda$ such that $u \equiv a(u)m(u)\mathsf{inv}(a(\mathsf{inv}(u)))$ and if $w = u_1 \circ \ldots \circ u_n$ for some $u_i \in U \cup \{\mathsf{inv}(u) \mid u \in U\}$, $u_i \circ u_{i+1} \neq \lambda$, then the words $m(u_i)$ remain uncancelled in the reduced form of w. In particular we get $|w| \geq n$. □

This property can be used to solve the subgroup problem for Nielsen reduced sets by computing appropriate right coset representations. Therefore, it remains to find Nielsen reduced sets. The following theorem gives an effective way to transform an arbitrary finite set U into a Nielsen reduced set. To see how the necessary Nielsen transformation can be constructed we include a proof.

Theorem 5.2.11
Let $U \subseteq \mathcal{F}$ be a finite set. Then there is a Nielsen transformation from U into some Nielsen reduced set V.

Proof :
Let U be a finite subset of $\mathcal{F}$. We will show how U can be carried over into a Nielsen reduced set by using elementary Nielsen transformations.
Condition (N0) can be achieved using finitely many transformation steps (T3), and hence we can assume that U satisfies (N0).
Now suppose that U does not fulfill (N1). Then without loss of generality we can assume that there are u_i, u_j such that $|u_i \circ u_j| < |u_i|$. Then $j \neq i$, as $|u^2| < |u|$ is not possible for $u \in \mathcal{F}$. Using transformation (T2) we can replace u_i by $u_i \circ u_j$ and for the new set U' we have $\sum_{u \in U'} |u| < \sum_{u \in U} |u|$. Hence, we can assume that U can be transformed using (T2) into a set U' with $\sum_{u \in U'} |u|$ minimal, i.e., no further applications of (T2) are possible and hence condition (N1) must hold. Since (T2) does not affect condition (N0) we can now assume that U satisfies (N0) and (N1).
Finally let us transform U into a set additionally fulfilling (N2). To see how this can be done let us consider a triple x, y, z such that $x \circ y \neq \lambda$ and $y \circ z \neq \lambda$. As U satisfies (N1) we know $|x \circ y| \geq |x|$ and $|y \circ z| \geq |z|$, i.e., the part of y which cancels in $x \circ y$ is no more than half of y, and likewise the part that cancels in $y \circ z$. Now let $x \equiv w_1 w_2$, $y \equiv \mathsf{inv}(w_2) w_3 w_4$, $z \equiv \mathsf{inv}(w_4) w_5$ such that $x \circ y \equiv w_1 w_3 \mathsf{inv}(w_4)$ and $y \circ z \equiv w_2 w_3 w_5$. In case $w_3 \neq \lambda$ we find $x \circ y \circ z \equiv w_1 w_3 w_5$ and hence $|x \circ y \circ z| = |x| - |y| + |z| + |w_3| > |x| - |y| + |z|$ and thus (N2) holds for this triple. Otherwise, we get $y \equiv w_2 \mathsf{inv}(w_4)$ and (N2) is violated. Note that, as U satisfies (N1), we have $|w_2| = |w_4| = \frac{1}{2}|y| \leq \min\{\frac{1}{2}|x|, \frac{1}{2}|z|\}$ and $w_2 \neq w_4$. We could now use transformation (T2) and either replace $\mathsf{inv}(x)$ by $\mathsf{inv}(x \circ y)$ or z by $y \circ z$ without changing the sum of the lengths of the elements in U. To decide which replacement should take place, we use the following technique:
Suppose there is a precedence on the letters $X \cup X^{-1}$ inducing a length-lexicographical ordering on the reduced words presenting the elements of $\mathcal{F}$. We define the left half of a reduced word w to be the initial segment $L(w)$ of length $[\frac{|w|+1}{2}]$. This can be used

to define a well-founded ordering on reduced words as follows: For two reduced words w_1, w_2 we set $w_1 \prec w_2$ if and only if $\min\{L(w_1), L(\mathsf{inv}(w_1))\} < \min\{L(w_2), L(\mathsf{inv}(w_2))\}$ or $(\min\{L(w_1), L(\mathsf{inv}(w_1))\} = \min\{L(w_2), L(\mathsf{inv}(w_2))\}$ and $\max\{L(w_1), L(\mathsf{inv}(w_1))\} < \max\{L(w_2), L(\mathsf{inv}(w_2))\})$. Now suppose $x \equiv w_1\mathsf{inv}(w_2)$, $y \equiv w_2\mathsf{inv}(w_4)$ and $z \equiv w_4w_5$ as above. If $w_2 \prec w_4$ then $y \circ z \equiv w_2w_5 \prec z \equiv w_4w_5$ and if $w_4 \prec w_2$ then $x \circ y \equiv w_1\mathsf{inv}(w_4) \prec x \equiv w_1\mathsf{inv}(w_2)$. We can now suppose that the set U is transformed using (T2) according to the relation $\prec$ as far as possible. Since this terminates and does not affect condition (N0) nor condition (N1) we are done.

q.e.d.

There are well-known algorithms for performing this task and Avenhaus and Madlener have provided one which works in polynomial time (see [AvMa84]). We will now proceed to show how Nielsen's method is related to solving the generalized word problem in free groups using Gröbner bases. Applying theorem 5.1.2 we find that the subgroup problem related to a finite set $U \subseteq \mathcal{F}$ can be transformed into the membership problem for the right ideal generated by the set of polynomials $P_U = \{u - 1 \mid u \in U\}$. The following lemma states that special prefix Gröbner bases of P_U exist.

Lemma 5.2.12
For a finite subset U of $\mathcal{F}$ let G be the reduced prefix Gröbner basis computed by procedure Completion in Free Group Rings *on input $P_U = \{u - 1 \mid u \in U\}$ assuming a length lexicographical ordering on $\mathcal{F}$ assuming that all polynomials are made monic. Then the following conditions hold:*

1. *No head term of a polynomial in G is a prefix of a head term of another polynomial in G.*

2. *For all $g \in G$ we have $g = u - v$ for some $u, v \in \mathcal{F}$.*

3. *For $u - v \in G$ we have $u \circ \mathsf{inv}(v) \equiv u\mathsf{inv}(v)$, in particular $\ell(u) \neq \mathsf{inv}(\ell(v))$.*

4. *For $u - v \in G$ we have $|u| - |v| \leq 2$.*

5. *If $u - v \in G$ so is its 'mate' $(-1) \cdot (u - v) * \mathsf{inv}(\ell(u))$.*

Proof :

1. This follows immediately from theorem 5.2.8.

2. The only possibilities of changing polynomials are the saturation process and the normal form computation. By definition 5.2.1, for $p = u - v$ the polynomials $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ are also of this form in case they are made monic. Let us hence take a closer look at prefix reducing $p = u - v$ by a polynomial $u' - v'$ at u. Then $u \equiv u'z$ for some $z \in \mathcal{F}$ and the result is $u - v - (u' - v') * z = -v + v' \circ z$ and again the monic version of this polynomial has the desired form.

3. This follows immediately from the fact that all polynomials in G are either in can or acan form.

4. The case $|u| - |v| > 2$ would contradict the previous statement.

5. To see this let us assume $(-1) \cdot (u - v) * \mathsf{inv}(\ell(u)) \notin G$ and set $a = \mathsf{inv}(\ell(u))$. Remember that $u - v$ is either in its can or acan form and hence $v \circ a \equiv va$. Since we assume $va - u \circ a \notin G$, then va must be prefix reducible by a polynomial $g \in G$. As $u - v \in G$, v is not prefix reducible using G, hence $\mathsf{HT}(g) \equiv va$, say $g = va - z$ for some $z \in \mathcal{F}$ and $z \neq u \circ a$. But then we have $(u - v) * a, va - z \in \mathsf{ideal}_r(G)$, implying $(u - v) * a - (va - z) = -u \circ a + z \in \mathsf{ideal}_r(G)$. Thus either z or $u \circ a$, which is a prefix of u, must be prefix reducible using G contradicting that $u - v$ and $va - z$ are supposed to belong to G and hence must be prefix reduced.

q.e.d.

Theorem 5.2.13
Let U be a finite subset of $\mathcal{F}$ and G the monic reduced prefix Gröbner of the right ideal generated by $\{u - 1 \mid u \in U\}$ in $\mathbf{K}[\mathcal{F}]$. Then the set $X_G = \{u\mathsf{inv}(v) \mid u - v \in G\}$ is Nielsen reduced for U.

Proof :
We have to show that the set X_G satisfies the conditions (N0), (N1) and (N2).
(N0) is valid, since $u\mathsf{inv}(v) \equiv \lambda$ would imply $u = v = \lambda$, but we assume that 0 is not contained in G.
To show that (N1) is true, we prove that for two polynomials $u - v, u' - v' \in G$, $u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \neq \lambda$ implies $|u\mathsf{inv}(v) \circ u'\mathsf{inv}(v')| \geq \max\{|u\mathsf{inv}(v)|, |u'\mathsf{inv}(v')|\}$. Let us assume $u\mathsf{inv}(v) \equiv w_1 w_2$ and $u'\mathsf{inv}(v') \equiv \mathsf{inv}(w_2) w_3$ such that $u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \equiv w_1 w_3$ and $w_1 w_3 \not\equiv \lambda$. Since $u - v \in G$ we know that its mate $(-1) \cdot (u - v) * a$ belongs to G, where $a = \mathsf{inv}(\ell(u))$, and this polynomial has head term va. Let us first assume that $\mathsf{inv}(va)$ is a suffix of w_2, i.e., va is a prefix of $\mathsf{inv}(w_2)$. Then, in case u' is a prefix of $\mathsf{inv}(w_2)$, this would imply that one of the terms va or u' is prefix of the other which would contradict the fact that G is a reduced prefix Gröbner basis unless we have $u' \equiv va$. But then, as G contains the mate of $u - v$, this mate must be $u' - v'$ contradicting the fact that we require $u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \neq \lambda$. Assuming that $\mathsf{inv}(w_2)$ is a prefix of u' would immediately give a contradiction as va then would be a prefix of u' implying that $u' - v'$ is prefix reducible by the mate of $u - v$. Hence let us assume that w_2 is a suffix of $\mathsf{inv}(v)$, i.e., $\mathsf{inv}(w_2)$ is a proper prefix of va. Then, as $|\mathsf{inv}(w_2)| < |va|$ and $|va| \leq [\frac{|u\mathsf{inv}(v)|}{2} + 1]$ as $|u| - |v| \leq 1$. Thus at most half of $u\mathsf{inv}(v)$ is cancelled by multiplication with w_2 and $|w_1| \geq |u|$. Now in case $\mathsf{inv}(w_2)$ is also a proper prefix of u' this implies $|w_2| < |u'|$ and $|w_3| > |v'|$. Hence, as $|u| - |v| \leq 1$ and $|u'| - |v'| \leq 1$ this implies $|w_2| \leq |w_1|$ and $|w_2| < |w_3|$, i.e. $|w_1 w_3| = |w_1| + |w_3| > |w_1| + |w_2| = |w_1 w_2| = |u\mathsf{inv}(v)|$ and $|w_1| + |w_3| \geq |w_2| + |w_3| = |\mathsf{inv}(w_2) w_3| = |u'\mathsf{inv}(v')|$ and hence

$|u\mathsf{inv}(v) \circ u'\mathsf{inv}(v')| \geq \max\{|u\mathsf{inv}(v)|, |u'\mathsf{inv}(v')|\}$. Note that u' cannot be a prefix of $\mathsf{inv}(w_2)$ as then va would be prefix reducible using u' contradicting that the mate of $u - v$ belongs to G.

To show that (N2) holds, we prove that for three polynomials $u - v, u' - v', u'' - v'' \in G$, $u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \neq \lambda$ and $u'\mathsf{inv}(v') \circ u''\mathsf{inv}(v'') \neq \lambda$ imply that the equation $|u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \circ u''\mathsf{inv}(v'')| > |u\mathsf{inv}(v)| - |u'\mathsf{inv}(v')| + |u''\mathsf{inv}(v'')|$ holds. Let us assume $u\mathsf{inv}(v) \equiv w_1w_2$, $u'\mathsf{inv}(v') \equiv \mathsf{inv}(w_2)w_3w_4$ and $u''\mathsf{inv}(v'') \equiv \mathsf{inv}(w_4)w_5$ such that $u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \equiv w_1w_3w_4$ and $u'\mathsf{inv}(v') \circ u''\mathsf{inv}(v'') \equiv \mathsf{inv}(w_2)w_3w_5$. Then, as $|u\mathsf{inv}(v) \circ u'\mathsf{inv}(v') \circ u''\mathsf{inv}(v'')| = |w_1w_3w_5| = |w_1w_2| - |\mathsf{inv}(w_2)w_3w_4| + |\mathsf{inv}(w_4)w_5| + |w_3| \geq |u\mathsf{inv}(v)| - |u'\mathsf{inv}(v')| + |u''\mathsf{inv}(v'')|$, in case $w_3 \neq \lambda$ we are done. Hence let us assume $w_3 = \lambda$. Then, as (N1) holds, we get $|u\mathsf{inv}(v) \circ u'\mathsf{inv}(v')| \geq \max\{|u\mathsf{inv}(v)|, u'\mathsf{inv}(v')|\}$ and $|u'\mathsf{inv}(v') \circ u''\mathsf{inv}(v'')| \geq \max\{|u'\mathsf{inv}(v')|, u''\mathsf{inv}(v'')|\}$ implying that $|w_2| = |w_4| = \frac{1}{2}|u'\mathsf{inv}(v')|$ and $w_2 \neq w_4$[5]. Thus, $u' \equiv \mathsf{inv}(w_2)$ and $v' \equiv \mathsf{inv}(w_4)$ since $|u'| - |v'| \leq 1$. This would imply that either v is prefix reducible, in case $\mathsf{inv}(w_2)$ is a prefix of v contradicting that $u - v \in G$, or u' is prefix reducible by the mate of $u - v$ contradicting that $u' - v' \in G$. Therefore, $w_3 = \lambda$ is not possible and we are done.

q.e.d.

In particular the steps performed in procedure REDUCED PREFIX GRÖBNER BASES modified for free group rings or in procedure COMPLETION IN FREE GROUP RINGS can be compared to Nielsen transformations on a set X corresponding to the actual sets of polynomials, namely in the first case $X = \{u \circ \mathsf{inv}(v) \mid u - v \in S_i \cup G_i\}$ and in the second case $X = \{u \circ \mathsf{inv}(v) \mid u - v \in G_i\}$. Both algorithms in changing the actual polynomials mainly involve saturation and prefix reduction. We close this section in sketching how these two operations are related to Nielsen transformations. Let us start with investigating the polynomials $\mathsf{can}(u-1)$ and $\mathsf{acan}(u-1)$ as saturating an arbitrary polynomial of the form $u - v$ can be reduced to saturating the polynomial $u \circ \mathsf{inv}(v) - 1$. We claim that replacing a polynomial $u - 1$ by $\mathsf{can}(u-1)$ and $\mathsf{acan}(u-1)$ corresponds to a Nielsen transformation involving the rules (T1) and (T1') on the respective set X involving the element $u \in X$. To see this let $L(u)$ be the initial segment of length $[\frac{|u|+1}{2}]$ of a reduced word u and $R(u)$ the remaining segment, then the candidates for $\mathsf{can}(u-1)$ and $\mathsf{acan}(u-1)$ belong to the set $\{L(u) - \mathsf{inv}(R(u)), (L(u) - \mathsf{inv}(R(u))) * \mathsf{inv}(\ell(L(u))), (L(u) - \mathsf{inv}(R(u))) * \mathsf{inv}(\ell(R(u)))\}$, i.e., the accompanying elements are of the form $L(u)R(u) \equiv u$ and $\mathsf{inv}(R(u))\mathsf{inv}(L(u)) \equiv \mathsf{inv}(u)$ and hence we can use the rules (T1) and (T1') to do the appropriate changes on the set X. It remains to show how prefix reduction steps in this context are related to Nielsen transformations. We show that a single reduction step corresponds to an application of a rule (T2). Let us assume $u - v \longrightarrow^{\mathrm{p}}_{u'-v'} v' \circ z - v$ and $u \equiv u'z$ for some $z \in \mathcal{F}$[6]. In case $v' \circ z > v$ we have to show that $v' \circ z \circ \mathsf{inv}(v)$ can be achieved from elements in X by a Nielsen transformation. As $u - v, u' - v'$ must belong to the actual set of polynomials we know

[5]We have $u'\mathsf{inv}(v') \neq \lambda$ since (N0) holds.

[6]The case $v \equiv u'z$ can be treated similarly.

$u \circ \mathsf{inv}(v), u' \circ \mathsf{inv}(v') \in X$. Hence, we can assume $\mathsf{inv}(u' \circ \mathsf{inv}(v')) \in X$[7]. Since we have $\mathsf{inv}(u' \circ \mathsf{inv}(v')) \circ (u \circ \mathsf{inv}(v)) = (v' \circ \mathsf{inv}(u')) \circ (u' \circ z \circ \mathsf{inv}(v)) = v' \circ z \circ \mathsf{inv}(v)$, we may replace $u \circ \mathsf{inv}(v)$ by $v' \circ z \circ \mathsf{inv}(v)$ using transformation (T2).

5.3 Plain Groups

A plain group is a free product of finite groups and a free group, and in [AvMaOt86]] it has been shown that these groups allow finite 2-monadic, convergent (even reduced) group presentations. Using these presentations and the syntactical information they provide we can show that a slight modification of procedure Prefix Gröbner Bases (see page 110) terminates.

Theorem 5.3.1
Given a 2-monadic confluent group presentation for a plain group $\mathcal{G}$ and a finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$, the procedure Prefix Gröbner Bases *terminates.*

Proof :
Note that if (Σ, T) is a convergent interreduced presentation of a cancellative monoid $\mathcal{M}$, then no rules of the form $wa \longrightarrow a$ or $aw \longrightarrow a$ appear in T for $a \in \Sigma$. This is of course always true if such presentations are given for groups.
Let us assume that procedure **normalform** computes a normalform of a polynomial allowing only prefix reduction steps at the respective head terms. Then the proof is done in two steps: first we show that all polynomials computed have a certain property that will be used in the second step to ensure termination. We say a polynomial q has property $\mathcal{P}_F$ if and only if

(α) $|\mathsf{HT}(q)| \leq K$, where $K = \max\{|\mathsf{HT}(f)| \mid f \in F\} + 1$.

(β) If $|\mathsf{HT}(q)| = K$ then there exists an element $a \in \Sigma$ such that

  (i) all terms of length K in q have a as a common suffix, and

  (ii) for all $s \in \mathsf{T}(q)$ with $|s| = K - 1$ we either have $s \equiv s_1 a$ or in case $s \equiv s_1 d$, $d \in \Sigma \backslash \{a\}$ there is a rule $ea \longrightarrow d \in T, e \in \Sigma$.

We will show that all polynomials q computed by the procedure on input F have property $\mathcal{P}_F$.
By the choice of K all input polynomials have $\mathcal{P}_F$. Hence, let G be the actual set of polynomials having $\mathcal{P}_F$, and let q be the next polynomial computed by our procedure. In case q is due to computing the normal form of a polynomial p having $\mathcal{P}_F$ using prefix reduction at head terms only the property is preserved. To see this we can restrict ourselves to a single step reduction. In case $|\mathsf{HT}(p)| < K$ we are done. Therefore, suppose

[7] This can always be achieved by an application of either (T1) or (T1').

$|\mathsf{HT}(p)| = K$ and $\mathsf{HM}(p)$ is reduced in the reduction step $p \longrightarrow^{\mathrm{p}}_{g \in G} q'$. We have to show that q' satisfies $\mathcal{P}_F$. Let $\mathsf{HT}(p) \equiv \mathsf{HT}(g)w$ and $q' = p - \alpha \cdot g * w$, $\alpha \in \mathbf{K}^*$, $w \in \mathcal{M}$. Now $g * w$ has $\mathcal{P}_F$ as $\mathsf{HT}(g * w) \equiv \mathsf{HT}(g)w$ and for all $s \in \mathsf{T}(\mathsf{RED}(g))$ we either have $|s \circ w| < |sw|$ or sw and $\mathsf{HT}(g)w$ have the same last letter. Since $\mathsf{T}(q') \subseteq \mathsf{T}(p) \cup \mathsf{T}(g*w)$, q' then likewise has $\mathcal{P}_F$. In case q is due to saturating a polynomial as specified e.g. in procedure PREFIX SATURATION on page 102 and results from a polynomial q' having $\mathcal{P}_F$ being overlapped with a rule $ab \longrightarrow c \in T$, $c \in \Sigma \cup \{\lambda\}$[8], we can also show that $\mathcal{P}_F$ is preserved. Note that only the case $|\mathsf{HT}(q)| = K$ is critical. In case $|\mathsf{HT}(q')| < K$ and $|\mathsf{HT}(q)| = K$ we know $\mathsf{HT}(q) \equiv tb$ and for all $s \in \mathsf{T}(q')$ with $|s \circ b| = K - 1$ either $s \circ b \equiv sb \in \mathrm{IRR}(T)$ or $s \equiv s_1 e$ and $s \circ b = s_1 e \circ b \equiv s_1 d$, where $eb \longrightarrow d \in T$. Note that these are the only possibilities to gain a term of length $K - 1$ from a term of length less or equal to $K - 1$ by multiplication with a letter b. On the other hand, if $|\mathsf{HT}(q')| = K$ with $\mathsf{HT}(q') \equiv ta$ we can only violate $\mathcal{P}_F$ in case we have $t_1, t_2 \in \mathsf{T}(q')$ such that $|t_1| = K, |t_2| = K - 1, t_1 \equiv t_1' a$ and $t_1 \circ b \equiv t_1' c, t_2 \circ b \equiv t_2 b$ with $c \neq \lambda$. Therefore, we examine all $s \in \mathsf{T}(q')$ with $|s| = K - 1$. If there are none q must have $\mathcal{P}_F$, since then a term $s \in \mathsf{T}(q')$ can only reach length $K - 1$ by multiplication with b in case $|s| = K - 2$ and $sb \in \mathrm{IRR}(T)$. Since $ab \longrightarrow c \in T$ and $\mathcal{G}$ is a group including inverses of length 1 for the generators, a has an inverse $\tilde{a}$ and $b \overset{*}{\longleftrightarrow}_T \underline{\tilde{a}a}b \equiv \tilde{a}\underline{ab} \overset{*}{\longleftrightarrow}_T \tilde{a}c$ gives us the existence of a rule $\tilde{a}c \longrightarrow b \in T$ as T is confluent[9]. Now let $s \in \mathsf{T}(q')$ have length $K - 1$. Then if $s \equiv s_1 a$ there is nothing to show[10]. On the other hand, in case $s \equiv s_1 d, d \neq a$ we know that there is a rule $ea \longrightarrow d \in T$ as q' has $\mathcal{P}_F$. Then we have $db \longleftarrow \underline{ea}b \equiv e\underline{ab} \longrightarrow ec$ and, since $ea \longrightarrow d \in T$ gives us $e \neq d$, there are rules $db \longrightarrow g, ec \longrightarrow g \in T, g \in \Sigma \cup \{\lambda\}$. Finally let us assume that q is due to s-polynomial computation. But computing s-polynomials can be compared to a single prefix reduction step on the head monomial of a polynomial and we have seen that prefix reduction preserves property $\mathcal{P}_F$.

It remains to show that the procedure does terminate. Thus let us assume the contrary. Then there are infinitely many polynomials $q_i, i \in \mathbf{N}$ resulting from s-polynomial computations added to G. Note that every such polynomial is in prefix normal from with respect to all polynomials in G so far. On the other hand, as $|\mathsf{HT}(q_i)| \leq K$, this would mean that there is a term t, which occurs infinitely often as a head term among these polynomials q_i contradicting the fact that the head terms of all added polynomials are in prefix normal form with respect to the polynomials added to the Gröbner set so far, and hence no head term can appear twice among the head terms of the polynomials ever added to the set G.

q.e.d.

[8]The polynomial q' here is said to overlap with the rule $ab \longrightarrow c \in T$ in case $\ell(\mathsf{HT}(q')) = a$.

[9]This is no longer true in case a has an inverse u_a of length $|u_a| > 1$ or no inverse at all.

[10]Then $s \circ b = s_1 a \circ b = s_1 \circ c$ and either $|s \circ b| < K - 1$ or $s \circ b \equiv s_1 c$.

An immediate consequence of this theorem is the existence of finite Gröbner bases for finitely generated right ideals in free and plain group rings.

Following the approach sketched for free group rings in the previous section, we can give a more efficient prefix saturating procedure for plain group rings. We will use the following observation from Kuhn in [Ku91].

Lemma 5.3.2
Let (Σ, T) be a 2-monadic, convergent, reduced group presentation of a plain group $\mathcal{G}$. Then for $w \in \mathcal{G}$ and $b \in \Sigma$ we have

$$w \circ b \equiv \begin{cases} wb & wb \text{ is irreducible} \\ w'c & w \equiv w'a, (ab, c) \in T, \end{cases}$$

in particular, $|w| - 1 \leq |w \circ b| \leq |w| + 1$.

Proof :
In case $w \circ b \equiv wb$ we immediately get $|w \circ b| = |w| + 1$. On the other hand, if $w \equiv w'a$ and $w \circ b \equiv w'c$ in case $c \in \Sigma$ we have $|w \circ b| = |w|$ or if $c = \lambda$, $|w \circ b| = |w| - 1$. It remains to show that multiplication with b cannot result in a larger decrease of length. Let us assume $w \equiv w'a_2a_1$ and $|w \circ b| < |w| - 1$. Then there must be at least two rules $a_1b \longrightarrow c$, $a_2c \longrightarrow d \in T$ with $c \in \Sigma \backslash \{a_1, b\}$, $d \in \Sigma \backslash \{a_2, c\} \cup \{\lambda\}$. This implies there is a rule $c\,\mathsf{inv}(b) \longrightarrow a_1 \in T$, as (Σ, T) is a group presentation and $|\mathsf{inv}(b)| = 1$. Thus $d\,\mathsf{inv}(b) \longleftarrow \underline{a_2c}\,\mathsf{inv}(b) \equiv a_2\underline{c\,\mathsf{inv}(b)} \longrightarrow a_2a_1$ either implies $a_2a_1 \longrightarrow \mathsf{inv}(b) \in T$ in case $d = \lambda$ or there exists $e \in \Sigma \cup \{\lambda\}$ such that $a_2a_1 \longrightarrow e$, $d\,\mathsf{inv}(b) \longrightarrow e \in T$ and in both cases a_2a_1 is reducible, contradicting our assumption that $w \equiv w'a_2a_1 \in \mathcal{G}$.

q.e.d.

Lemma 5.3.3
Let (Σ, T) be a 2-monadic, convergent, reduced group presentation of a plain group $\mathcal{G}$. For a polynomial $p \in \mathbf{K}[\mathcal{G}]$ containing more than one monomial we define $\sigma_1(p)$ and $\sigma_2(p)$ as in definition 5.2.1. Further for $q \in \mathbf{K}[\mathcal{G}]$ let

$$C_q = \{b \in \Sigma \mid (ab, c) \in T, \text{ where } a = \ell(\mathsf{HT}(q)), c \in \Sigma\}.$$

Then

$$\text{SAT}_p(p) = \{\mathsf{can}(p), \mathsf{acan}(p)\} \cup \{\mathsf{can}(p) * d \mid d \in C_{\mathsf{can}(p)}\} \cup \{\mathsf{acan}(p) * d \mid d \in C_{\mathsf{acan}(p)}\}$$

is a prefix saturating set for p. In case $p = \alpha \cdot t \in \mathbf{K}[\mathcal{G}]$ we can set $\text{SAT}_p(p) = \{\lambda\}$.

Proof :
We have to show that the polynomials in the set $\{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{G}\}$ are prefix reducible to zero in one step by $\text{SAT}_p(p)$. In case $p = \alpha \cdot t$, $\alpha \in \mathbf{K}^*$, $t \in \mathcal{G}$, we are done as $\text{SAT}_p(p) = \{\lambda\} \in \mathcal{SAT}(p)$. In case the polynomial p contains more than one

monomial, we use procedure PREFIX SATURATED CHECK on page 107 to prove our claim by showing that for every polynomial $q \in \mathrm{SAT}_p(p)$ and every $w \in C(\mathsf{HT}(q))$ the multiple $q * w$ is prefix reducible to zero in one step using $\mathrm{SAT}_p(p)$. Let $\mathsf{HT}(\mathsf{can}(p)) \equiv ta$ and $\mathsf{HT}(\mathsf{acan}(p)) = t' \circ \mathsf{inv}(a)$ for some $t, t' \in \mathcal{G}$, $a \in \Sigma$. In case $q \in \{\mathsf{can}(p), \mathsf{acan}(p)\}$, the fact that $C(\mathsf{HT}(q)) = C_q \cup \{\mathsf{inv}(\ell(\mathsf{HT}(q)))\}$ and the definition of $\mathrm{SAT}_p(p)$ imply that for all $b \in C(\mathsf{HT}(q))$ we have $q * b \longrightarrow^{\mathrm{p}}_{S_p} 0$. Now, let us assume that $q = \mathsf{can}(p) * b$ for some $b \in C_{\mathsf{can}(p)}$ and $(ab, c) \in T$, $c \in \Sigma$. We have to distinguish the following two cases. If $\mathsf{HT}(q) \equiv tc$, then $C(tc) = \{d \mid (cd, e) \in T, d \in \Sigma, e \in \Sigma \cup \{\lambda\}\}$ and in case this set is not empty let us look at such a rule $(cd, e) \in T$. Since our presentation is a reduced convergent group presentation, there exists a rule of the form $\mathsf{inv}(a)c \longrightarrow b \in T$ where $|\mathsf{inv}(a)| = 1$. Now this gives us

$$bd \longleftarrow \underline{\mathsf{inv}(a)c}d \equiv \mathsf{inv}(a)\underline{cd} \longrightarrow \mathsf{inv}(a)e$$

and as $d \neq e$ and $b \neq \mathsf{inv}(a)$, there exists an element $f \in \Sigma \cup \{\lambda\}$ such that $bd \longrightarrow f$, $\mathsf{inv}(a)e \longrightarrow f \in T$. Again this results in the situation

$$cd \longleftarrow \underline{ab}d \equiv a\underline{bd} \longrightarrow af$$

and we either have $b \circ d = \lambda$ in case $f = \lambda$ or there exists a rule $af \longrightarrow e \in T$. In case $b \circ d = \lambda$ this implies $q * d = (\mathsf{can}(p) * b) * d = \mathsf{can}(p) * (b \circ d) = \mathsf{can}(p)$ and hence $q * d \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$. Otherwise, $q * d = (\mathsf{can}(p) * b) * d = \mathsf{can}(p) * (b \circ d) = \mathsf{can}(p) * f$ implies $q * d \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$ as $f \in C_{\mathsf{can}(p)}$ and hence $\mathsf{can}(p) * f \in \mathrm{SAT}_p(p)$. On the other hand, if $\mathsf{HT}(q) \not\equiv tc$ there exists a term $s \in \mathsf{T}(\mathsf{can}(p))$ such that $\mathsf{HT}(q) = s \circ b$ and $s \circ b \succ tc$. We have to distinguish two cases: In case $|s| < |ta|$ we know $s \circ b \equiv sb$, as $|s \circ b| = |tc|$. If $C(sb)$ is not empty let $be \longrightarrow f \in T$ be a corresponding rule. We get

$$ce \longleftarrow \underline{ab}e \equiv a\underline{be} \longrightarrow af.$$

As $c \neq a$ we either get $b \circ e = \lambda$ in case $f = \lambda$ implying that $q * e = (\mathsf{can}(p) * b) * e = \mathsf{can}(p) * (b \circ e) = \mathsf{can}(p)$ and hence $q * e \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$, or there exists an element $g \in \Sigma \cup \{\lambda\}$ such that $ce \longrightarrow g$, $af \longrightarrow g \in T$, giving us $q * e = (\mathsf{can}(p) * b) * e = \mathsf{can}(p) * (b \circ e) = \mathsf{can}(p) * f$ and thus $q * e \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$ as $f \in C_{\mathsf{can}(p)}$. On the other hand, if $|s| = |ta|$ with $s \equiv s'd$ and $db \longrightarrow f \in T$, then $s \prec ta$ and $s \circ b \equiv s'f \succ tc$ implies $s' \equiv t$ and $f \succ c$. Now suppose $C(s'f) \neq \emptyset$ and let $fg \longrightarrow h \in T$ be a corresponding rule. Since $db \longrightarrow f \in T$ we also have $\mathsf{inv}(d)f \longrightarrow b \in T$, resulting in

$$bg \longleftarrow \underline{\mathsf{inv}(d)f}g \equiv \mathsf{inv}(d)\underline{fg} \longrightarrow \mathsf{inv}(d)h.$$

Since $g \neq h$ in case $h = \lambda$ we have $bg \longrightarrow \mathsf{inv}(d) \in T$ giving us $cg \longleftarrow \underline{ab}g = a\underline{bg} \longrightarrow a\,\mathsf{inv}(d)$. But then, as $a, c, g, \mathsf{inv}(d)$ all are not equal to λ, there exists $i \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow i$, $a\,\mathsf{inv}(d) \longrightarrow i \in T$, and thus $\mathsf{inv}(d) \in C_{\mathsf{can}(p)}$. This implies $q * g = (\mathsf{can}(p) * b) * g = \mathsf{can}(p) * \mathsf{inv}(d) \in \mathrm{SAT}_p(p)$. On the other hand, in case $h \neq \lambda$, there exists $i \in \Sigma \cup \{\lambda\}$ such that $bg \longrightarrow i$, $\mathsf{inv}(d)h \longrightarrow i \in T$. Hence, $cg \longleftarrow \underline{ab}g \equiv a\underline{bg} \longrightarrow ai$. In

case $i = \lambda$, $bg \longrightarrow \lambda \in T$ immediately implies $q * g = (\mathsf{can}(p) * b) * g = \mathsf{can}(p) * (b \circ g) = \mathsf{can}(p)$. Otherwise there exists $j \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow j$, $ai \longrightarrow j \in T$, and hence $i \in C_{\mathsf{can}(p)}$, giving us $q * g = (\mathsf{can}(p) * b) * g = \mathsf{can}(p) * (b \circ g) = \mathsf{can}(p) * i \in \mathrm{SAT}_p(p)$. Hence in all these cases we have $q * g \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$.
The case $q = \mathsf{acan}(p) * b$ is similar in case $\mathsf{HT}(\mathsf{acan}(p)) \equiv t'\mathsf{inv}(a)$. Hence let us assume $\mathsf{HT}(\mathsf{acan}(p)) = t' \circ \mathsf{inv}(a) \not\equiv t'\mathsf{inv}(a)$. Then $t' \equiv t''k$, $t' \circ \mathsf{inv}(a) = t''l$ and $k\mathsf{inv}(a) \longrightarrow l \in T$. The rule corresponding to $b \in C_{\mathsf{acan}(p)}$ then is $lb \longrightarrow c \in T$. We have to distinguish the following two cases. If $\mathsf{HT}(q) \equiv tc$, then $C(tc) = \{d \mid (cd, e) \in T, d \in \Sigma, e \in \Sigma \cup \{\lambda\}\}$ and in case this set is not empty let us look at such a rule $(cd, e) \in T$. Since our presentation is a reduced convergent group presentation, there exists a rule of the form $\mathsf{inv}(l)c \longrightarrow b \in T$ where $|\mathsf{inv}(l)| = 1$. Now this gives us

$$bd \longleftarrow \underline{\mathsf{inv}(l)c}d \equiv \mathsf{inv}(l)\underline{cd} \longrightarrow \mathsf{inv}(l)e$$

and as $d \neq e$ and $b \neq \mathsf{inv}(l)$, there exists an element $f \in \Sigma \cup \{\lambda\}$ such that $bd \longrightarrow f$, $\mathsf{inv}(l)e \longrightarrow f \in T$. Again this results in the situation

$$cd \longleftarrow \underline{lb}d \equiv l\underline{bd} \longrightarrow lf$$

and we either have $b \circ d = \lambda$ in case $f = \lambda$ or there exists a rule $lf \longrightarrow e \in T$. In case $b \circ d = \lambda$ this implies $q * d = (\mathsf{acan}(p) * b) * d = \mathsf{acan}(p) * (b \circ d) = \mathsf{acan}(p)$ and hence $q * d \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$. Otherwise, $q * d = (\mathsf{acan}(p) * b) * d = \mathsf{acan}(p) * (b \circ d) = \mathsf{acan}(p) * f$ implies $q * d \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$ as $f \in C_{\mathsf{acan}(p)}$ and hence $\mathsf{acan}(p) * f \in \mathrm{SAT}_p(p)$. On the other hand, if $\mathsf{HT}(q) \neq tc$ there exists a term $s \in \mathsf{T}(\mathsf{acan}(p))$ such that $\mathsf{HT}(q) = s \circ b$ and $s \circ b \succ tc$. We have to distinguish two cases: In case $|s| < |tl|$ we know $s \circ b \equiv sb$, as $|s \circ b| = |tc|$. If $C(sb)$ is not empty let $be \longrightarrow f \in T$ be a corresponding rule. We get

$$ce \longleftarrow \underline{lb}e \equiv l\underline{be} \longrightarrow lf.$$

As $c \neq l$ we either get $b \circ e = \lambda$ in case $f = \lambda$ implying that $q * e = (\mathsf{acan}(p) * b) * e = \mathsf{acan}(p) * (b \circ e) = \mathsf{acan}(p)$ and hence $q * e \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$, or there exists an element $g \in \Sigma \cup \{\lambda\}$ such that $ce \longrightarrow g$, $lf \longrightarrow g \in T$, giving us $q * e = (\mathsf{acan}(p) * b) * e = \mathsf{acan}(p) * (b \circ e) = \mathsf{acan}(p) * f$ and thus $q * e \longrightarrow^{\mathrm{p}}_{\mathrm{SAT}_p(p)} 0$ as $f \in C_{\mathsf{acan}(p)}$. On the other hand, if $|s| = |tl|$ with $s \equiv s'd$ and $db \longrightarrow f \in T$ then $s \prec tl$ and $s \circ b \equiv s'f \succ tc$ implies $s' \equiv t$ and $f \succ c$. Now suppose $C(s'f) \neq \emptyset$ and let $fg \longrightarrow h \in T$ be a corresponding rule. Since $db \longrightarrow f \in T$ we also have $\mathsf{inv}(d)f \longrightarrow b \in T$, resulting in

$$bg \longleftarrow \underline{\mathsf{inv}(d)f}g \equiv \mathsf{inv}(d)\underline{fg} \longrightarrow \mathsf{inv}(d)h.$$

Since $g \neq h$ in case $h = \lambda$ we have $bg \longrightarrow \mathsf{inv}(d) \in T$ giving us $cg \longleftarrow \underline{lb}g = l\underline{bg} \longrightarrow l\,\mathsf{inv}(d)$. But then, as $l, c, g, \mathsf{inv}(d)$ all are not equal to λ, there exists $i \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow i$, $l\,\mathsf{inv}(d) \longrightarrow i \in T$, and thus $\mathsf{inv}(d) \in C_{\mathsf{acan}(p)}$. This implies $q * g = (\mathsf{acan}(p) * b) * g = \mathsf{acan}(p) * \mathsf{inv}(d) \in \mathrm{SAT}_p(p)$. On the other hand, in case $h \neq \lambda$, there exists $i \in \Sigma \cup \{\lambda\}$ such that $bg \longrightarrow i$, $\mathsf{inv}(d)h \longrightarrow i \in T$. Hence,

$cg \longleftarrow \underline{lb}g \equiv l\underline{bg} \longrightarrow li$. In case $i = \lambda$, $bg \longrightarrow \lambda \in T$ immediately implies $q * g = (\mathsf{acan}(p) * b) * g = \mathsf{acan}(p) * (b \circ g) = \mathsf{acan}(p)$. Otherwise there exists $j \in \Sigma \cup \{\lambda\}$ such that $cg \longrightarrow j$, $li \longrightarrow j \in T$, and hence $i \in C_{\mathsf{acan}(p)}$, giving us $q * g = (\mathsf{acan}(p) * b) * g = \mathsf{acan}(p) * (b \circ g) = \mathsf{acan}(p) * i \in \textsc{Sat}_p(p)$.
Hence in all these cases we have $q * g \longrightarrow^{\mathrm{p}}_{\textsc{Sat}_p(p)} 0$.

q.e.d.

Notice that unlike in the case of free groups, the sets $\textsc{Sat}_p$ as defined in lemma 5.3.3 need not be prefix Gröbner bases.

Example 5.3.4
Let $\Sigma = \{a, b, c, d, b^{-1}, c^{-1}\}$ and $T = \{a^2 \longrightarrow \lambda, d^2 \longrightarrow \lambda, bb^{-1} \longrightarrow \lambda, b^{-1}b \longrightarrow \lambda, cc^{-1} \longrightarrow \lambda, c^{-1}c \longrightarrow \lambda, ab \longrightarrow c, ac \longrightarrow b, c^{-1}b \longrightarrow d, c^{-1}a \longrightarrow b^{-1}, cb^{-1} \longrightarrow a, cd \longrightarrow b, db^{-1} \longrightarrow c^{-1}, dc^{-1} \longrightarrow b^{-1}, bc^{-1} \longrightarrow a, bd \longrightarrow c, b^{-1}a \longrightarrow c^{-1}, b^{-1}c \longrightarrow d\}$ be a presentation of a plain group $\mathcal{G}$[11] with a length-lexicographical ordering induced by $a \succ b^{-1} \succ b \succ c^{-1} \succ c \succ d$.
For the polynomial $p = ad + a + \lambda \in \mathbf{Q}[\mathcal{G}]$ we get $\sigma_1(p) = \lambda$, $\sigma_2(p) = d$,$\mathsf{can}(p) = p * \lambda = ad + a + \lambda$ and $\mathsf{acan}(p) = p * d = ad + a + d$. In contrary to the case of free groups the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$ alone is not prefix saturated and even not confluent since we have $\mathsf{HT}(\mathsf{can}(p)) = \mathsf{HT}(\mathsf{acan}(p))$. By lemma 5.3.3 we can give a prefix saturating set for p, namely $\textsc{Sat}_p(ad+a+\lambda) = \{ad+a+\lambda, ad+a+d, ab^{-1}+ac^{-1}+b^{-1}, ab^{-1}+ac^{-1}+c^{-1}\}$ where the polynomials arise from the multiplications $(ad + d + \lambda) * d = a + \underline{ad} + d$, $(ad+a+\lambda) * b^{-1} = ac^{-1} + \underline{ab^{-1}} + b^{-1}$ and $(a + \underline{ad} + d) * b^{-1} = ac^{-1} + \underline{ab^{-1}} + c^{-1}$. Note that this set is no prefix Gröbner basis as for the prefix s-polynomial

$$\mathsf{spol}_p(ad + a + \lambda, ad + a + d) = d - \lambda$$

we get that it is not prefix reducible by the polynomials in $\textsc{Sat}_p(ad + a + \lambda)$. $\diamond$

Specifying saturation of polynomials in procedure Reduced Prefix Gröbner Bases on page 114 we we can compute finite reduced prefix Gröbner bases in plain group rings.

5.4 Context-free Groups

As stated in the introductory chapter, a finitely generated context-free group $\mathcal{G}$ is a group with a free normal subgroup of finite index. Hence, let the group $\mathcal{G}$ be given by X a finite set of generators for a free subgroup $\mathcal{F}$ and $\mathcal{E}$ a finite group such that $(\mathcal{E}\backslash\{\lambda\}) \cap (X \cup X^{-1}) = \emptyset$ and $\mathcal{G}/\mathcal{F} \cong \mathcal{E}$. For all $e \in \mathcal{E}$ let $\phi_e : X \cup X^{-1} \longrightarrow \mathcal{F}$ be a function such that ϕ_λ is the inclusion and for all $x \in X \cup X^{-1}$, $\phi_e(x) = \mathsf{inv}(e) \circ_{\mathcal{G}} x \circ_{\mathcal{G}} e$. For all $e_1, e_2 \in \mathcal{E}$ let $z_{e_1,e_2} \in \mathcal{F}$ such that $z_{e_1,\lambda} \equiv z_{\lambda,e_1} \equiv \lambda$ and for all $e_1, e_2, e_3 \in \mathcal{E}$ with $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$, $e_1 \circ_{\mathcal{G}} e_2 \equiv e_3 z_{e_1,e_2}$. Let $\Sigma = (\mathcal{E}\backslash\{\lambda\}) \cup X \cup X^{-1}$ and let T contain the following rules:

[11] This follows as the presentation is 2-monadic convergent and includes inverses of length 1 for all generators.

$$\begin{array}{lcll} xx^{-1} & \longrightarrow & \lambda & \text{and} \\ x^{-1}x & \longrightarrow & \lambda & \text{for all } x \in X, \\ e_1e_2 & \longrightarrow & e_3z_{e_1,e_2} & \text{for all } e_1, e_2 \in \mathcal{E}\backslash\{\lambda\}, e_3 \in \mathcal{E} \text{ such that } e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3, \\ xe & \longrightarrow & e\phi_e(x) & \text{and} \\ x^{-1}e & \longrightarrow & e\phi_e(x^{-1}) & \text{for all } e \in \mathcal{E}\backslash\{\lambda\}, x \in X. \end{array}$$

(Σ, T) then is a canonical and is called a virtually free presentation (compare [CrOt94]). Presenting $\mathcal{G}$ in this way we find that the elements of the group are of the form eu where $e \in \mathcal{E}$ and $u \in \mathcal{F}$. We can specify a total well-founded ordering on our group by combining a total well-founded ordering $\succeq_{\mathcal{E}}$ on $\mathcal{E}$ and a length-lexicographical ordering $\geq_{\text{lex}}$ on $\mathcal{F}$: Let $w_1, w_2 \in \mathcal{G}$ such that $w_i \equiv e_iu_i$ where $e_i \in \mathcal{E}$, $u_i \in \mathcal{F}$. Then we define $w_1 \succ w_2$ if and only if $|w_1| > |w_2|$ or ($|w_1| = |w_2|$ and $e_1 \succ_{\mathcal{E}} e_2$) or ($|w_1| = |w_2|$ and $e_1 =_{\mathcal{E}} e_2$ and $u_1 >_{\text{lex}} u_2$). This ordering is compatible with right concatenation using elements in $\mathcal{F}$ in the following sense: Given $w_1, w_2 \in \mathcal{G}$ presented as described above, $w_1 \succ w_2$ implies $w_1u \succ w_2u$ for all $u \in \mathcal{F}$ in case $w_1u, w_2u \in \mathcal{G}$.

Example 5.4.1
Let $\mathcal{E}$ be the finite group presented by $\Sigma' = \{a\}$ and $T' = \{a^2 \longrightarrow \lambda\}$ and $\mathcal{F}$ the free group generated by $X = \{x\}$. Further let $\phi_a(x) = x$ and $\phi_a(x^{-1}) = x^{-1}$ be a conjugation homomorphism.
Then $\Sigma = \{a, x, x^{-1}\}$ and $T = \{xx^{-1} \longrightarrow \lambda, x^{-1}x \longrightarrow \lambda\} \cup \{a^2 \longrightarrow \lambda\} \cup \{xa \longrightarrow ax, x^{-1}a \longrightarrow ax^{-1}\}$ is a virtually free presentation of $\mathcal{G}$. ◇

Let us take a closer look at prefix reduction in $\mathbf{K}[\mathcal{G}]$.

Example 5.4.2
Let $\mathcal{G}$ be the group specified in example 5.4.1. Further let $p = ax^2 + x + \lambda$, $q_1 = a + x$ and $q_2 = x^2 + \lambda$ be polynomials in $\mathbf{Q}[\mathcal{G}]$.
Then the polynomial p is prefix reducible at its head term ax^2 by q_1 giving us

$$p \longrightarrow^{\mathrm{p}}_{q_1} p - q_1 * x^2 = \underline{ax^2} + x + \lambda - \underline{ax^2} - x^3 = x + \lambda + \underline{x^3}.$$

On the other hand, as x^2 is no prefix of ax^2, this is not true for q_2. ◇

Definition 5.4.3
Let $\mathcal{H}$ be a subgroup of a group $\mathcal{N}$ and p a non-zero polynomial in $\mathbf{K}[\mathcal{N}]$. A set $S \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{H}\}$ is called a **$\mathcal{H}$-prefix saturating set** for p, if for all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{H}$ the polynomial $\alpha \cdot p * w$ is prefix reducible to zero using S in one step. A set of polynomials $F \subseteq \mathbf{K}[\mathcal{N}]$ is called a **$\mathcal{H}$-prefix saturated set**, if for all $f \in F$ and for all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{H}$ the polynomial $\alpha \cdot f * w$ is prefix reducible to zero using F in one step. ◇

Reviewing the results on free groups, for a polynomial p in $\mathbf{K}[\mathcal{G}]$ we can specify $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ as follows.

Definition 5.4.4
For a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ we define

$$\sigma_1(p) = \max\{u \in \mathcal{F} \mid \mathsf{inv}(u) \text{ is a suffix of } \mathsf{HT}(p) \text{ and } \mathsf{HT}(p * u) = \mathsf{HT}(p) \circ u\},$$

In case p contains more than one monomial or $\mathsf{HT}(p) \neq e\mathsf{inv}(\sigma_1(p))$ for $e \in \mathcal{E}$ we define

$$\sigma_2(p) = \min\{u \in \mathcal{F} \mid \mathsf{inv}(u) \text{ is a suffix of } \mathsf{HT}(p) \text{ and } \mathsf{HT}(p * u) \neq \mathsf{HT}(p) \circ u\}$$

and else $\sigma_2(p) = \sigma_1(p)$. Then we can set $\mathsf{can}(p) = p * \sigma_1(p)$ and $\mathsf{acan}(p) = p * \sigma_2(p)$. $\diamond$

Lemma 5.4.5
Let $p \in \mathbf{K}[\mathcal{G}]$ be a non-zero polynomial. Then the set $\{\mathsf{can}(p), \mathsf{acan}(p)\}$, is a $\mathcal{F}$-prefix saturating set for p.

Proof :
The proof is straightforward as in lemma 5.2.6. We only have to consider the additional case $\mathsf{HT}(p * \sigma_1(p)) \equiv e \in \mathcal{E}$. Since for all $w \in \mathcal{F}$ we get $\mathsf{HT}(p * w) = \mathsf{HT}(p) * w \equiv ew'$ for some $w' \in \mathcal{F}$, then $\{\mathsf{can}(p) = \mathsf{acan}(p) = p * \sigma_1(p)\}$ is a prefix saturating set.

q.e.d.

Example 5.4.6
Let $\mathcal{G}$ be the group specified in example 5.4.1. Then for the polynomial $p = ax^2 + x + \lambda$ in $\mathbf{Q}[\mathcal{G}]$ we get $\sigma_1(p) = x^{-1}$ and $\sigma_2(p) = x^{-2}$ giving us $\mathsf{can}(p) = p * \sigma_1(p) = \underline{ax} + \lambda + x^{-1}$ and $\mathsf{acan}(p) = p * \sigma_2(p) = a + x^{-1} + \underline{x^{-2}}$.
On the other hand $q = a + x$ gives us $\sigma_1(q) = \sigma_2(q) = \lambda$ and thus $\mathsf{can}(q) = \mathsf{acan}(q) = q$.

$\diamond$

The following lemma will be used as an analogon to lemma 4.4.13 when we characterize prefix Gröbner bases by using prefix reduction, prefix s-polynomials and now $\mathcal{F}$-prefix saturated sets.

Lemma 5.4.7
Let p be a non-zero polynomial and F a set of polynomials in $\mathbf{K}[\mathcal{G}]$. Then $p \xrightarrow{*}{}^{\mathrm{p}}_{F} 0$ gives us a prefix standard representation of $p = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, with $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{G}$ such that for all $w \in \mathcal{F}$ with $\mathsf{HT}(p * w) \equiv \mathsf{HT}(p)w$, we get $\mathsf{HT}(p)w \succeq \mathsf{HT}(f_i * w_i * w)$. Note that additionally for all $t \in \mathcal{M}$ with $t \succeq \mathsf{HT}(p)$, if $t \circ w \equiv tw$ for some $w \in \mathcal{M}$, then $tw \succeq \mathsf{HT}(f_i * w_i * w)$. $\square$

For every $e \in \mathcal{E}$ let the mapping $\psi_e : \mathbf{K}[\mathcal{G}] \longrightarrow \mathbf{K}[\mathcal{G}]$ be defined by $\psi_e(f) = f * e$ for $f \in \mathbf{K}[\mathcal{G}]$. We now can give a characterization of prefix Gröbner bases by transforming a generating set for a right ideal using these finitely many mappings. This will enable us to restrict ourselves to $\mathcal{F}$-prefix saturated sets when characterizing prefix Gröbner bases.

Theorem 5.4.8
Let $F \subseteq \mathbf{K}[\mathcal{G}]$ and $G \subseteq \mathbf{K}[\mathcal{G}]$ such that

- $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$
- $\{\psi_e(f) \mid f \in F, e \in \mathcal{E}\} \subseteq G$
- *G is $\mathcal{F}$-prefix saturated.*

. Then the following statements are equivalent:

1. *For all $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}^{\mathrm{p}}_G 0$.*
2. *For all $f_k, f_l \in G$ we have $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}^{\mathrm{p}}_G 0$.*

Proof :
$1 \Longrightarrow 2$: Let $\mathsf{HT}(f_k) \equiv \mathsf{HT}(f_l)w$ for $f_k, f_l \in G$ and $w \in \mathcal{G}$. Then by definition 4.4.34 we get

$$\mathsf{spol}_p(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k - \mathsf{HC}(f_l)^{-1} f_l * w \ \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F),$$

and hence $\mathsf{spol}_p(f_k, f_l) \xrightarrow{*}^{\mathrm{p}}_G 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow^{\mathrm{p}}_G$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$, $h \longrightarrow^{\mathrm{p}}_G h'$ implies $h' \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F)$. Thus as $\longrightarrow^{\mathrm{p}}_G$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{p}}_G$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{G}$. Further for all $1 \leq j \leq m$, let $w_j \equiv e_j u_j$, with $e_j \in \mathcal{E}$, $u_j \in \mathcal{F}$. Then, we can modify our representation of g to $g = \sum_{j=1}^{m} \alpha_j \cdot \psi_{e_j}(f_j) * u_j$. Since G is $\mathcal{F}$-prefix saturated and $\psi_{e_j}(f_j) \in G$ we can assume $g = \sum_{j=1}^{m} \alpha_j \cdot g_j * v_j$, where $\alpha_j \in \mathbf{K}^*, g_j \in G, v_j \in \mathcal{F}$ and $\mathsf{HT}(g_j * v_j) \equiv \mathsf{HT}(g_j)v_j$. Depending on this representation of g and our well-founded total ordering $\succeq$ on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(g_j)v_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $g_j * v_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{p}}_G$-reducible. So by lemma 4.2.14 it is sufficient to show that g has a prefix standard representation, as this implies that g is top-reducible using G. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[12]. If $t \succ \mathsf{HT}(g)$ there are two polynomials g_k, g_l in the corresponding representation[13] and $t \equiv \mathsf{HT}(g_k)v_k \equiv \mathsf{HT}(g_l)v_l$. Without loss of generality let us assume $\mathsf{HT}(g_k) \equiv \mathsf{HT}(g_l)z$ for some $z \in \mathcal{F}$ and $v_l \equiv z v_k$. Then by definition 4.4.34 we have a prefix s-polynomial $\mathsf{spol}_p(g_k, g_l) = \mathsf{HC}(g_k)^{-1} \cdot g_k - \mathsf{HC}(g_l)^{-1} \cdot g_l * z$. We will now change our representation of g by using the additional information on this s-polynomial in such

[12]Note that this ordering is well-founded since $\succeq$ is and $K \in \mathbf{N}$.
[13]Not necessarily $g_l \neq g_k$.

a way that for the new representation of g we either have a smaller maximal term or the occurrences of the term t are decreased by at least 1. Let us assume $\mathsf{spol}_p(g_k, g_l) \neq 0$[14]. Hence, the reduction sequence $\mathsf{spol}_p(g_k, g_l) \xrightarrow{*}{}^{\mathrm{p}}_{G} 0$ yields a prefix standard representation of the form $\mathsf{spol}_p(g_k, g_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v_i'$, $\delta_i \in \mathbf{K}^*$,$h_i \in G$,$v_i' \in \mathcal{F}$ and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_p(g_k, g_l))$. By lemma 5.4.7 we can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i' * v_k$ and again we can substitute all polynomials h_i, where $\mathsf{HT}(h_i * v_i' * v_k) \neq \mathsf{HT}(h_i)(v_i' \circ v_k)$ without increasing t or K. Similarly, in case $v_i' \in \mathcal{E}$, we can substitute h_i by $\psi_{v_i'}(h_i) \in G$ by our assumption. Therefore, without loss of generality we can assume that the representation has the required form. This gives us:

$$\begin{aligned}
& \alpha_k \cdot g_k * v_k + \alpha_l \cdot g_l * v_l \\
= \quad & \alpha_k \cdot g_k * v_k + \underbrace{\alpha_l' \cdot \beta_k \cdot g_k * v_k - \alpha_l' \cdot \beta_k \cdot g_k * v_k}_{=0} + \alpha_l' \cdot \beta_l \cdot g_l * v_l \\
= \quad & (\alpha_k + \alpha_l' \cdot \beta_k) \cdot g_k * v_k - \alpha_l' \cdot \underbrace{(\beta_k \cdot g_k * v_k - \beta_l \cdot g_l * v_l)}_{=\mathsf{spol}_p(g_k, g_l) * v_k} \\
= \quad & (\alpha_k + \alpha_l' \cdot \beta_k) \cdot g_k * v_k - \alpha_l' \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v_i' * v_k) \qquad (5.1)
\end{aligned}$$

where $\beta_k = \mathsf{HC}(g_k)^{-1}$, $\beta_l = \mathsf{HC}(g_l)^{-1}$ and $\alpha_l' \cdot \beta_l = \alpha_l$. By substituting (5.1) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

q.e.d.

Next we give a procedure to compute reduced prefix Gröbner bases by modifying procedure Reduced Prefix Gröbner Bases on page 114.

Procedure: Reduced Gröbner Bases in Context-Free Group Rings

Given: $F \subseteq \mathbf{K}[\mathcal{G}]$, (Σ, T) a virtually free presentation of $\mathcal{G}$.
Find: $\mathrm{GB}(F)$, a (prefix) Gröbner basis of F.

$G_0 := \emptyset$;
$S_0 := \{\mathsf{can}(\psi_e(f)), \mathsf{acan}(\psi_e(f)) \mid e \in \mathcal{E}, f \in F\}$;
$i := 0$;
while $S_i \neq \emptyset$ **do** % $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_i \cup S_i)$
  $i := i + 1$;
  $q_i :=$ remove(S_{i-1});
  % Remove an element using a fair strategy
  $q_i' :=$ normalform$(q_i, \longrightarrow^{\mathrm{p}}_{G_{i-1}})$;
  % Compute a normal form using prefix reduction

[14]In case $\mathsf{spol}_p(g_k, g_l) = 0$, just substitute 0 for $\sum_{i=1}^{n} \delta_i \cdot h_i * v_i'$ in the equations below.

if $q'_i \neq 0$
  then **if** $|\mathsf{T}(q'_i)| = 1$
    % The right ideal is trivial
    then $G_i := \{\lambda\}$;
      $S_i := \emptyset$;
    else
      $H_i := \{g \in G_i \mid \mathsf{HT}(g)$ is prefix reducible using $q'_i\}$;
      % These polynomials would have new head terms when prefix
      % reduced using q'_i
      $G_i := (G_{i-1} \backslash H_i) \cup \{q'_i\}$;
      $S_i := S_{i-1} \cup H_i \cup \{\mathsf{can}(q'_i), \mathsf{acan}(q'_i)\}$;
  endif
endif
endwhile
$\textsc{Gb}(F)$:= reduce(G_i)
% reduce$(F) = \{\text{normalform}(f, \longrightarrow^{\mathrm{p}}_{F \backslash \{f\}}) \mid f \in F\}$[15]

Remark 5.4.9
For all sets computed we have $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G_i \cup S_i) = \mathsf{ideal}_r(G)$. But note that the set G need not fulfill the condition that $\{\psi_e(f) \mid e \in \mathcal{E}, f \in F\} \subseteq G$. Hence theorem 5.4.8 cannot be applied to ensure that G is a prefix Gröbner basis. We will see later on that $\{\mathsf{can}(\psi_a(f)) \mid a \in \mathcal{E}, f \in F\} \subseteq G_0$ in fact is sufficient to ensure correctness. $\diamond$

Termination of the procedure follows by the same arguments used for plain groups.

Theorem 5.4.10
Procedure Reduced Gröbner Bases in Context-Free Group Rings *terminates on finite input F.*

Proof :
The proof is done in two steps: first we show that all polynomials computed have a certain property that will be used in the second step to ensure termination. We say a polynomial q has property $\mathcal{P}_F$ if and only if

(α) $|\mathsf{HT}(q)| \leq K$, where
$K = \max\{|\mathsf{HT}(f)| \mid f \in \{\mathsf{can}(\psi_e(f)), \mathsf{acan}(\psi_e(f)) \mid e \in \mathcal{E}, f \in F\}\} + 1.$

(β) If $|\mathsf{HT}(q)| = K$ then there exists an element $a \in X \cup X^{-1}$ such that all terms of length K in q have a as a common suffix.

[15]Notice that only the reducts are touched in this procedure.

We will show that all polynomials q computed by the procedure on input F have property $\mathcal{P}_F$.

By the choice of K all polynomials in G_0 and S_0 have $\mathcal{P}_F$. Let G_i and S_i be actual computed sets of polynomials having $\mathcal{P}_F$ and let q_i be the next polynomial chosen by our procedure. Then q_i is first prefix reduced to normal form with respect to G_i and only polynomials having $\mathcal{P}_F$ are involved. By the definition of prefix reduction this operation preserves property $\mathcal{P}_F$.

It remains to show that computing the polynomials $\mathsf{can}(p)$ and $\mathsf{acan}(p)$ of a polynomial having $\mathcal{P}_F$ does not destroy this property. In case $q = \alpha \cdot t$ or $\mathsf{HT}(q * \sigma_1(q)) \in \mathcal{E}$ we are done. Hence let us assume $\mathsf{HT}(q * \sigma_1(q)) \equiv eu$ for some $e \in \mathcal{E}$, $u \in \mathcal{F}$ and let $|eu| = K$. Then $\sigma_1(p) = \lambda$ as $|\mathsf{HT}(q * \sigma_1(q))| \leq |\mathsf{HT}(q)|$ and q has $\mathcal{P}_F$. Furthermore, all $t \in \mathsf{T}(q)$ of length K have a common last letter, say $a \in X \cup X^{-1}$. Since $\sigma_2(p) = \mathsf{inv}(a)$, the head term of $q * \mathsf{inv}(a)$ must again have length less equal to K and all terms of length K must have $\mathsf{inv}(a)$ as last letter.

It remains to show that the procedure terminates. Let us assume the contrary. Then there are infinitely many polynomials q_i', $i \in \mathbf{N}$, with heads in normal form added.

But since no term occurs more than once among the head terms of polynomials added to a set G_i, $i > 0$, and for every such polynomial we have $|\mathsf{HT}(q_i')| \leq K$ this is not possible.

q.e.d.

Theorem 5.4.11

Procedure Reduced Gröbner Bases in Context-Free Group Rings *is correct.*

Proof :

Let G be the output of procedure Reduced Gröbner Bases in Context-Free Group Rings on input F. Without loss of generality let us assume that $\mathsf{ideal}_r(F)$ is not trivial, i.e., it is neither $\{0\}$ nor $\mathbf{K}[\mathcal{G}]$. Then by theorem 4.4.20 it is sufficient to show that every non-zero polynomial g in $\mathsf{ideal}_r(F)$ has a prefix standard representation with respect to G. This will be done by transforming an arbitrary representation of g with respect to F into a prefix standard representation with respect to G. Let $g = \sum_{i=1}^{k} \alpha_i \cdot f_i \cdot w_i$ with $\alpha_i \in \mathbf{K}^*$, $f_i \in F$, $w_i \in \mathcal{G}$ and $w_i \equiv e_i u_i$ for $e_i \in \mathcal{E}$, $u_i \in \mathcal{F}$. Then since the set $\{\mathsf{can}(\psi_e(f)) | e \in \mathcal{E}, f \in F\} \subseteq G_0 \cup S_0$ we can represent g as $g = \sum_{i=1}^{k} \alpha_i \cdot \psi_{e_i}(f_i) * u_i$. Furthermore, as the set $G_0 \cup S_0$ is $\mathcal{F}$-prefix saturated we even get a representation $g = \sum_{i=1}^{m'} \beta_i \cdot g_i * v_i$ with $\beta_i \in \mathbf{K}^*$, $g_i \in G_0 \cup S_0$ and $v_i \in \mathcal{F}$[16] such that $\mathsf{HT}(g_i * v_i) \equiv \mathsf{HT}(g_i) v_i$. In showing that every $f \in G_0 \cup S_0$ has a prefix standard representation with respect to G by lemma 4.4.10 then a prefix standard representation for g with respect to G also exists. Remember that lemma 4.4.10 states that in case a polynomial has a prefix standard representation with respect to a set and

[16] This is due to the fact that $\mathsf{ideal}_r(F)$ does not contain the identity.

all polynomials in this set have prefix standard representations with respect to another set, the polynomial itself again has a prefix standard representation with respect to the latter set. Let us proceed now in showing our last claim. Since our procedure terminates there exists an index $k \in \mathbf{N}$ such that $G = \text{reduce}(G_k)$ and $S_k = \emptyset$. We will now prove that our claim holds for every $f \in G_i \cup S_i$ by induction on j where $i = k - j$. In case $j = 0$ we are immediately done since by lemma 4.4.10 $f \in G_k$ has a prefix standard representation with respect to G. Hence let $f \in G_{k-(j+1)} \cup S_{k-(j+1)}$ and suppose $f \notin G_{k-j} \cup S_{k-j}$, as then our induction hypothesis can be applied and therefore the claim holds. Now if $f \in G_{k-(j+1)}$, $\mathsf{HT}(f)$ must be prefix reducible using the polynomial q'_{k-j} computed in this iteration, as we assume $f \notin G_{k-j}$. Therefore we get $f \in H_{k-j}$ and hence $f \in S_{k-j}$ and we are done. It remains to study the case that $f \in S_{k-(j+1)}$. Since $f \notin S_{k-j}$, f is chosen to compute the polynomial q'_{k-j} and again we can conclude that f has a prefix standard representation with respect to $G_{k-j} \cup S_{k-j}$ and hence with respect to G.

q.e.d.

5.5 Nilpotent Groups

Nilpotent groups and their presentations were briefly described in section 2.4. The fact that their elements can be presented by ordered group words motivates an approach similar to the one for commutative monoids. Since multiplication is no longer commutative, we will first restrict ourselves to right ideals and show the existence of finite right Gröbner bases for finitely generated right ideals. Later on this approach will be extended to two-sided ideals. Let us start by generalizing the concept of special divisors which can be interpreted as (commutative) "prefixes" in the set of ordered group words as in the commutative case. This will be done by extending the tuple ordering on ordered words (compare definition 4.5.1) to a tuple ordering on the set of ordered group words $\mathsf{ORD}(\Sigma) = \{a_1^{i_1} \dots a_n^{i_n} | i_j \in \mathbf{Z}\}$.

Definition 5.5.1
For $w \equiv a_1^{i_1} \dots a_n^{i_n}, v \equiv a_1^{j_1} \dots a_n^{j_n} \in \mathsf{ORD}(\Sigma)$, we define $w \geq_{\text{tup}} v$ if for each $1 \leq l \leq n$ we have either $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ and $|i_l| \geq |j_l|$. Further we define $w >_{\text{tup}} v$ if $w \geq_{\text{tup}} v$ and $|i_l| > |j_l|$ for some $1 \leq l \leq n$. $\diamond$

According to this ordering we call v a prefix of w if $v \leq_{\text{tup}} w$. Notice that an element then has finitely many prefixes.

Let us now start by investigating the special case of torsion-free nilpotent groups. As seen in section 2.4, such a group can be presented by a convergent CNI-system over an alphabet $\Sigma = \{a_1, a_1^{-1}, \dots, a_n, a_n^{-1}\}$, and we show that for such presentations (which contain no P-rules) additional syntactical lemmata hold which enable a weakening of reduction comparable to commutative reduction.

Example 5.5.2
The free nilpotent group of class 2 with 2 generators described in example 2.1.20 can be presented by the convergent CNI-system $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$ and $T = \{a_2a_1 \longrightarrow a_1a_2a_3, a_2^{-1}a_1^{-1} \longrightarrow a_1^{-1}a_2^{-1}a_3, a_2^{-1}a_1 \longrightarrow a_1a_2^{-1}a_3^{-1}, a_2a_1^{-1} \longrightarrow a_1^{-1}a_2a_3^{-1}, a_3^{\delta}a_2^{\delta'} \longrightarrow a_2^{\delta'}a_3^{\delta}, a_3^{\delta}a_1^{\delta'} \longrightarrow a_1^{\delta'}a_3^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$. $\diamond$

The ordering on our group $\mathcal{G}$ will be the syllable ordering and for $w, v \in \mathcal{G}$ we have that $w >_{\text{tup}} v$ implies $w >_{\text{syll}} v$, but the converse is not true, as $\geq_{\text{tup}}$ is not total. Reviewing example 5.5.2 we find $a_1a_2 >_{\text{tup}} a_1$ and $a_1a_2 >_{\text{syll}} a_1$, but $a_1^{-1}a_2 >_{\text{syll}} a_1$ and $a_1^{-1}a_2 \not>_{\text{tup}} a_1$. The following lemma reveals a connection between these two orderings in nilpotent groups having convergent CNI-presentations which specifies under which conditions a term remains a proper bound for $>_{\text{syll}}$-smaller terms under restricted right multiplication.

Lemma 5.5.3
Let $\mathcal{G}$ be a finitely generated nilpotent group presented by a convergent CNI-system on $\Sigma = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$. Further let $w, v, \tilde{v} \in \mathcal{G}$ with $w \geq_{\text{tup}} v$ and $v >_{\text{syll}} \tilde{v}$. Then for $u \in \mathcal{G}$ such that $w = v \circ u$, we get $w >_{\text{syll}} \tilde{v} \circ u$. Notice that since $\mathcal{G}$ is a group such an element u always exists, namely $u = \mathsf{inv}(v) \circ w$, and u is unique.

Proof :
Let $w, v, \tilde{v}, u \in \mathcal{G}$ be presented by ordered group words, i.e., $w \equiv a_1^{w_1} \ldots a_n^{w_n}$, $v \equiv a_1^{v_1} \ldots a_n^{v_n}$, $\tilde{v} \equiv a_1^{\tilde{v}_1} \ldots a_n^{\tilde{v}_n}$, and $u \equiv a_1^{u_1} \ldots a_n^{u_n}$ with $w_i, v_i, \tilde{v}_i, u_i \in \mathbf{Z}$. Further let a_d be the distinguishing letter between v and $\tilde{v}$, i.e., $v_d >_{\mathbf{Z}} \tilde{v}_d$. Since the commutation system only includes rules of the form $a_j^{\delta}a_i^{\delta'} \longrightarrow a_i^{\delta'}a_j^{\delta}z$, $j > i$, $z \in \mathsf{ORD}(\Sigma_{j+1})$, $\delta, \delta' \in \{1, -1\}$ and we have no P-rules, we can conclude

$$a_1^{v_1} \ldots a_{d-1}^{v_{d-1}} \circ a_1^{u_1} \ldots a_{d-1}^{u_{d-1}} = a_1^{\tilde{v}_1} \ldots a_{d-1}^{\tilde{v}_{d-1}} \circ a_1^{u_1} \ldots a_{d-1}^{u_{d-1}} \equiv a_1^{w_1} \ldots a_{d-1}^{w_{d-1}} a_d^{s_d} \ldots a_n^{s_n}$$

for some $s_i \in \mathbf{Z}$. Moreover, $a_d^{v_d} \circ a_d^{s_d} \circ a_d^{u_d} = a_d^{w_d}$, i.e., $v_d + s_d + u_d = w_d$. To prove $w_d >_{\mathbf{Z}} \tilde{v}_d + s_d + u_d$ and hence $w >_{\text{syll}} \tilde{v} \circ u$, we have to take a closer look at v_d and $\tilde{v}_d$.

1. In case $v_d > 0$ this implies $w_d > 0$ as $w \geq_{\text{tup}} v$. Therefore, $v_d + s_d + u_d = w_d$ and $w_d \geq v_d > 0$ give us $s_d + u_d \geq 0$. Now $v >_{\text{syll}} \tilde{v}$ and $v_d > 0$ imply that $v_d > \tilde{v}_d \geq 0$, as otherwise $\tilde{v}_d \geq_{\mathbf{Z}} v_d$ would contradict our assumption. Hence we get $\tilde{v}_d + s_d + u_d < w_d$, implying $w >_{\text{syll}} \tilde{v} \circ u$.

2. In case $v_d < 0$ this implies $w_d < 0$, $|w_d| \geq |v_d|$ and thus $v_d + s_d + u_d = w_d$ yields $s_d + u_d \leq 0$. Further we know $|v_d| + |s_d + u_d| = |w_d|$. We have to distinguish two cases:

   (a) In case $\tilde{v}_d \leq 0$, then $v >_{\text{syll}} \tilde{v}$ implies $|v_d| > |\tilde{v}_d|$. Therefore, we get $|\tilde{v}_d| + |s_d + u_d| < |w_d|$ and $w >_{\text{syll}} \tilde{v} \circ u$.

(b) In case $\tilde{v}_d > 0$, as $s_d + u_d \leq 0$ we have to take a closer look at $\tilde{v}_d + s_d + u_d$. In case $\tilde{v}_d + s_d + u_d \geq 0$ we are done as this implies $w >_{\text{syll}} \tilde{v} \circ u$. In case $\tilde{v}_d + s_d + u_d < 0$ we get that $\tilde{v}_d < |s_d + u_d|$ implying $|\tilde{v}_d + s_d + u_d| < |s_d + u_d| < |w_d|$ and hence $w >_{\text{syll}} \tilde{v} \circ u$.

q.e.d.

Remark 5.5.4
In the previous proof it is very important that the modifications due to the changes of the occurrences of the letters $a_1, \ldots, a_{d-1}$ are the same in v and $\tilde{v}$. Further all changes of the occurrence of the letter a_d due to those modifications are actually the same and are expressed in the exponent s_d. This is true since "moving" a letter with a smaller index past a_d can only add a word in $\mathsf{ORD}(\Sigma_{d+1})$ and moving a newly introduced letter with an index $k > d$ back past the letter a_d can only add words in $\mathsf{ORD}(\Sigma_{k+1})$ (compare lemma 2.4.14). Note that this argumentation need no longer hold for arbitrary CR-rules $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} z$, $z \in \mathsf{ORD}(\Sigma_{i+1})$, as a rule $a_d a_i \longrightarrow a_i z$ can have additional influence on the occurrence of the distinguishing letter a_d. Similar problem occur in case the presentation contains a power rule $a_d^{m_d} \longrightarrow r$, $r \in \mathsf{ORD}(\Sigma_{d+1})$. The existence of a P-rule yields $0 \leq \tilde{v}_d < v_d \leq w_d$, but we only know $(v_d + s_d + u_d) \ \mathsf{mod}\ m_d = w_d$ and hence $(\tilde{v}_d + s_d + u_d) \ \mathsf{mod}\ m_d > w_d$, i.e., $\tilde{v} \circ u >_{\text{syll}} w$, is possible. $\diamond$

Notice that the observations of this remark on the behaviour of CNI-presentations are essential and will be frequently used in the proofs of this section.

Henceforth, let $\mathcal{G}$ be a torsion-free nilpotent group with a convergent CNI-presentation (Σ, T). We are using the syllable ordering to induce the ordering on the group ring $\mathbf{K}[\mathcal{G}]$ and the tuple ordering to restrict this ordering. This is similar to the concepts of prefix and commutative reduction. Note that these reductions correspond to the property described in lemma 5.5.3 as follows: If $\mathcal{M}$ is a monoid and $w, v, \tilde{v} \in \mathcal{M}$ such that v is a prefix of w as a word, i.e., $w \equiv vu$ for some $u \in \mathcal{M}$, then $v \succ \tilde{v}$ implies $vu \succ \tilde{v}u \succeq \tilde{v} \circ u$. On the other hand, if $\mathcal{M}$ is a commutative monoid, $w \geq_{\text{tup}} v$ and $w = v \circ_T u$, then similarly $v \succ \tilde{v}$ implies $w = v \circ_T u \succ \tilde{v} \circ_T u \succeq \tilde{v} \circ u$. In chapter 4 these properties were used to characterize appropriate Gröbner bases by special s-polynomials. We will now give a similar approach by introducing special standard representations and a reduction corresponding to "prefixes" in the set of ordered group words defined by the extended tuple-ordering.

Definition 5.5.5
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. A representation

$$p = \sum_{i=1}^{n} \alpha_i \cdot f_i * w_i, \quad \text{with } \alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{G}$$

is called a **quasi-commutative (qc-)standard representation** in case for all $1 \leq i \leq n$ we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ w_i \succeq \mathsf{HT}(f_i * w_i)$ and $\mathsf{HT}(f_i * w_i) \geq_{\text{tup}} \mathsf{HT}(f_i)$. $\diamond$

Definition 5.5.6
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{G}]$. We say f **quasi-commutatively (right) reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{qc}}_{f} q$, if

(a) $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, and

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

We write $p \longrightarrow^{\mathrm{qc}}_{f}$ if there is a polynomial q as defined above and p is then called quasi-commutatively reducible by f. Further we can define $\xrightarrow{*}^{\mathrm{qc}}$, $\xrightarrow{+}^{\mathrm{qc}}$, $\xrightarrow{n}^{\mathrm{qc}}$ as usual. Quasi-commutative reduction by a set $F \subseteq \mathbf{K}[\mathcal{G}]$ is denoted by $p \longrightarrow^{\mathrm{qc}}_{F} q$ and abbreviates $p \longrightarrow^{\mathrm{qc}}_{f} q$ for some $f \in F$, which is also written as $p \longrightarrow^{\mathrm{qc}}_{f \in F} q$. $\diamond$

Notice that if f quasi-commutatively reduces p at $\alpha \cdot t$ to q, then $t \notin \mathsf{T}(q)$. This reduction is effective, as it is possible to decide, whether $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$. Further it is Noetherian, as by lemma 5.5.3, $p \longrightarrow^{\mathrm{qc}}_{f} q$ implies $p > q$.

For a commutative group $\mathcal{G}$, quasi-commutative right reduction and commutative reduction coincide as follows: For $w, v \in \mathcal{G}$, $w \geq_{\mathrm{tup}} v$ implies $v \circ_{\mathcal{T}} u = w$ where $u = \mathsf{inv}(v) \circ w$ and on the other hand $v \circ_{\mathcal{T}} u = w$ implies $w \geq_{\mathrm{tup}} v$.

Furthermore, the translation lemma holds.

Lemma 5.5.7
Let F be a set of polynomials in $\mathbf{K}[\mathcal{G}]$ and $p, q, h \in \mathbf{K}[\mathcal{G}]$ some polynomials.

1. *Let $p - q \longrightarrow^{\mathrm{qc}}_{F} h$. Then there are $p', q' \in \mathbf{K}[\mathcal{G}]$ such that $p \xrightarrow{*}^{\mathrm{qc}}_{F} p'$, $q \xrightarrow{*}^{\mathrm{qc}}_{F} q'$ and $h = p' - q'$.*

2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow^{\mathrm{qc}}_{F}$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{G}]$ such that $p \xrightarrow{*}^{\mathrm{qc}}_{F} g$ and $q \xrightarrow{*}^{\mathrm{qc}}_{F} g$.*

Proof :

1. Let $p - q \longrightarrow^{\mathrm{qc}}_{F} h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*, f \in F, w \in \mathcal{G}$ and $\mathsf{HT}(f) \circ w = t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, i.e. $\alpha \cdot \mathsf{HC}(f)$ is the coefficient of t in $p - q$. We have to distinguish three cases:

   (a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$: Then we can eliminate the term t in the polynomials p respectively q by qc-reduction. We then get $p \longrightarrow^{\mathrm{qc}}_{f} p - \alpha_1 \cdot f * w = p'$ and $q \longrightarrow^{\mathrm{qc}}_{f} q - \alpha_2 \cdot f * w = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f)$ and $\alpha_2 \cdot \mathsf{HC}(f)$ are the coefficients of t in p respectively q.

(b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$: Then we can eliminate the term t in the polynomial p by qc-reduction and get $p \longrightarrow^{\mathrm{qc}}_{f} p - \alpha \cdot f * w = p'$ and $q = q'$.

(c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$: Then we can eliminate the term t in the polynomial q by qc-reduction and get $q \longrightarrow^{\mathrm{qc}}_{f} q + \alpha \cdot f * w = q'$ and $p = p'$.

In all cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

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

q.e.d.

Let us continue by defining Gröbner bases with respect to quasi-commutative reduction.

Definition 5.5.8
A set $G \subseteq \mathbf{K}[\mathcal{G}]$ is said to be a **(right) Gröbner basis** with respect to $\longrightarrow^{\mathrm{qc}}$ or a **quasi-commutative Gröbner basis**, if

(i) $\xleftrightarrow{*}^{\mathrm{qc}}_{G} \;=\; \equiv_{\mathsf{ideal}_r(G)}$, and

(ii) $\longrightarrow^{\mathrm{qc}}_{G}$ is confluent. $\diamond$

As before, when weakening our reduction we have to do saturation to express the right ideal congruence. Reviewing our previous approaches to saturation, we can restrict saturation for a polynomial p in a torsion-free nilpotent group ring to computing appropriate representatives for the sets Y_t, $t \in \mathsf{T}(t)$ as specified in definition 4.3.20 (compare procedure SATURATION 2 on page 4.3). We show that it is decidable whether Y_t is empty and how in case $Y_t \neq \emptyset$ a representative for Y_t can be constructed, in particular that we can construct a polynomial $q \in Y_t$ such that for all $q' \in Y_t$ we have $q' \longrightarrow^{\mathrm{qc}}_{q} 0$. First let us look at an example to illustrate how a term can be brought into head position and what candidates are likely to cause such a situation.

Example 5.5.9
Let $\mathcal{G}$ be the free nilpotent group of class 2 with 2 generators with the CNI-presentation (Σ, T) given in example 5.5.2. Further let us take a look at the polynomial $p = a_1^{-1}a_2^2a_3^3 + a_1^{-1}a_2a_3^{-2} + a_1^{-1}a_2a_3$. where the term $t \equiv a_1^{-1}a_2a_3$ is the one to be brought in head position. For $w \equiv a_1a_2^{-2}a_3$ we get $p * w = a_3^5 + a_2^{-1} + \underline{a_2^{-1}a_3^3}$, i.e., $Y_t \neq \emptyset$ as $\mathsf{HT}(p * w) = t \circ w$. Now all terms in p start with the prefix a_1^{-1} and the distinguishing letter between the head term $a_1^{-1}a_2^2a_3^3$ of p and the term $t \equiv a_1^{-1}a_2a_3$ is a_2. Notice that in order to bring the latter term into head position one has to change the occurrence of a_2. One idea might be to split w into a prefix in the letters smaller than the distinguishing letter a_2 and a remaining part in $\mathsf{ORD}(\Sigma_2)$, i.e., $w \equiv w'w''$ with $w' \equiv a_1$, $w'' \equiv a_2^{-2}a_3$.

Let us now look at $p * w''$. We get $p * w'' = a_1^{-1}a_3^4 + \underline{a_1^{-1}a_2^{-1}a_3^{-1}} + a_1^{-1}a_2^{-1}a_3^2$ and unfortunately $\mathsf{HT}(p*w'') \neq t \circ w''$. This is due to the fact that although multiplication with a_1 is the same on the prefix a_1^{-1} for all three terms, it does have influence on the remaining part of the terms as multiplication is not commutative[17]. On the other hand there is an element in $\mathsf{ORD}(\Sigma_2)$ that can bring t into head position, namely $v \equiv a_2^{-2}a_3^2$. We get $p * v = a_1^{-1}a_3^5 + a_1^{-1}a_2^{-1} + \underline{a_1^{-1}a_2^{-1}a_3^3}$. $\diamond$

The next lemma shows that if a term can be brought into head position in a polynomial by right multiplication with a group element, then there is a group element of a special form that will also do. Since this special element will only depend on the polynomial and is given in a constructive way, we then can decide whether there exists such an element and if this is not the case the term cannot be brought into head position.

Lemma 5.5.10
Let (Σ, T) be a convergent CNI-presentation of a group $\mathcal{G}$ and p a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. In case there exists an element $w \in \mathcal{G}$ such that $\mathsf{HT}(p * w) = t \circ w$ for some $t \in \mathsf{T}(p)$, let a_d is the distinguishing letter between t and $\mathsf{HT}(p)$. Then one can construct an element $v \in \mathsf{ORD}(\Sigma_d)$ such that $\mathsf{HT}(p * v) = t \circ v$.

Proof :
We show that for all polynomials $q \in \{p * u | u \in \mathcal{G}\}$ the following holds: In case $\mathsf{HT}(q * w) = t_i \circ w$ for some $w \in \mathcal{G}$, $t_i \in \mathsf{T}(q)$ then one can construct an element $v \in \mathsf{ORD}(\Sigma_d)$ where a_d is the distinguishing letter between t_i and $\mathsf{HT}(q)$, and $\mathsf{HT}(q*v) = t_i \circ v$. This will be done by induction on k where $d = n - k$. In the base case let $k = 0$, i.e., a_n is the distinguishing letter between $\mathsf{HT}(q) = t_1 \equiv a_1^{1_1} \ldots a_n^{1_n}$ and $t_i \equiv a_1^{i_1} \ldots a_n^{i_n}$. Hence $1_j = i_j$ for all $1 \leq j \leq n-1$ and $1_n >_{\mathbf{Z}} i_n$. By our assumption there exists $w \in \mathcal{G}$ such that $\mathsf{HT}(q * w) = t_i \circ w$, with $w \equiv w' a_n^{w_n}$, $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_n)$, and there exist $k_1, \ldots, k_{n-1}, x \in \mathbf{Z}$ such that $t_1 \circ w = a_1^{1_1} \ldots a_n^{1_n} \circ w = a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w \circ a_n^{1_n} = (a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w') \circ a_n^{1_n + w_n} \equiv a_1^{k_1} \ldots a_{n-1}^{k_{n-1}} a_n^{1_n + x}$ and $t_i \circ w = a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} a_n^{i_n} \circ w = a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w \circ a_n^{i_n} = (a_1^{1_1} \ldots a_{n-1}^{1_{n-1}} \circ w') \circ a_n^{i_n + w_n} \equiv a_1^{k_1} \ldots a_{n-1}^{k_{n-1}} a_n^{i_n + x}$. Thus $1_n + x <_{\mathbf{Z}} i_n + x$ must hold. Let us set $v \equiv a_n^{-1_n}$. We show that for all $t_j \in T(q) \backslash \{t_i\}$ we have $t_i \circ v \succ t_j \circ v$. Note that for all t_j with prefix $a_1^{j_1} \ldots a_{n-1}^{j_{n-1}} \prec a_1^{1_1} \ldots a_{n-1}^{1_{n-1}}$ we have $t_j \circ v \prec t_i \circ v$, as right multiplication with v only changes the exponent of a_n in the respective term. It remains to look at those terms t_j with $a_1^{j_1} \ldots a_{n-1}^{j_{n-1}} \equiv a_1^{1_1} \ldots a_{n-1}^{1_{n-1}}$. Hence, let us assume that there exists a term t_j such that $t_j \circ v \succ t_i \circ v$, i.e., $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n$. Since $\mathsf{HT}(q * w) = t_i \circ w$ we know $j_n + x <_{\mathbf{Z}} i_n + x$ and $1_n + x <_{\mathbf{Z}} i_n + x$. Furthermore, as $t_1 = \mathsf{HT}(q)$ we have $1_n >_{\mathbf{Z}} i_n$ and $1_n >_{\mathbf{Z}} j_n$. We prove that $t_j \circ v \succ t_i \circ v$ yields $j_n + x >_{\mathbf{Z}} i_n + x$ contradicting our assumption by analysing the possible cases for these exponents. First suppose that $1_n < 0$ and thus $1_n + x <_{\mathbf{Z}} i_n + x$ implies $x \geq |1_n| > 0$. Then in case $i_n \leq 0$ this gives us $|1_n| > |i_n|$. Now $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n > 0$ and $j_n - 1_n > 0$ yields either $j_n > 0$ or ($j_n \leq 0$ and $|j_n| < |i_n|$), both implying $j_n + y > i_n + y$ for all $y \geq |1_n|$, especially for $y = x$. In case $i_n > 0$ as before $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n > 0$,

[17] For C-presentations w'' is the appropriate candidate to bring t into head position.

$j_n - 1_n > 0$ imply $j_n > i_n$ and for all $y \geq |1_n|$ we get $j_n + y > i_n + y$, especially for $y = x$. Hence let us assume that $1_n > 0$ and thus $1_n + x <_{\mathbf{Z}} i_n + x$ implies $x < 0$ and $|x| > i_n$, since $1_n > i_n \geq 0$ and $1_n > j_n \geq 0$. Now $j_n - 1_n >_{\mathbf{Z}} i_n - 1_n$ and $i_n - 1_n < 0$ imply $j_n - 1_n < 0$ and $|i_n - 1_n| < |j_n - 1_n|$. Hence we get $j_n < i_n$ and for all $y < 0$ with $|y| > j_n$ we have $j_n + y >_{\mathbf{Z}} i_n + y$, especially for $y = x$ as $|x| > i_n > j_n$.

In the induction step let us assume that for all polynomials $q \in \{p * u | u \in \mathcal{G}\}$ and $w \in \mathcal{G}$ with $\mathsf{HT}(q * w) = t_i \circ w$, if the distinguishing letter a_d between $\mathsf{HT}(q)$ and t_i has index $d \geq n - (k-1)$ there exists an element $v \in \mathsf{ORD}(\Sigma_d)$ such that $\mathsf{HT}(q * v) = t_i \circ v$. Now for $q \in \{p * u | u \in \mathcal{G}\}$, $w \in \mathcal{G}$ with $\mathsf{HT}(q * w) = t_i \circ w$ let us assume that the distinguishing letter between $\mathsf{HT}(q)$ and t_i has index $d = n - k$. Since $\mathsf{HT}(q * w) = t_i \circ w$, for $w \equiv w' a_d^{w_d} w''$ with $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_d)$, $w'' \in \mathsf{ORD}(\Sigma_{d+1})$, we know that there exist $k_1, \ldots, k_{d-1}, x \in \mathbf{Z}$ and $z_1, z_i, \tilde{z}_1 \in \mathsf{ORD}(\Sigma_{d+1})$ such that $t_1 \circ w = a_1^{1_1} \ldots a_n^{1_n} \circ w = a_1^{1_1} \ldots a_{d-1}^{1_{d-1}} \circ w' \circ a_d^{1_d} \circ \tilde{z}_1 \equiv a_1^{k_1} \ldots a_{d-1}^{k_{d-1}} a_n^{1_d + x} z_1$ and similarly $t_i \circ w = a_1^{k_1} \ldots a_{d-1}^{k_{d-1}} a_n^{i_d + x} z_i$. As $1_d \neq i_d$ then $1_d + x <_{\mathbf{Z}} i_d + x$ must hold and we can set $v \equiv a_n^{-1_d}$. We have to show that for all $t_j \in T(q) \backslash \{t_i\}$ we have $t_i \circ v \succ t_j \circ v$. Note that for all t_j with prefix $a_1^{j_1} \ldots a_{d-1}^{j_{d-1}} \prec a_1^{1_1} \ldots a_{d-1}^{1_{d-1}}$ we have $t_j \circ v \prec t_i \circ v$, as right multiplication with v has no influence on the prefix in $\mathsf{ORD}(\Sigma \backslash \Sigma_d)$. Therefore, it remains to look at those terms t_j with $a_1^{j_1} \ldots a_{d-1}^{j_{d-1}} \equiv a_1^{1_1} \ldots a_{d-1}^{1_{d-1}}$. Let us assume that there exists a term t_j such that $t_j \circ v \succ t_i \circ v$, i.e., $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d$. We will show that then $j_d = i_d$ and hence our induction hypothesis can be applied since for the polynomial $q * v$ the distinguishing letter between $\mathsf{HT}(q * v)$ and $t_i \circ v$ is of index $d' > d = n - k$ and by our assumption there exists $\mathsf{inv}(v) \circ w \in \mathcal{G}$ such that $\mathsf{HT}((q * v) * (\mathsf{inv}(v) \circ w)) = \mathsf{HT}(q * w) = t_i \circ w = t_i \circ (\mathsf{inv}(v) \circ w)$. We know $j_d + x \leq_{\mathbf{Z}} i_d + x$ and $1_d + x <_{\mathbf{Z}} i_d + x$ since $\mathsf{HT}(q * w) = t_i \circ w$. Next we prove that $t_j \circ v \succ t_i \circ v$ implies $j_d = i_d$ by analysing the possible cases. First suppose that $1_d < 0$ and thus $1_d + x <_{\mathbf{Z}} i_d + x$ implies $x \geq |1_d| > 0$. Then in case $i_d \leq 0$ this gives us $|1_d| > |i_d|$. Now $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d > 0$ and $j_d - 1_d > 0$ yield either $j_d > 0$ or ($j_d \leq 0$ and $|j_d| \leq |i_d|$), both implying $j_d + y \geq i_d + y$ for all $y \geq |1_d|$. Thus as $x \geq |1_d|$ we get $j_d + x \geq i_d + x$ yielding $j_d = i_d$. In case $i_d > 0$ as before $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d > 0$, $j_d - 1_d > 0$ yield $j_d \geq i_d$ and for all $y \geq |1_n|$ we get $j_d + y \geq i_d + y$. Thus as $x \geq |1_d|$, $j_d + x \geq i_d + x$ again yields $j_d = i_d$. Therefore, let us assume that $1_d > 0$ and thus $1_d + x <_{\mathbf{Z}} i_d + x$ implies $x < 0$ and $|x| > i_d$, since $1_d > i_d \geq 0$ and $1_d \geq j_d \geq 0$. Now $j_d - 1_d \geq_{\mathbf{Z}} i_d - 1_d$ and $i_d - 1_d < 0$ imply $j_d - 1_d < 0$ and $|i_d - 1_d| \leq |j_d - 1_d|$. Hence we get $j_d \leq i_d$ and for all $y < 0$ with $|y| > j_d$, we have $j_d + y \geq_{\mathbf{Z}} i_d + y$. Thus as $|x| > i_d \geq j_d$, then $j_d + x \geq_{\mathbf{Z}} i_d + x$ yields $j_d = i_d$.

q.e.d.

Corollary 5.5.11
Let (Σ, T) be a convergent CNI-presentation of a group $\mathcal{G}$ and p a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. Then it is decidable whether $Y_t \neq \emptyset$ for some $t \in \mathsf{T}(p)$.

Proof :
The proof of lemma 5.5.10 can be turned into a procedure which, given a polynomial $p \in \mathbf{K}[\mathcal{G}]$ and a term $t \in \mathsf{T}(p)$, tries to compute a representative of Y_t. This can be done by starting with the distinguishing letter between t and $\mathsf{HT}(p)$ and proceeding to compute an appropriate $v \in \mathsf{ORD}(\Sigma_d)$ if possible. Remember that for each modification step the multiple is defined by the exponent of the distinguishing letter of the respective polynomial. Hence let $p_0 = p$, $t_0 = t$ and d_0 be the index of the distinguishing letter between $\mathsf{HT}(p_0)$ and t_0 and further let i_0 be the exponent of a_{d_0} in the term $\mathsf{HT}(p_0)$. Now proceed for p_j, t_j, d_j and $v_j \equiv a_{d_j}^{-i_j}$, $j \geq 0$ as follows: If the exponent of a_{d_j} in $\mathsf{HT}(p_j * v_j)$ differs from its exponent in $t_j \circ v_j$ then t_j cannot be brought to head position. If $\mathsf{HT}(p_j * v_j) = t_j \circ v_j$ then we are done. Else we set $p_{j+1} = p_j * v_j$, $t_{j+1} = t_j \circ v_j$ and $i_{j+1} > i_j$ is the index of the distinguishing letter between $\mathsf{HT}(p_{j+1})$ and t_{j+1}.
Now either we find that t cannot be brought to head position or for some $0 \leq k < n$ we have $v \equiv v_0 \dots v_k$.

q.e.d.

Hence we can compute a saturating set for a polynomial in a torsion-free nilpotent group ring with respect to right reduction. We will now move on to show how these polynomials can be modified in order to compute a saturating set with respect to quasi-commutative reduction.

Definition 5.5.12
A set of polynomials $F \subseteq \{\alpha \cdot p * w | \alpha \in \mathbf{K}, w \in \mathcal{G}\}$ is called a **quasi-commutatively saturating set** for a polynomial $p \in \mathbf{K}[\mathcal{G}]$, if for all $\alpha \in \mathbf{K}^*$, $w \in \mathcal{G}$, $\alpha \cdot p * w \longrightarrow_F^{\mathrm{qc}} 0$ holds. $\mathcal{SAT}_{qc}(p)$ denotes the family of all quasi-commutatively saturating sets for p. We call a set $F \subseteq \mathbf{K}[\mathcal{G}]$ **quasi-commutatively saturated**, if for all $f \in F$, $\alpha \in \mathbf{K}^*$, $w \in \mathcal{G}$, we have $\alpha \cdot f * w \longrightarrow_F^{\mathrm{qc}} 0$. ◇

Important is that quasi-commutative saturated sets allow special representations.

Lemma 5.5.13
Let F be a quasi-commutatively saturated set of polynomials in $\mathbf{K}[\mathcal{G}]$. Then every non-zero polynomial $g \in \mathsf{ideal}_r(F)$ has a representation $g = \sum_{i=1}^{k} \alpha_i \cdot f_i * w_i$, where $\alpha_i \in \mathbf{K}^*, f_i \in F, w_i \in \mathcal{G}$, $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ w_i$ and $\mathsf{HT}(f_i * w_i) \geq_{\mathrm{tup}} \mathsf{HT}(f_i)$. □

For a polynomial p and a term $t \in \mathsf{T}(p)$ we call a term s in a multiple $p * w$ a **t-term**, if $s = t \circ w$. The following lemma states that if in two multiples of a polynomial the head terms result from the same term t, then there is also a multiple of the polynomial with a t-term as head term which is in some sense a greatest common divisor of the head terms of the original two polynomials. This leads to the existence of one representative for each t-term occurring as a head term comparable to the existence of a unique minimal element in the set Y_t with respect to the ordering $<_{\mathrm{tup}}$ which is not obvious, as $<_{\mathrm{tup}}$ is no total ordering.

Lemma 5.5.14
Let (Σ, T) be a convergent CNI-presentation of a group $\mathcal{G}$. Further let $p * u$ and $p * v$ be two multiples of a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ such that for some term $t \in \mathsf{T}(p)$ the head terms are t-terms, i.e., $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \ldots a_n^{j_n}$. Then there exists a term $\tilde{t} \leq_{\mathrm{tup}} a_1^{\rho_1} \ldots a_n^{\rho_n}$ where

$$\rho_l = \begin{cases} \mathsf{sgn}(i_l) \cdot \min\{|i_l|, |j_l|\} & \mathsf{sgn}(i_l) = \mathsf{sgn}(j_l) \\ 0 & \textit{otherwise} \end{cases}$$

and an element $\tilde{z} \in \mathcal{G}$ such that $\mathsf{HT}(p * \tilde{z}) = t \circ \tilde{z} = \tilde{t}$.

Proof :
Let p, $p * u$ and $p * v$ be as described in the lemma and let $a_1, \ldots, a_n$ be the letters corresponding to our presentation. We show the existence of $\tilde{z}$ by constructing a sequence $z_1, \ldots, z_n \in \mathcal{G}$, such that for $1 \leq l \leq n$ we have $\mathsf{HT}(p*z_l) = t \circ z_l \equiv a_1^{s_1} \ldots a_l^{s_l} r_l$ with $r_l \in \mathsf{ORD}(\Sigma_{l+1})$ and $a_1^{s_1} \ldots a_l^{s_l} \leq_{\mathrm{tup}} a_1^{\rho_1} \ldots a_l^{\rho_l}$. Then for $\tilde{z} = z_n$ our claim holds.
Let us start by constructing an element $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(p * z_1) = t \circ z_1 \equiv a_1^{s_1} r_1$, $r_1 \in \mathsf{ORD}(\Sigma_2)$ and $a_1^{s_1} \leq_{\mathrm{tup}} a_1^{\rho_1}$. In case $i_1 = j_1$ or $j_1 = 0$ we can set $z_1 = v$ and $s_1 = j_1 = \rho_1$ since $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \ldots a_n^{j_n}$. Similarly in case $i_1 = 0$ we can set $z_1 = u$ and $s_1 = i_1 = 0 = \rho_1$ since $\mathsf{HT}(p * u) = t \circ u \equiv a_2^{i_2} \ldots a_n^{i_n} \in \mathsf{ORD}(\Sigma_2)$. Hence let us assume $i_1 \neq j_1$ and both are non-zero. First suppose that $\mathsf{sgn}(i_1) = \mathsf{sgn}(j_1)$. Then if $|i_1| \geq |j_1|$ we again set $z_1 = v$ since for $s_1 = j_1 = \rho_1$ our claim holds. In case $|j_1| > |i_1|$ we set $z_1 = u$ because for $s_1 = i_1 = \rho_1$ our claim holds. Now let us proceed with the case $\mathsf{sgn}(i_1) \neq \mathsf{sgn}(j_1)$, i.e., we construct $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(p*z_1) = t \circ z_1 \in \mathsf{ORD}(\Sigma_2)$ as $\rho_1 = 0$. We claim that the letter a_1 has the same exponent for all terms in $\mathsf{T}(p)$, say b. In case this holds, no term in the polynomial $p * a_1^{-b}$ will contain the letter a_1 and the distinguishing letter between $\mathsf{HT}(p * a_1^{-b})$ and the term $t \circ a_1^{-b}$ is at least of index 2. Furthermore we know $\mathsf{HT}((p * a_1^{-b}) * (a_1^b \circ v)) = \mathsf{HT}(p * v) = t \circ v$. Thus by lemma 5.5.10 there exists an element $r \in \mathsf{ORD}(\Sigma_2)$ such that $\mathsf{HT}((p * a_1^{-b}) * r) = t \circ a_1^{-b} \circ r \in \mathsf{ORD}(\Sigma_2)$ and thus we can set $z_1 = a_1^{-b} r$ and $s_1 = 0 = \rho_1$.
Hence it remains to prove our initial claim. Suppose we have the representations $s' \equiv a_1^{b_{s'}} x_s$, $b_{s'} \in \mathbf{Z}$, $x_{s'} \in \mathsf{ORD}(\Sigma_2)$ for the terms $s' \in \mathsf{T}(p)$ and $\mathsf{HT}(p) = s \equiv a_1^{b_s} x_s$. Then we know $b_s \geq_{\mathbf{Z}} b_t$ since $t \in \mathsf{T}(p)$. Hence in showing that the case $b_s >_{\mathbf{Z}} b_t$ is not possible we find that the exponents of a_1 in s and t are equal. To see this, let us study the possible cases. If $b_s > 0$ we have $b_s > b_t \geq 0$ and hence there exists no $x \in \mathbf{Z}$ such that $b_t + x > b_s + x \geq 0$. On the other hand $b_s < 0$ either implies $b_t > 0$ or $b_t \leq 0$ and $|b_s| > |b_t|$. In both cases there exists no $x \in \mathbf{Z}$ such that $b_t + x < 0$ and $|b_t + x| > |b_s + x|$. Hence $b_t = b_s$ must hold as we know that t can be brought to head position by u respectively v such that the exponents of a_1 in $\mathsf{HT}(p * u)$ respectively $\mathsf{HT}(p * v)$ have different sign. It remains to show that there cannot exist a term $s' \in \mathsf{T}(p)$ with $b_{s'} <_{\mathbf{Z}} b_s = b_t$. Let us assume such an s' exists. Since $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \ldots a_n^{j_n}$ there then must exist $x_1, x_2 \in \mathbf{Z}$ such that $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1 = i_1$ and $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2 = j_1$. Without

loss of generality let us assume $i_1 > 0$ and $j_1 < 0$ (the other case is symmetric). In case $b_t < 0$ we get that $b_t + x_1 = i_1 > 0$ implies $x_1 > |b_t| > 0$. Now, as $b_{s'} <_{\mathbf{Z}} b_t$ either implies $b_{s'} > 0$ or $b_{s'} \leq 0$ and $|b_{s'}| < |b_t|$, we find $b_{s'} + x_1 > b_t + x_1$ contradicting $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1$. On the other hand, in case $b_t > 0$ we know $b_t > b_{s'} \geq 0$. Furthermore, $b_t + x_2 = j_1 < 0$ implies $x_2 < 0$ and $|x_2| > b_t$. Hence we get $b_{s'} + x_2 < 0$ and $|b_{s'} + x_2| > |b_t + x_2|$ contradicting $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2$.

Thus let us assume that for the letter a_{k-1} we have constructed $z_{k-1} \in \mathcal{G}$ such that $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} r_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ with $r_{k-1} \in \mathsf{ORD}(\Sigma_k)$, $r' \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} \leq_{\text{tup}} a_1^{\rho_1} \ldots a_{k-1}^{\rho_{k-1}}$. We now show that we can find $z_k = z_{k-1} \circ \tilde{w} \in \mathcal{G}$ such that $\mathsf{HT}(p * z_k) = t \circ z_k \equiv a_1^{s_1} \ldots a_k^{s_k} r_k$ with $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \ldots a_k^{s_k} \leq_{\text{tup}} a_1^{\rho_1} \ldots a_k^{\rho_k}$. This will be done in two steps. First we show that for the polynomials $p*u$ and $p*z_{k-1}$ with head terms $a_1^{i_1} \ldots a_n^{i_n}$ respectively $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ we can find an element $w_1 \in \mathcal{G}$ such that $\mathsf{HT}(p*z_{k-1}*w_1) = t \circ z_{k-1} \circ w_1 \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$, $\tilde{r} \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{\tilde{s}_k} \leq_{\text{tup}} a_k^{\tilde{\rho}_k}$ with

$$\tilde{\rho}_k = \begin{cases} \mathsf{sgn}(i_k) \cdot \min\{|i_k|, |l_k|\} & \mathsf{sgn}(i_k) = \mathsf{sgn}(l_k) \\ 0 & \text{otherwise.} \end{cases}$$

Then in case $a_k^{\tilde{\rho}_k} \leq_{\text{tup}} a_k^{\rho_k}$ we are done and set $z_k = z_{k-1} \circ w_1$ and $s_k = \tilde{s}_k$. Else we can similarly proceed for the polynomials $p * v$ and $p * z_{k-1} * w_1$ with head terms $a_1^{j_1} \ldots a_n^{j_n}$ respectively $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$ and find an element $w_2 \in \mathcal{G}$ such that for $z_k = z_{k-1} \circ w_1 \circ w_2$ we have $\mathsf{HT}(p * z_k) = t \circ z_k \equiv a_1^{s_1} \ldots a_k^{s_k} r_k$, $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{s_k} \leq_{\text{tup}} a_k^{\tilde{\rho}'_k}$ with

$$\tilde{\rho}'_k = \begin{cases} \mathsf{sgn}(j_k) \cdot \min\{|j_k|, |\tilde{s}_k|\} & \mathsf{sgn}(j_k) = \mathsf{sgn}(\tilde{s}_k) \\ 0 & \text{otherwise.} \end{cases}$$

Then we can conclude $a_k^{s_k} \leq_{\text{tup}} a_k^{\rho_k}$ as in case $s_k = 0$ we are immediately done and otherwise we get $\mathsf{sgn}(j_k) = \mathsf{sgn}(\tilde{s}_k) = \mathsf{sgn}(\tilde{\rho}_k) = \mathsf{sgn}(i_k)$ and $\min\{|i_k|, |\tilde{s}_k|, |j_k|\} \leq \min\{|i_k|, |j_k|\}$.

Let us hence show how to construct w_1. Remember that $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ for some $r' \in \mathsf{ORD}(\Sigma_{k+1})$.

In case $i_k = l_k$ or $l_k = 0$ we can set $w_1 = \lambda$ and $\tilde{s}_k = l_k = \tilde{\rho}_k$ as $\mathsf{HT}(p*z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$. Hence let $i_k \neq l_k$ and $l_k \neq 0$.

First let us assume that $\mathsf{sgn}(i_k) = \mathsf{sgn}(l_k)$. Then in case $|i_k| \geq |l_k|$ we are done by setting $w_1 = \lambda$ as again $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ will do with $\tilde{s}_k = l_k = \tilde{\rho}_k$. Therefore, let us assume that $|l_k| > |i_k|$. Then we consider the multiple $p * z_{k-1} * a_k^{-l_k+i_k}$, i.e., the exponent of the letter a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ will be i_k. If $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k}) = t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ we are done because then $t \circ z_{k-1} \circ a_k^{-l_k+i_k} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}_k$ for some $\tilde{r}_k \in \mathsf{ORD}(\Sigma_{k+1})$ and we can set $w_1 = a_k^{-l_k+i_k}$ and $\tilde{s}_k = i_k = \tilde{\rho}_k$. Otherwise we show that the t-term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ in this multiple can be brought to head position using an element $r \in \mathsf{ORD}(\Sigma_{k+1})$ thus allowing to set $\tilde{s}_k = i_k = \tilde{\rho}_k$ and $w_1 = a_k^{-l_k+i_k} r$ as then we have $\mathsf{HT}(p*z_{k-1}*w_1) = t \circ z_{k-1} \circ w_1 =$

$a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r' \circ a_k^{-l_k+i_k} r \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}$ where $a_k^{l_k} r' \circ a_k^{-l_k+i_k} r \equiv a_k^{i_k} \tilde{r}$[18]. This follows immediately if we can prove that the exponent of a_k in the term $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k}$ is also i_k. Then we can apply lemma 5.5.10 to the polynomial $p * z_{k-1} * a_k^{-l_k+i_k}$ and the term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$. Note that $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ and $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ have then distinguishing letter of at least index $k+1$ and further $\mathsf{HT}((p*z_{k-1}*a_k^{-l_k+i_k})*a_k^{-l_k+i_k}) = \mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1}$. Therefore, we show that the exponent of a_k in the term $\mathsf{HT}(p*z_{k-1}*a_k^{-l_k+i_k})$ is also i_k. Let $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{b_k} r''$ with $r'' \in \mathsf{ORD}(\Sigma_{k+1})$ be the term in $p*z_{k-1}$ that became head term[19], i.e., $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{b_k} r'' \circ a_k^{-l_k+i_k} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{c_k} x \succ a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{i_k} y \equiv t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ for some $x, y \in \mathsf{ORD}(\Sigma_{k+1})$ and therefore $c_k \geq_{\mathbf{Z}} i_k$. Then by lemma 2.4.14 there exist $u_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_{k-1})$ and $u_2 \in \mathsf{ORD}(\Sigma_k)$ such that $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{i_k} y \circ u_1 \equiv a_1^{i_1} \ldots a_{k-1}^{i_{k-1}} a_k^{i_k+f_k} z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{i_k+f_k} z \circ u_2 \equiv a_k^{i_k} a_{k+1}^{i_{k+1}}$, i.e., $u_2 \equiv a_k^{-f_k} u_2'$ for some $u_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Note that the t-term is brought to head position by this multiplication. Now multiplying $\mathsf{HT}(p*z_{k-1}*a_k^{-l_k+i_k})$ by $u_1 u_2$ we find $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{c_k} x \circ u_1 u_2 \equiv a_1^{i_1} \ldots a_{k-1}^{i_{k-1}} a_k^{c_k+f_k-f_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. This gives us $c_k \leq_{\mathbf{Z}} i_k$ and thus $i_k \leq_{\mathbf{Z}} c_k$ yields $c_k = i_k$.

Finally, we have to check the case that $\mathsf{sgn}(i_k) \neq \mathsf{sgn}(l_k)$ and $l_k \neq 0$. Let us take a look at the polynomial $p * z_{k-1} * a_k^{-l_k}$, i.e., the exponent of the letter a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k}$ will be 0. Suppose $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k}) \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{c_k} x$, for some term $s \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{b_s} x_s \in \mathsf{T}(p * z_{k-1})$, $x, x_s \in \mathsf{ORD}(\Sigma_{k+1})$, i.e., $c_k = b_s - l_k$. In case this head term is already the corresponding t-term $t \circ z_{k-1} \circ a_k^{-l_k}$, we are done and we set $w_1 = a_k^{-l_k}$ and $\tilde{s}_k = 0 = \tilde{\rho}_k$. Now if we can show $c_k = 0$, by lemma 5.5.10 the t-term $t \circ z_{k-1} \circ a_k^{-l_k}$ can be brought to head position using an element in $\mathsf{ORD}(\Sigma_{k+1})$ since the distinguishing letter between $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k})$ and the term $t \circ z_{k-1} \circ a_k^{-l_k}$ then has at least index $k+1$ and we know $\mathsf{HT}((p * z_{k-1} * a_k^{-l_k}) * a_k^{l_k}) = \mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1}$. Hence, in showing that $c_k = 0$ we are done. As before there exist $u_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_{k-1})$ and $u_2 \in \mathsf{ORD}(\Sigma_k)$ such that $t \circ z_{k-1} \circ a_k^{-l_k} \circ u_1 u_2 \equiv a_1^{i_1} \ldots a_n^{i_n}$. Remember that this multiplication brings the t-term to head position. Since the exponent of a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k}$ is 0, multiplying $\mathsf{HT}(p*z_{k-1}*a_k^{-l_k})$ by $u_1 u_2$ we find $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{c_k} x \circ u_1 u_2 \equiv a_1^{i_1} \ldots a_{k-1}^{i_{k-1}} a_k^{c_k+i_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. Thus we know $c_k + i_k \leq_{\mathbf{Z}} i_k$. To see that this implies $c_k = 0$ we have to distinguish three cases. Remember that $c_k = b_s - l_k$ and since our head term is an s-term $s \circ a_k^{-l_k}$ for some $s \in \mathsf{T}(p * z_{k-1})$ we know $b_s \leq_{\mathbf{Z}} l_k$. In case $i_k = 0$, we have $c_k \leq_{\mathbf{Z}} 0$ implying $c_k = 0$. In case $i_k > 0$ then $c_k + i_k = b_s - l_k + i_k \leq_{\mathbf{Z}} i_k$ implies $0 \leq b_s - l_k + i_k \leq i_k$. Furthermore, as $l_k < 0$ we have $-l_k + i_k > i_k$ implying $b_s < 0$ and hence $|b_s| \leq |l_k|$. But then $b_s - l_k \geq 0$ and $0 \leq b_s - l_k + i_k \leq i_k$ yields $c_k = b_s - l_k = 0$. On the other hand, $i_k < 0$ and $l_k > 0$ imply $0 \leq b_s \leq l_k$ and hence $b_s - l_k + i_k < 0$ yielding $|b_s - l_k + i_k| \leq |i_k|$. Since $b_s - l_k \leq 0$ this inequation can only hold in case $c_k = b_s - l_k = 0$.

q.e.d.

[18]Note that the product of two elements in $\mathsf{ORD}(\Sigma_i)$ is again an element in $\mathsf{ORD}(\Sigma_i)$.

[19]Note that a candidate in $\mathsf{T}(p * z_{k-1})$ for the head term in $p * z_{k-1} * a_k^{-l_k+i_k}$ must have prefix $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}}$ since $\mathsf{HT}(p*z_{k-1}) \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} r_{k-1}$ and multiplication with $a_k^{-l_k+i_k}$ only involves r_{k-1}.

Corollary 5.5.15
For $p*v$, $p*u$ and $q = p*\tilde{z}$ in the previous lemma we have $p*u \longrightarrow_q^{\mathrm{qc}} 0$ and $p*v \longrightarrow_q^{\mathrm{qc}} 0$.

Proof :
This follows immediately, as for the term $\tilde{t} = \mathsf{HT}(q)$ we have $\tilde{t} \leq_{\mathrm{tup}} \mathsf{HT}(p*u)$ and $\tilde{t} \leq_{\mathrm{tup}} \mathsf{HT}(p*v)$.

q.e.d.

Corollary 5.5.16
Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$ and $t \in \mathsf{T}(p)$ such that $Y_t \neq \emptyset$. Then Y_t contains a polynomial q such that for all $q' \in Y_t$ we have $q' \longrightarrow_q^{\mathrm{qc}} 0$.

Proof :
The set of head terms that are t-terms can be ordered with respect to $\geq_{\mathrm{tup}}$. Now suppose there are two different polynomials $p*u, p*v$ in Y_t, both having minimal head terms with respect to $\geq_{\mathrm{tup}}$. Then lemma 5.5.14 yields $t \circ u = t \circ v$ and hence $u = v$ contradicting our assumption.

q.e.d.

Now quasi-commutatively saturating sets can be constructed by computing the appropriate minimal polynomials for the non-empty sets Y_t.

Procedure: QUASI-COMMUTATIVE SATURATION

Given: A polynomial $p \in \mathbf{K}[\mathcal{G}]$ and
(Σ, T) a convergent CNI-Presentation of $\mathcal{G}$.
Find: $S_{qc} \in \mathcal{SAT}_{qc}(p)$.

for all $t \in \mathsf{T}(p)$ **do**
  $S_t := \emptyset$;
  if $Y_t \neq \emptyset$
    then compute $q = p * w \in Y_t$ as described in lemma 5.5.10
      $H_t := \{s \in \mathcal{G} | \mathsf{HT}(q) \geq_{\mathrm{tup}} s\}$;
      % These are candidates for smaller polynomials in Y_t
      $q := \min\{\{p * (\mathsf{inv}(t) \circ s) \mid s \in H_t\} \cap Y_t\}$;
      $S_t := \{q\}$;
  endif
endfor
$S_{qc} := \bigcup_{t \in \mathsf{T}(p)} S_t$

Quasi-commutative saturation enriches a polynomial p by adding a set of polynomials $S \in \mathcal{SAT}_{qc}(p)$ such that we can substitute $q \longrightarrow_p^{(\mathrm{s,r})} q'$ by $q \longrightarrow_{p' \in S}^{\mathrm{qc}} q'$. Therefore, we have more information on the reduction step than using (strong) right reduction and we define s-polynomials corresponding to this reduction.

Definition 5.5.17
Let p_1, p_2 be two polynomials in $\mathbf{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p_2) \equiv a_1^{j_1} \dots a_n^{j_n}$ with either $i_l = 0$ or $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$. Then setting

$$\rho_l = \begin{cases} \mathsf{sgn}(j_l) & i_l = 0 \\ \mathsf{sgn}(i_l) & \text{otherwise} \end{cases}$$

the situation

$$\mathsf{qclcm}(t_1, t_2) = a_1^{\rho_1 \cdot \max\{|i_1|, |j_1|\}} \dots a_n^{\rho_n \cdot \max\{|i_n|, |j_n|\}} = t_1 \circ w_1 = t_2 \circ w_2$$

for some $w_1, w_2 \in \mathcal{G}$ defines a **quasi-commutative s-polynomial**

$$\mathsf{spol}_{qc}(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w_2.$$

$\diamond$

A quasi-commutative s-polynomial is called non-trivial in case it is non-zero. Furthermore, we get $\mathsf{HT}(\mathsf{spol}_{qc}(p_1, p_2)) \prec \mathsf{qclcm}(t_1, t_2)$ and $\mathsf{HT}(p_i) \leq_{\mathrm{tup}} \mathsf{qclcm}(t_1, t_2)$. Notice that a finite set $F \subseteq \mathbf{K}[\mathcal{G}]$ only gives us finitely many such s-polynomials. As before Gröbner bases cannot be characterized by these s-polynomials alone unless they are quasi-commutatively saturated sets.

Theorem 5.5.18
For a quasi-commutatively saturated set F of polynomials in $\mathbf{K}[\mathcal{G}]$, the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}^{\mathrm{qc}}_F 0$.*
2. *For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}_{qc}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{qc}}_F 0$.*

Proof :
$1 \Longrightarrow 2$: Let $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l$ for $w_k, w_l \in \mathcal{G}$ such that we have an overlap as described in definition 5.5.17. We get the following

$$\mathsf{spol}_{qc}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * w_k - \mathsf{HC}(f_l)^{-1} \cdot f_l * w_l \in \mathsf{ideal}_r(F),$$

and hence $\mathsf{spol}_{qc}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{qc}}_F 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow^{\mathrm{qc}}_F$-reducible to zero. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{qc}}_F h'$ implies $h' \in \mathsf{ideal}_r(F)$. As $\longrightarrow^{\mathrm{qc}}_F$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F) \backslash \{0\}$ is $\longrightarrow^{\mathrm{qc}}_F$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g with $\alpha_j \in \mathbf{K}^*$, $f_j \in F, w_j \in \mathcal{G}$. By lemma 5.5.13 we can assume $\mathsf{HT}(f_i * w_i) = \mathsf{HT}(f_i) \circ w_i \geq_{\mathrm{tup}} \mathsf{HT}(f_i)$. Depending on this representation of g and our well-founded total ordering $>_{\mathrm{syll}}$ on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \dots m\}\}$ and K is the number of polynomials

$f_j * w_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow_F^{\rm qc}$-reducible. So we show that g has a special representation (a standard representation corresponding to quasi-commutative reduction) where all terms are bounded by $\mathsf{HT}(g)$, as this implies that g is top-reducible using F since then $\mathsf{HT}(g) = t$. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' <_{\rm syll} t$ or ($t' = t$ and $K' < K$)[20]. If $t \succ \mathsf{HT}(g)$ there are two polynomials f_k, f_l in the corresponding representation[21] with $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l$ and $t \geq_{\rm tup} \mathsf{HT}(f_k)$,$t \geq_{\rm tup} \mathsf{HT}(f_l)$. By definition 5.5.17 we then have an s-polynomial $\mathsf{spol}_{qc}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * z_1 - \mathsf{HC}(f_l)^{-1} \cdot f_l * z_2$ such that $t \geq_{\rm tup} \mathsf{HT}(f_k) \circ z_1$, $t \geq_{\rm tup} \mathsf{HT}(f_l) \circ z_2$ and $\mathsf{HT}(f_k) \circ w_k = \mathsf{HT}(f_l) \circ w_l = \mathsf{HT}(f_k) \circ z_1 \circ w = \mathsf{HT}(f_l) \circ z_2 \circ w$ for some $z_1, z_2, w \in \mathcal{G}$. Let us assume $\mathsf{spol}_{qc}(f_k, f_l) \neq 0$[22]. Hence, $\mathsf{spol}_{qc}(f_k, f_l) \overset{*}{\longrightarrow}{}_F^{\rm qc} 0$ implies $\mathsf{spol}_{qc}(f_k, f_l) = \sum_{i=1}^n \delta_i \cdot h_i * v_i, \delta_i \in \mathbf{K}^*, h_i \in F, v_i \in \mathcal{G}$, where the h_i are due to the reduction of the s-polynomial and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}_{qc}(f_k, f_l))$. Since $t \geq_{\rm tup} \mathsf{HT}(f_k) \circ z_1$ and $t = \mathsf{HT}(f_k) \circ z_1 \circ w$ by lemma 5.5.3 we can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^n \delta_i \cdot h_i * v_i * w$. We can assume that this representation is of the required form, as we can substitute all polynomials h_i violating $\mathsf{HT}(h_i * v_i * w_k) \not\geq_{\rm tup} \mathsf{HT}(h_i)$ without increasing t or K. This gives us:

$$\begin{aligned}
& \alpha_k \cdot f_k * w_k + \alpha_l \cdot f_l * w_l \\
= \;& \alpha_k \cdot f_k * w_k + \underbrace{\alpha_l' \cdot \beta_k \cdot f_k * w_k - \alpha_l' \cdot \beta_k \cdot f_k * w_k}_{=0} + \alpha_l' \cdot \beta_l \cdot f_l * w_l \\
= \;& (\alpha_k + \alpha_l' \cdot \beta_k) \cdot f_k * w_k - \alpha_l' \cdot \underbrace{(\beta_k \cdot f_k * w_k - \beta_l \cdot f_l * w_l)}_{=\mathsf{spol}_{qc}(f_k, f_l) * w} \\
= \;& (\alpha_k + \alpha_l' \cdot b_k) \cdot f_k * w_k - \alpha_l' \cdot (\sum_{i=1}^n \delta_i \cdot h_i * v_i * w) \qquad (5.2)
\end{aligned}$$

where $\beta_k = \mathsf{HC}(f_k)^{-1}$, $\beta_l = \mathsf{HC}(f_l)^{-1}$ and $\alpha_l' \cdot \beta_l = \alpha_l$. By substituting (5.2) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

q.e.d.

Due to Dickson's lemma finite quasi-commutative Gröbner bases exist.

Lemma 5.5.19
Let $\mathcal{G}$ be a nilpotent group with a convergent CNI-presentation. Then every Gröbner basis with respect to $\longrightarrow^{\rm qc}$ of a finitely generated right ideal contains a finite one.

[20] Note that this ordering is well-founded since $>_{\rm syll}$ is and $K \in \mathbf{N}$.

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

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

Proof :
Let F be a finite subset of $\mathbf{K}[\mathcal{G}]$ and G a infinite Gröbner basis of $\mathsf{ideal}_r(F)$ with respect to quasi-commutative reduction. Further let $H = \{\mathsf{HT}(g) \mid g \in G\} \subseteq \mathcal{G}$. Then for every polynomial $f \in \mathsf{ideal}_r(F)$ there exists a term $t \in H$ such that $\mathsf{HT}(f) \geq_{\mathrm{tup}} t$. Each element of H can be viewed as an n-tuples over $\mathbf{Z}$ as it is presented by an ordered group word. But we can also view it as a 2n-tuples over $\mathbf{N}$ by representing each element $u \in H$ by an extended ordered group word $u \equiv a_1^{-i_1} a_1^{j_1} \ldots a_n^{-i_n} a_n^{j_n}$, where $i_l, j_l \in \mathbf{N}$ and the representing 2n-tuple is $(i_1, j_1, \ldots, i_n, j_n)$. Notice that at most one of the two exponents i_l and j_l is non-zero. Now H can be considered as a (possibly infinite) subset of a free commutative monoid $\mathcal{T}_{2n}$ with $2 \cdot n$ generators. Thus by Dickson's lemma there exists a finite subset B of H such that for every $w \in H$ there is a $b \in B$ with $w = b \circ_{\mathcal{T}_{2n}} u$ for some $u \in \mathcal{T}_{2n}$, and hence $w \geq_{\mathrm{tup}} b$. Now we can use the set B to distinguish a finite Gröbner basis in G as follows. To each term $t \in B$ we can assign a polynomial $g_t \in G$ such that $\mathsf{HT}(g_t) = t$. Then the set $G_B = \{g_t \mid t \in B\}$ is again a Gröbner basis with respect to quasi-commutative reduction since for every polynomial $f \in \mathsf{ideal}_r(F)$ there still exists a polynomial g_t now in G_B such that $\mathsf{HT}(f) \geq_{\mathrm{tup}} \mathsf{HT}(g_t) = t$. Hence all polynomials in $\mathsf{ideal}_r(F)$ are quasi-commutatively reducible to zero using G_B.

q.e.d.

Finite Gröbner bases with respect to $\longrightarrow^{\mathrm{qc}}$ can now be computed as follows:

Procedure: Quasi-Commutative Gröbner Bases

Given: A finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$.
Find: $\mathrm{GB}(F)$, a quasi-commutative Gröbner basis of $\mathsf{ideal}_r(F)F$.
Using: SAT_{qc} a quasi-commutatively saturating procedure for polynomials.

$G := \bigcup_{f \in F} \mathrm{SAT}_{qc}(f)$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do**
  % Test if statement 2 of theorem 5.5.18 is valid
  $(q_1, q_2) := \mathrm{remove}(B)$;
  % Remove an element using a fair strategy
  if $\mathsf{spol}_{qc}(q_1, q_2)$ exists
    % The s-polynomial is not trivial
    then $h := \mathrm{normalform}(\mathsf{spol}_{qc}(q_1, q_2), \longrightarrow_G^{\mathrm{qc}})$;
      % Compute a normal form using quasi-commutative reduction
      if $h \neq 0$
        % Statement 2 of theorem 5.5.18 does not hold
        then $G := G \cup \mathrm{SAT}_{qc}(h)$;
          % G is quasi-commutatively saturated
          $B := B \cup \{(f, \tilde{h}), (\tilde{h}, f) \mid f \in G, \tilde{h} \in \mathrm{SAT}_{qc}(h)\}$;
      endif
  endif
endwhile

$\textsc{Gb}(F) := G$

It is possible to use the concept of quasi-commutative representations to introduce interreduction to this setting as well.

We will proceed to show how Gröbner bases can be presented for arbitrary nilpotent group rings. As stated in the introductory chapter, a finitely generated arbitrary nilpotent group $\mathcal{G}$ is a group containing a torsion-free subgroup of finite index. Therefore, we can apply the approach used for context free groups to this situation and see how completion in a nilpotent group can be reduced to completion in the torsion-free quotient.

Let our group be given by a torsion-free subgroup subgroup $\mathcal{N}$ with a convergent CNI-presentation $(\Sigma, C \cup I)$ and $\mathcal{E}$ a finite group such that $(\mathcal{E}\backslash\{\lambda\}) \cap \Sigma = \emptyset$ and $\mathcal{G}/\mathcal{N} \cong \mathcal{E}$. Then every element $g \in \mathcal{G}$ can be uniquely expressed in the form $g \equiv ew$ where $e \in \mathcal{G}/\mathcal{N}$ and w is an ordered group word in $\mathcal{N}$. For all $e \in \mathcal{E}$ let $\phi_e : \Sigma \longrightarrow \mathcal{N}$ be a function such that ϕ_λ is the inclusion and for all $a \in \Sigma$, $\phi_e(a) = \mathsf{inv}(e) \circ_{\mathcal{G}} a \circ_{\mathcal{G}} e$. For all $e_1, e_2 \in \mathcal{E}$ let $z_{e_1,e_2} \in \mathcal{N}$ such that $z_{e_1,\lambda} \equiv z_{\lambda,e_1} \equiv \lambda$ and for all $e_1, e_2, e_3 \in \mathcal{E}$ with $e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3$, $e_1 \circ_{\mathcal{G}} e_2 \equiv e_3 z_{e_1,e_2}$. Let $\Gamma = (\mathcal{E}\backslash\{\lambda\}) \cup \Sigma$ and let T contain the sets of rules C and I, and the additional rules:

$$\begin{array}{lcll} e_1e_2 & \longrightarrow & e_3z_{e_1,e_2} & \text{for all } e_1, e_2 \in \mathcal{E}\backslash\{\lambda\}, e_3 \in \mathcal{E} \text{ such that } e_1 \circ_{\mathcal{E}} e_2 =_{\mathcal{E}} e_3, \\ ae & \longrightarrow & e\phi_e(a) & \text{for all } e \in \mathcal{E}\backslash\{\lambda\}, a \in \Sigma. \end{array}$$

Then (Γ, T) is a canonical presentation of $\mathcal{G}$ as an extension of $\mathcal{N}$ by $\mathcal{E}$. The elements of our group $\mathcal{G}$ are words of the form eu where $e \in \mathcal{E}$ and $u \in \mathcal{N}$. We can specify a total well-founded ordering on our group by combining a total well-founded ordering $\succeq_{\mathcal{E}}$ on $\mathcal{E}$ and a syllable ordering $\geq_{\mathrm{syll}}$ on $\mathcal{N}$: Let $e_1u_1, e_2u_2 \in \mathcal{G}$ such that $e_i \in \mathcal{E}$, $u_i \in \mathcal{N}$. Then we define $e_1u_1 \succ e_2u_2$ if and only if $e_1 \succ e_2$ or ($e_1 = e_2$ and $u_1 >_{\mathrm{syll}} u_2$).

For every $e \in \mathcal{E}$ let the mapping $\psi_e : \mathbf{K}[\mathcal{G}] \longrightarrow \mathcal{G}$ be defined by $\psi_e(f) := f * e$ for $f \in \mathbf{K}[\mathcal{G}]$. We now can give a characterization of Gröbner bases by transforming a finite generating set for a right ideal using these finitely many mappings and then applying our results for finitely generated torsion-free nilpotent groups to this modified generating set. We start by modifying quasi-commutative reduction in order to enable a lifting of the characterization of Gröbner bases in terms of special s-polynomials and restricted saturation. The tuple ordering can be extended by setting $e_1u_1 \geq_{\mathrm{tup}} e_2u_2$ if and only if $e_1 = e_2$ and $u_1 \geq_{\mathrm{tup}} u_2$. Similarly the concept of quasi-commutative right reduction is extended.

Definition 5.5.20
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{G}]$. We say f **quasi-commutatively reduces** p to q at a monomial $\alpha \cdot eu$ of p in one step, denoted by $p \longrightarrow^{\mathrm{qc}}_{f} q$, if

(a) $eu \geq_{\mathrm{tup}} eu'$, where $eu' \equiv \mathsf{HT}(f)$, and

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

We write $p \longrightarrow_f^{\mathrm{qc}}$ if there is a polynomial q as defined above and p is then called quasi-commutatively reducible by f. Further we can define $\xrightarrow{*}^{\mathrm{qc}}$, $\xrightarrow{+}^{\mathrm{qc}}$, $\xrightarrow{n}^{\mathrm{qc}}$ as usual. Quasi-commutative reduction by a set $F \subseteq \mathbf{K}[\mathcal{G}]$ is denoted by $p \longrightarrow_F^{\mathrm{qc}} q$ and abbreviates $p \longrightarrow_f^{\mathrm{qc}} q$ for some $f \in F$, which is also written as $p \longrightarrow_{f \in F}^{\mathrm{qc}} q$. ◇

Notice that if f quasi-commutatively reduces p at $\alpha \cdot eu$ to q, then eu is no longer in the set $\mathsf{T}(q)$ and $p > q$.

Definition 5.5.21
Let $\mathcal{H}_1$ be a subgroup of a group $\mathcal{H}_2$ and p a non-zero polynomial in $\mathbf{K}[\mathcal{H}_2] \backslash \{0\}$. A set $S \subseteq \{p * w \mid w \in \mathcal{H}_1\}$ is called a **$\mathcal{H}_1$-quasi-commutatively saturating set** for p, if for all $w \in \mathcal{H}_1$, $p * w \longrightarrow_S^{\mathrm{qc}} 0$ A set of polynomials $F \subseteq \mathbf{K}[\mathcal{H}_2]$ is called a **$\mathcal{H}_1$-quasi-commutatively saturated set**, if for all $f \in F$ and for all $w \in \mathcal{H}_1$, $f * w \longrightarrow_F^{\mathrm{qc}} 0$. ◇

Applying this definition to the subgroup $\mathcal{N}$ of $\mathcal{G}$ we find that the essential lemmata 5.5.10 and 5.5.13 for describing and computing saturating sets in torsion-free nilpotent groups can be applied to describe $\mathcal{N}$-quasi-commutatively saturating sets. The definition of s-polynomials can be extended by demanding that the $\mathcal{E}$ part of the head terms must coincide.

Definition 5.5.22
Let p_1, p_2 be two polynomials in $\mathbf{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv e a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p_2) \equiv e a_1^{j_1} \ldots a_n^{j_n}$ with either $i_l = 0$ or $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$. Setting

$$\rho_l = \begin{cases} \mathsf{sgn}(j_l) & i_l = 0 \\ \mathsf{sgn}(i_l) & \text{otherwise} \end{cases}$$

the situation

$$e a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}} = t_1 \circ w_1 = t_2 \circ w_2$$

for some $w_1, w_2 \in \mathcal{N}$ defines a **quasi-commutative s-polynomial**

$$\mathsf{spol}_{qc}(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot p_1 * w_1 - \mathsf{HC}(p_2)^{-1} \cdot p_2 * w_2.$$

◇

We can now give a characterization of Gröbner bases in this setting. Notice that $\mathsf{HT}(p_i) \leq_{\mathrm{tup}} e a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$ for $i \in \{1, 2\}$ holds in case such an s-polynomial exists. Furthermore, if there exists a term t such that $t \geq_{\mathrm{tup}} \mathsf{HT}(p_1) \equiv e a_1^{i_1} \ldots a_n^{i_n}$ and $t \geq_{\mathrm{tup}} \mathsf{HT}(p_2) \equiv e a_1^{j_1} \ldots a_n^{j_n}$ an s-polynomial always exists[23] and we even have $t \geq_{\mathrm{tup}} e a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$. For every $e \in \mathcal{E}$ let the mapping $\psi_e : \mathbf{K}[\mathcal{G}] \longrightarrow \mathbf{K}[\mathcal{G}]$ be defined by $\psi_e(f) = f * e$ for $f \in \mathbf{K}[\mathcal{G}]$. We now can give a characterization of a right Gröbner basis in a familiar way after transforming a generating set for the right ideal using these mappings.

[23]Notice that the condition for the existence of an s-polynomial is fulfilled as the tuple-ordering requires that the exponent of a letter a_i in the smaller term is either zero or has the same sign as the exponent of a_i in the tuple-larger term.

Theorem 5.5.23
Let $F, G \subseteq \mathbf{K}[\mathcal{G}]$ such that

(i) $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$

(ii) $\{\psi_e(f) \mid f \in F, e \in \mathcal{E}\} \subseteq G$

(iii) *G is $\mathcal{N}$- saturated.*

Then the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}^{\mathrm{qc}}_{G} 0$.*
2. *For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow{*}^{\mathrm{qc}}_{G} 0$.*

Proof :
$1 \Longrightarrow 2$: By definition 5.5.22 in case for $f_k, f_l \in G$ the s-polynomial exists we get

$$\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * w_1 - \mathsf{HC}(f_l)^{-1} f_l * w_2 \ \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F),$$

and then $\mathsf{spol}(f_k, f_l) \xrightarrow{*}^{\mathrm{qc}}_{G} 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(F)$ is $\longrightarrow^{\mathrm{qc}}_{G}$-reducible to zero. Without loss of generality we assume that G contains no constant polynomials, as then we are done at once. Remember that for $h \in \mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$, $h \longrightarrow^{\mathrm{qc}}_{G} h'$ implies $h' \in \mathsf{ideal}_r(G) = \mathsf{ideal}_r(F)$. Thus as $\longrightarrow^{\mathrm{qc}}_{G}$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is $\longrightarrow^{\mathrm{qc}}_{G}$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{G}$. Further for all $1 \leq j \leq m$, let $w_j \equiv e_j u_j$, with $e_j \in \mathcal{E}$, $u_j \in \mathcal{N}$. Then, we can modify our representation of g to $g = \sum_{j=1}^{m} \alpha_j \cdot \psi_{e_j}(f_j) * u_j$. Since G is $\mathcal{N}$-saturated and $\psi_{e_j}(f_j) \in G$ by definition 5.5.12 there exists $g_j \in G$ such that $\psi_{e_j}(f_j) * u_j \longrightarrow^{\mathrm{qc}}_{g_j} 0$ and hence we can assume $g = \sum_{j=1}^{m} \alpha_j \cdot g_j * v_j$, where $\alpha_j \in \mathbf{K}^*, g_j \in G, v_j \in \mathcal{N}$ and $\mathsf{HT}(g_j * v_j) = \mathsf{HT}(g_j) \circ v_j \geq_{\mathrm{tup}} \mathsf{HT}(g_j)$. Depending on this representation of g and our well-founded total ordering on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(g_j) \circ v_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $g_j * v_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\mathrm{qc}}_{G}$-reducible. Otherwise we show that g has a special representation (a standard representation corresponding to qc-reduction) where all terms are bounded by $\mathsf{HT}(g)$, as this implies that g is top-reducible using G. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$)[24]. In case $t \succ \mathsf{HT}(g)$ there are two polynomials g_k, g_l in the corresponding representation[25] such that $t = \mathsf{HT}(g_k) \circ v_k = \mathsf{HT}(g_l) \circ v_l$ and we have $t \geq_{\mathrm{tup}} \mathsf{HT}(g_k)$,$t \geq_{\mathrm{tup}} \mathsf{HT}(g_l)$. Hence by definition 5.5.22 there exists

[24] Note that this ordering is well-founded since $\geq_{\mathrm{syll}}$ is and $K \in \mathbf{N}$.

[25] Not necessarily $g_l \neq g_k$.

an s-polynomial $\mathsf{spol}(g_k, g_l) = \mathsf{HC}(g_k)^{-1} \cdot g_k * z_1 - \mathsf{HC}(g_l)^{-1} \cdot g_l * z_2$ and $\mathsf{HT}(g_k) \circ v_k = \mathsf{HT}(g_l) \circ v_l = \mathsf{HT}(g_k) \circ z_1 \circ w = \mathsf{HT}(g_l) \circ z_2 \circ w \geq_{\mathrm{tup}} \mathsf{HT}(g_k) \circ z_1 = \mathsf{HT}(g_l) \circ z_2$ for some $z_1, z_2, w \in \mathcal{N}$. Let us assume $\mathsf{spol}(g_k, g_l) \neq 0$[26]. Hence, $\mathsf{spol}(g_k, g_l) \xrightarrow{*}^{\mathrm{qc}}_G 0$ implies $\mathsf{spol}(g_k, g_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v'_i, \delta_i \in \mathbf{K}^*, h_i \in G, v'_i \in \mathcal{N}$[27], where the h_i are due to the qc-reduction of the s-polynomial and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}(g_k, g_l))$. By lemma 5.5.3, since $t = \mathsf{HT}(g_k) \circ z_1 \circ w \geq_{\mathrm{tup}} \mathsf{HT}(g_k) \circ z_1$ and $\mathsf{HT}(g_k) \circ z_1 \succ \mathsf{HT}(\mathsf{spol}(g_k, g_l))$, we can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v'_i * w$. Since $w \in \mathcal{N}$ and G is $\mathcal{N}$-saturated, without loss of generality we can assume that the representation has the the required form. We now have:

$$
\begin{aligned}
& \alpha_k \cdot g_k * v_k + \alpha_l \cdot g_l * v_l \\
= \; & \alpha_k \cdot g_k * v_k + \underbrace{\alpha'_l \cdot \beta_k \cdot g_k * v_k - \alpha'_l \cdot \beta_k \cdot g_k * v_k}_{=0} + \alpha'_l \cdot \beta_l \cdot g_l * v_l \\
= \; & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot g_k * v_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot g_k * v_k - \beta_l \cdot g_l * v_l)}_{=\mathsf{spol}(g_k, g_l) * w} \\
= \; & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot g_k * v_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v'_i * w) \qquad (5.3)
\end{aligned}
$$

where $\beta_k = \mathsf{HC}(g_k)^{-1}$, $\beta_l = \mathsf{HC}(g_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (5.3) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased.

q.e.d.

On first sight this characterization might seem artificial. The crucial point is that in losing the property "admissible" for our ordering, an essential lemma in Buchberger's context, namely that $p \xrightarrow{*}_F 0$ implies $p * w \xrightarrow{*}_F 0$ for any term w no longer holds. Defining reduction by restricting ourselves to commutative prefixes we gain enough structural information to weaken this lemma, but we have to do additional work to still describe the right ideal congruence. One step is to close the set of polynomials generating the right ideal with respect to the finite group $\mathcal{E}$: For a set of polynomials F using the $\mathcal{E}$-closure $F_{\mathcal{E}} = \{\psi_e(f) \mid f \in F, e \in \mathcal{E}\}$ we can characterize the right ideal generated by F as a set of $\mathcal{N}$-right-multiples since $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{k} \alpha_i \cdot f_i * u_i \mid \alpha_i \in \mathbf{K}, f_i \in F_{\mathcal{E}}, u_i \in \mathcal{N}\}$. If we additionally incorporate the concept of $\mathcal{N}$-saturation, qc-reduction can be used to express the right ideal congruence and then a right Gröbner basis can be characterized as usual by s-polynomials. Now, using the characterization given in theorem 5.5.23 we can state a procedure which enumerates right Gröbner bases in nilpotent group rings:

[26]In case $\mathsf{spol}(g_k, g_l) = 0$, just substitute 0 for $\sum_{i=1}^{n} \delta_i \cdot h_i * v'_i$ in the equations below.

[27]Note that the case $v'_i \in \mathcal{E}$ cannot occur as it implies that h_i is a constant polynomial and we assumed that G does not contain constant polynomials.

Procedure: Right Gröbner Bases in Nilpotent Group Rings

Given: $F \subseteq \mathbf{K}[\mathcal{G}]$ and a presentation of $\mathcal{G}$ by $\mathcal{E}$ and $\mathcal{N}$ as specified above
Find: $\text{GB}_r(F)$, a right Gröbner basis of $\text{ideal}_r(F)$.

$G := \{\psi_e(f) \mid f \in F, e \in \mathcal{E}\}$; % G contains $F_{\mathcal{E}}$
$G := \bigcup_{g \in G} \text{SAT}(g)$; % G is $\mathcal{N}$-saturated and $\text{ideal}_r(F) = \text{ideal}_r(G)$
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ **do** % Test if statement 2 of theorem 5.5.23 is valid
  $(q_1, q_2) :=$ remove(B); % Remove an element using a fair strategy
  if $h := \text{spol}(q_1, q_2)$ exists
    then $h' := \text{normalform}(h, \longrightarrow^{\text{qc}}_{G})$; % Compute a normal form
      if $h' \neq 0$ % The s-polynomial does not reduce to zero
        then $G := G \cup \{g \mid g \in \text{SAT}(h')\}$;
          % G is $\mathcal{N}$-saturated and $\text{ideal}_r(F) = \text{ideal}_r(G)$
          $B := B \cup \{(f, g) \mid f \in G, g \in \text{SAT}(h')\}$;
      endif
  endif
endwhile
$\text{GB}_r(F) := G$

The set G enumerated by this procedure fulfills the requirements of theorem 5.5.23, i.e., we have $F_{\mathcal{E}} \subseteq G$ and the set G at each stage generates the right ideal $\text{ideal}_r(F)$ and is $\mathcal{N}$-saturated. Using a fair strategy to remove elements from the test set B ensures that for all polynomials entered into G the s-polynomial is considered in case it exists. Hence, in case the procedure terminates, it computes a right Gröbner basis. Later on we will see that every right Gröbner basis contains a finite one and hence this procedure must terminate. Let us first continue to show how similar to the case of solvable polynomial rings or skew polynomial rings ([Kr93, We92]), Gröbner bases of two-sided ideals can be characterized by right Gröbner bases which have additional properties. We will call a set of polynomials a **Gröbner basis** with respect to qc-reduction of the two-sided ideal it generates, if it fulfills one of the equivalent statements in the next theorem.

Theorem 5.5.24
For a set of polynomials $G \subseteq \mathbf{K}[\mathcal{G}]$, assuming that $\mathcal{G}$ is presented by (Γ, T) as described above, the following properties are equivalent:

1. *G is a right Gröbner basis and $\text{ideal}_r(G) = \text{ideal}(G)$.*
2. *For all $g \in \text{ideal}(G)$ we have $g \overset{*}{\longrightarrow}^{\text{qc}}_{G} 0$.*
3. *G is a right Gröbner basis and for all $w \in \mathcal{G}$, $g \in G$ we have $w * g \in \text{ideal}_r(G)$.*
4. *G is a right Gröbner basis and for all $a \in \Gamma$, $g \in G$ we have $a * g \in \text{ideal}_r(G)$.*

Proof :

$1 \Longrightarrow 2$: Since $g \in \mathsf{ideal}(G) = \mathsf{ideal}_r(G)$ and G is a right Gröbner basis, we are done.

$2 \Longrightarrow 3$: To show that G is a right Gröbner basis we have to prove $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$ and for all $g \in \mathsf{ideal}_r(G)$, $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$. The latter follows immediately since $\mathsf{ideal}_r(G) \subseteq \mathsf{ideal}(G)$ and hence for all $g \in \mathsf{ideal}_r(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$. The inclusion $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} \subseteq \equiv_{\mathsf{ideal}_r(G)}$ is obvious. Hence let $f \equiv_{\mathsf{ideal}_r(G)} g$, i.e., $f - g \in \mathsf{ideal}_r(G)$. But then we have $f - g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$ and hence by lemma 5.5.7 there exists a polynomial $h \in \mathbf{K}[\mathcal{G}]$ such that $f \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} h$ and $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} h$, yielding $f \overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} g$. Finally, $w * f \in \mathsf{ideal}(G)$ and $w * f \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$ implies $w * f \in \mathsf{ideal}_r(G)$.

$3 \Longrightarrow 4$: This follows immediately.

$4 \Longrightarrow 1$: Since it is obvious that $\mathsf{ideal}_r(G) \subseteq \mathsf{ideal}(G)$ it remains to show that $\mathsf{ideal}(G) \subseteq \mathsf{ideal}_r(G)$ holds. Let $g \in \mathsf{ideal}(G)$, i.e., $g = \sum_{i=1}^{n} \alpha_i \cdot u_i * g_i * w_i$ for some $\alpha_i \in \mathbf{K}$, $g_i \in G$ and $u_i, w_i \in \mathcal{G}$. We will show by induction on $|u_i|$ that for $u_i \in \mathcal{G}$, $g_i \in G$, $u_i * g_i \in \mathsf{ideal}_r(G)$ holds. Then g also has a representation in terms of right multiples and hence lies in the right ideal generated by G as well. In case $|u_i| = 0$ we are immediately done. Hence let us assume $u_i \equiv ua$ for some $a \in \Gamma$ and by our assumption we know $a * g_i \in \mathsf{ideal}_r(G)$. Let $a * g_i = \sum_{j=1}^{m} \beta_j \cdot g'_j * v_j$ for some $\beta_j \in \mathbf{K}$, $g'_j \in G$ and $v_j \in \mathcal{G}$. Then we get $u_i * g_i = ua * g_i = u * (a * g_i) = u * (\sum_{j=1}^{m} \beta_j \cdot g'_j * v_j) = \sum_{j=1}^{m} \beta_j \cdot (u * g'_i) * v_j$ and by our induction hypothesis $u * g'_j \in \mathsf{ideal}_r(G)$ holds for every $1 \leq j \leq m$. Therefore, we can conclude $u_i * g_i \in \mathsf{ideal}_r(G)$.

q.e.d.

Statement 4 enables a constructive approach to use procedure Right Gröbner Bases in Nilpotent Group Rings in order to compute Gröbner bases of two-sided ideals and item 2 states that such bases can be used to decide the membership problem for the two-sided ideal by using qc-reduction. The following corollary of the previous two theorems will be the foundation of a procedure to compute two-sided Gröbner bases.

Corollary 5.5.25
Let $F, G \subseteq \mathbf{K}[\mathcal{G}]$ such that

(i) $\mathsf{ideal}(F) = \mathsf{ideal}(G)$

(ii) $\{\psi_e(f) \mid f \in F, e \in \mathcal{E}\} \subseteq G$

(iii) G is $\mathcal{N}$- saturated.

Then the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}(F)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$.*
2. *(a) For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$.*

   (b) For all $a \in \Gamma$, $g \in G$ we have $a * g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$.

Proof :

$1 \Longrightarrow 2$: By definition 5.5.22 we find that in case for $f_k, f_l \in G$ an s-polynomial exists,

$$\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot f_k * w_1 - \mathsf{HC}(f_l)^{-1} f_l * w_2 \in \mathsf{ideal}(G) = \mathsf{ideal}(F),$$

and then $\mathsf{spol}(f_k, f_l) \xrightarrow{*}_G^{\mathrm{qc}} 0$. Similarly, since $g \in G$ implies $a * g \in \mathsf{ideal}(G) = \mathsf{ideal}(F)$ for all $a \in \Gamma$, we have $a * g \xrightarrow{*}_G^{\mathrm{qc}} 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}(F)$ is $\longrightarrow_G^{\mathrm{qc}}$-reducible to zero. Without loss of generality we assume that G contains no constant polynomials, as then we are done at once. Let $g = \sum_{j=1}^m \alpha_j \cdot u_j * f_j * w_j$ be a representation of such a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*$, $f_j \in F$, $u_j, w_j \in \mathcal{G}$ and suppose for $1 \leq j \leq m$ we have $w_j \equiv e_j v_j$ with $e_j \in \mathcal{E}$ and $v_j \in \mathcal{N}$. Then we can modify this representation to $g = \sum_{j=1}^m \alpha_j \cdot u_j * \psi_{e_j}(f_j) * v_j$ as $\psi_{e_j}(f_j) \in G$ by our assumption. Next we will show that every multiple $u_j * \psi_{e_j}(f_j)$ has a representation $u_j * \psi_{e_j}(f_j) = \sum_{i=1}^{m_j} \beta_i \cdot g_i * v_i'$ with $\beta_i \in \mathbf{K}^*$, $g_i \in G$ and $v_i' \in \mathcal{N}$. More general, we will show that this is true for every multiple $u * g$, $u \in \mathcal{G}$, $g \in G$. As in the previous theorem this will be done by induction on $|u|$. The case $|u| = 0$ is obvious. Hence let $u \equiv u'a$ for some $a \in \Gamma$. By our assumption we know $a * g \xrightarrow{*}_G^{\mathrm{qc}} 0$ and as we assume that G does not contain constant polynomials, this reduction sequence results in a representation $a * g = \sum_{i=1}^k \gamma_i \cdot g_i' * v_i''$ with $\gamma_i \in \mathbf{K}^*$, $g_i' \in G$ and $v_i'' \in \mathcal{N}$. Hence, $u * g = u' * (a * g) = u' * (\sum_{i=1}^k \gamma_i \cdot g_i' * v_i'') = \sum_{i=1}^k \gamma_i \cdot (u' * g_i') * v_i''$ and now our induction hypothesis can be applied to each multiple $u' * g_i'$, and since products of elements in $\mathcal{N}$ are again in $\mathcal{N}$, we are done. Therefore, we find that g has a representation $g = \sum_{j=1}^n \alpha_j' \cdot f_j' * w_j'$ where $\alpha_j' \in \mathbf{K}^*$, $f_j' \in G$, $w_j' \in \mathcal{N}$ and now we can proceed as in theorem 5.5.23 to prove our claim.

q.e.d.

Procedure: GRÖBNER BASES IN NILPOTENT GROUP RINGS

Given: $F \subseteq \mathbf{K}[\mathcal{G}]$ and a presentation (Γ, T) of $\mathcal{G}$ by $\mathcal{E}$ and $\mathcal{N}$ as specified above.
Find: $\mathrm{GB}(F)$, a Gröbner basis of $\mathsf{ideal}(F)$.

$G := \{\psi_e(f) \mid f \in F, e \in \mathcal{E}\}$; % G contains $F_{\mathcal{E}}$ and $\mathsf{ideal}(F) = \mathsf{ideal}(G)$
$G := \bigcup_{g \in G} \mathrm{SAT}(g)$; % G is $\mathcal{N}$-saturated
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
$M := \{a * f \mid f \in G, a \in \Gamma\}$;
while $M \neq \emptyset$ or $B \neq \emptyset$ **do**
  if $M \neq \emptyset$
    then $h :=$ remove(M); % Remove an element using a fair strategy
      $h' :=$ normalform$(h, \longrightarrow_G^{\mathrm{qc}})$;
      if $h' \neq 0$
        then $G := G \cup \mathrm{SAT}(h')$;
          % G is $\mathcal{N}$-saturated and $\mathsf{ideal}(F) = \mathsf{ideal}(G)$
          $B := B \cup \{(f, g) \mid f \in G, g \in \mathrm{SAT}(h')\}$;

$M := \{a * g \mid a \in \Gamma, g \in \textsc{Sat}(h')\};$
endif
endif
if $B \neq \emptyset$
then $(q_1, q_2) :=$ remove(B); % Remove an element using a fair strategy
if $h := \mathsf{spol}(q_1, q_2)$ exists
then $h' :=$ normalform$(h, \longrightarrow^{\mathrm{qc}}_{G})$;
if $h' \neq 0$ % The s-polynomial does not reduce to zero
then $G := G \cup \textsc{Sat}(h')$;
% G is $\mathcal{N}$-saturated and $\mathsf{ideal}(F) = \mathsf{ideal}(G)$
$B := B \cup \{(f, g) \mid f \in G, g \in \textsc{Sat}(h')\}$;
$M := \{a * g \mid a \in \Gamma, g \in \textsc{Sat}(h')\}$;
endif
endif
endif
endwhile
$\textsc{Gb}(F) := G$

Correctness of this procedure follows from corollary 5.5.25. For the set G enumerated by this procedure we have $F_{\mathcal{E}} \subseteq G$ and the set G at each stage generates the ideal $\mathsf{ideal}(F)$ and is $\mathcal{N}$-saturated. Using a fair strategy to remove elements from the test sets B and M ensures that for all polynomials entered into G the existing s-polynomials and the critical left multiples are considered. To show termination we need the following theorem which makes use of Dickson's lemma due to the special representatives of the group elements.

Theorem 5.5.26
Every (right) Gröbner basis contains a finite one.

Proof : Let F be a subset of $\mathbf{K}[\mathcal{G}]$ and G a Gröbner basis[28] of $\mathsf{ideal}(F)$, i.e., $\mathsf{ideal}(F) = \mathsf{ideal}(G) = \mathsf{ideal}_r(G)$ and for all $g \in \mathsf{ideal}(F)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$. We can assume that G is infinite as otherwise we are done. Further let $H = \{\mathsf{HT}(g) \mid g \in G\} \subseteq \mathcal{G}$. Then for every polynomial $f \in \mathsf{ideal}(F)$ there exists a term $t \in H$ such that $\mathsf{HT}(f) \geq_{\mathrm{tup}} t$. H can be decomposed into $H = \bigcup_{e \in \mathcal{E}} H_e$ where H_e contains those terms in H starting with e. For each element of $eu \in H_e$ the element u then can be viewed as an n-tuple over $\mathbf{Z}$ as it is presented by an ordered group word. But we can also view it as a 2n-tuple over $\mathbf{N}$ by representing each element $u \in \mathcal{N}$ by an extended ordered group word $u \equiv a_1^{-i_1} a_1^{j_1} \ldots a_n^{-i_n} a_n^{j_n}$, where $i_l, j_l \in \mathbf{N}$ and the representing 2n-tuple is $(i_1, j_1, \ldots, i_n, j_n)$. Notice that at most one of the two exponents i_l and j_l is non-zero. Now only considering the ordered group word parts of the terms, each set H_e can be seen as a (possibly infinite) subset of a free commutative monoid $\mathcal{T}_{2n}$ with $2 \cdot n$ generators. Thus by Dickson's lemma there exists a finite subset B_e of H_e such that

[28] The proof for the existence of a finite right Gröbner basis for $\mathsf{ideal}_r(F)$ is similar.

for every $w \in H_e$ there is a $b \in B_e$ with $w \geq_{\rm tup} b$. Now we can use the sets B_e to distinguish a finite Gröbner basis in G as follows. To each term $t \in B_e$ we can assign a polynomial $g_t \in G$ such that $\mathsf{HT}(g_t) = t$. Then the set $G_B = \{g_t \mid t \in B_e, e \in \mathcal{E}\}$ is again a Gröbner basis since for every polynomial $f \in \mathsf{ideal}(F)$ there still exists a polynomial g_t now in G_B such that $\mathsf{HT}(f) \geq_{\rm tup} \mathsf{HT}(g_t) = t$. Hence all polynomials in $\mathsf{ideal}(F)$ are qc-reducible to zero using G_B.

q.e.d.

Since both procedures enumerate respective Gröbner bases and the sets enumerated contain finite Gröbner bases, the procedures terminate as soon as all polynomials of the contained bases are entered into G. Therefore we now are able to solve problems related to right and two-sided ideals in nilpotent group rings using reduction similar to Buchberger's approach to commutative polynomial rings.

Chapter 6

Monoid Rings over Reduction Rings

More matter, with less art.

HAMLET

In this chapter we want to outline how the ideas of completion in a monoid ring over a field can be modified and carried over to monoid rings over reduction rings as defined by Madlener in [Ma86]. The special case of monoid rings over the integers has been studied explicitly in [MaRe93b] and will be used to provide an example when following the more general approach given by Kapur and Narendran in [KaNa85].

Let $\mathbf{R}$ be a commutative ring with a reduction $\Longrightarrow_B$ associated with subsets $B \subseteq \mathbf{R}$ satisfying the following axioms

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

(A2) $\alpha \Longrightarrow_\beta \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}^{\mathbf{R}}(\beta)$, i.e., $\gamma = \alpha - \beta \cdot \rho$ for some $\rho \in \mathbf{R}$.

(A3) $\alpha \Longrightarrow_\alpha 0$ for all $\alpha \in \mathbf{R}\backslash\{0\}$.

Notice that 0 has to be irreducible for all $\Longrightarrow_\alpha$, $\alpha \in \mathbf{R}$. Therefore, 0 will be chosen as the normal form of the ideal elements. Let us recall the definition of G-bases (Gröbner bases) for ideals in such a ring $\mathbf{R}$.

Definition 6.0.1
A finite subset B of $\mathbf{R}$ is called a **G-basis** of an ideal $\mathfrak{i}$, if $\overset{*}{\Longleftrightarrow}_B = \equiv_{\mathfrak{i}}$ and $\Longrightarrow_B$ is confluent. $\diamond$

$\mathbf{R}$ is called a **reduction ring** if every finitely generated ideal has a G-basis. It is often useful, if $\mathbf{R}$ satisfies an additional axiom strongly related to interreduction.

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

In the following we will always assume that the reduction ring fulfills the axioms (A1) to (A4).

Lemma 6.0.2
Let $B \subseteq \mathbf{R}$ be a G-basis and $B' \subseteq B$ such that for all $\beta \in B$, $\beta \stackrel{*}{\Longrightarrow}_{B'} 0$ holds. Then for all $\alpha \in \mathbf{R}$, $\alpha \stackrel{*}{\Longrightarrow}_B 0$ implies $\alpha \stackrel{*}{\Longrightarrow}_{B'} 0$. In particular, B' is a G-basis of $\mathsf{ideal}^{\mathbf{R}}(B)$.

Proof :
Notice that by axiom (A4) and our assumptions on B', all elements reducible using B are also reducible using B' and $\mathrm{IRR}(\Longrightarrow_{B'}) \subseteq \mathrm{IRR}(\Longrightarrow_B)$. Assuming $\alpha \stackrel{*}{\Longrightarrow}_B 0$ but $\alpha \stackrel{*}{\Longrightarrow}_{B'} \alpha\Downarrow_{B'} \neq 0$ we find $\alpha\Downarrow_{B'} \in \mathrm{IRR}(\Longrightarrow_{B'}) \subseteq \mathrm{IRR}(\Longrightarrow_B)$ and $\alpha\Downarrow_{B'} \in \mathsf{ideal}^{\mathbf{R}}(B)$, contradicting that B is a G-basis of $\mathsf{ideal}^{\mathbf{R}}(B)$.
In particular, as B is a G-basis we have $\alpha \stackrel{*}{\Longrightarrow}_{B'} \alpha \Downarrow_B$ since $\stackrel{*}{\Longleftrightarrow}_{B'} \subseteq \stackrel{*}{\Longleftrightarrow}_B = \equiv_{\mathsf{ideal}^{\mathbf{R}}(B)}$ and $\Longrightarrow_B$ is confluent. This implies that $\Longrightarrow_{B'}$ is also confluent, as $\alpha\Downarrow_B$ is unique. Now it remains to show that $\stackrel{*}{\Longleftrightarrow}_B \subseteq \stackrel{*}{\Longleftrightarrow}_{B'}$ holds. This follows immediately, as for $\alpha \stackrel{*}{\Longleftrightarrow}_B \beta$ the confluence of $\Longrightarrow_B$ yields $\alpha\Downarrow_{B'} = \alpha\Downarrow_B = \beta\Downarrow_B = \beta\Downarrow_{B'}$ which implies $\alpha \stackrel{*}{\Longleftrightarrow}_{B'} \beta$.

q.e.d.

Given a cancellative[1] monoid $\mathcal{M}$, we call $\mathbf{R}[\mathcal{M}]$ the monoid ring over $\mathbf{R}$. Using an appropriate ordering $\succ$ on the monoid, we can proceed as described in chapter 4 and specify reduction in $\mathbf{R}[\mathcal{M}]$ depending on reduction in $\mathbf{R}$. We additionally define a partial ordering on $\mathbf{R}$ by setting for $\alpha, \beta \in \mathbf{R}$, $\alpha >_{\mathbf{R}} \beta$ if and only if there exists a set $B \subseteq \mathbf{R}$ such that $\alpha \stackrel{+}{\Longrightarrow}_B \beta$. Then we can define a Noetherian ordering on $\mathbf{R}[\mathcal{M}]$ as follows: for $f, g \in \mathbf{R}[\mathcal{M}]$, $f > g$ if and only if either $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ or ($\mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HC}(f) >_{\mathbf{R}} \mathsf{HC}(g)$) or ($\mathsf{HM}(f) = \mathsf{HM}(g)$ and $\mathsf{RED}(f) > \mathsf{RED}(g)$). Notice that this ordering in general is not total on $\mathbf{R}[\mathcal{M}]$.

Definition 6.0.3
Let p, f be two non-zero polynomials in $\mathbf{R}[\mathcal{M}]$.
We say f **right reduces** p to q at a monomial $\alpha \cdot t$ in p in one step, denoted by $p \longrightarrow^{\mathrm{r}}_f q$, if

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

(b) $\alpha \Longrightarrow_{\mathsf{HC}(f)} \beta$ with $\alpha = \gamma \cdot \mathsf{HC}(f) + \beta$ for some $\beta, \gamma \in \mathbf{R}$, and

(c) $q = p - \gamma \cdot f * w$.

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

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

Notice that in case f right reduces p to q at a monomial $\alpha \cdot t$ this no longer implies $t \notin \mathsf{T}(q)$. But when using a set of polynomials for reduction we know by (A1) that reducing α in $\mathbf{R}$ with respect to the head coefficients of the applicable polynomials must terminate and then either the term t disappears or is not further reducible. Hence the so-defined right reduction is Noetherian.

Analogous definitions can be introduced for strong, prefix and the other notions of reduction considered previously. As before, for right reduction $\alpha \cdot p * w \longrightarrow^{\mathrm{r}}_{p} 0$ need not hold. Hence, we have to introduce the concept of saturation as in section 4.3, extended to include possible problems caused by multiplication with coefficients.

Definition 6.0.4
A set of polynomials $F \subseteq \{\alpha \cdot p * w \mid \alpha \in \mathbf{K}^*, w \in \mathcal{M}\}$ is called a **saturating set** for a polynomial $p \in \mathbf{R}[\mathcal{M}]$, if for all $\alpha \in \mathbf{R}^*$, $w \in \mathcal{M}$, $\alpha \cdot p * w \longrightarrow^{\mathrm{r}}_{F} 0$ holds in case $\alpha \cdot p * w \neq 0$. Let $\mathcal{SAT}(p)$ denote the family of all saturating sets for p. A set F of polynomials in $\mathbf{R}[\mathcal{M}]$ is called **saturated**, if $\alpha \cdot f * w \longrightarrow^{\mathrm{r}}_{F} 0$ holds for all $f \in F$ and all $\alpha \in \mathbf{R}^*$, $w \in \mathcal{M}$ in case $\alpha \cdot f * w \neq 0$. $\diamond$

Definition 6.0.5
A set $G \subseteq \mathbf{R}[\mathcal{M}]$ is called a **Gröbner basis** with respect to the reduction $\longrightarrow^{\mathrm{r}}$ or a **right (or stable) Gröbner basis**, if

(i) $\stackrel{*}{\longleftrightarrow}^{\mathrm{r}}_{G} \;=\; \equiv_{\mathsf{ideal}_r(G)}$, and

(ii) $\longrightarrow^{\mathrm{r}}_{G}$ is confluent. $\diamond$

We will assume that for the reduction ring $\mathbf{R}$ there is an algorithm to compute G-bases and a representation of the elements of these bases in terms of the elements of the generating set. Further we require that it is possible to compute a finite basis for a module of solutions to linear homogeneous equations over $\mathbf{R}$. These sets are necessary to describe "overlaps" due to coefficients that we will need to characterize right Gröbner bases in the monoid ring later on. Next we give a criterion for checking whether a given basis of a right ideal is a right Gröbner basis. We start by defining special polynomials for finite subsets of polynomials, called G-polynomials and M-polynomials.

Definition 6.0.6
Let $P = \{p_1, \ldots, p_k\}$ be a set of polynomials in $\mathbf{R}[\mathcal{M}]$ and t an element in $\mathcal{M}$ such that there are $w_1, \ldots, w_k \in \mathcal{M}$ with $\mathsf{HT}(p_i * w_i) = \mathsf{HT}(p_i) \circ w_i = t$, for all $1 \leq i \leq k$. Further let $\gamma_i = \mathsf{HC}(p_i)$ for $1 \leq i \leq k$[2].
Let $\{\alpha_1, \ldots, \alpha_n\}$ be a G-basis of $\{\gamma_1, \ldots, \gamma_k\}$ and

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

[2]Note that this definition would have to be modified for non-cancellative monoids, as then $\mathsf{HT}(p * w) = \mathsf{HT}(p) \circ w$ does not imply $\mathsf{HC}(p * w) = \mathsf{HC}(p)$.

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

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

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

$$m_i = \sum_{j=1}^{k} \alpha_{i,j} \cdot p_j * w_j \text{ for each } 1 \leq i \leq r.$$

Notice that $\mathsf{HT}(m_i) \prec t$ for each $1 \leq i \leq r$. $\diamond$

Given a set of polynomials F, the set of corresponding G- and M-polynomials contains those which are specified by definition 6.0.6 for each finite subset $P \subseteq F$ and each term $t \in \mathcal{M}$ fulfilling the respective conditions. For a set consisting of one polynomial the corresponding M-polynomials reflect the multiplication of the polynomial with zero-divisors of the head coefficient, i.e., by a basis of the annihilator of the head coefficient. This case is also treated by the idea of saturation. Notice that given a finite set of polynomials the corresponding sets of G- and M-polynomials in general can be infinite (e.g., reviewing example 4.3.21, for the polynomials $p = a + f$ and $q = b + \lambda$ infinitely many critical situations at the terms ba^i, $i \in \mathbf{N}^+$ have to be considered).

We can use G- and M-polynomials to characterize right Gröbner bases in monoid rings over a reduction ring in case they are additionally saturated.

Theorem 6.0.7
For a saturated subset F of $\mathbf{R}[\mathcal{M}]$ the following statements are equivalent:

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

Proof :
$1 \Longrightarrow 2$: This follows from the fact that all G-polynomials and M-polynomials belong to the right ideal generated by F.

$2 \Longrightarrow 1$: We have to show that every element $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is right reducible to zero using F. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{r}}_{F} h'$ implies $h' \in \mathsf{ideal}_r(F)$. Thus as $\longrightarrow^{\mathrm{r}}_{F}$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(F)\backslash\{0\}$ is right reducible using F. This will be done by assuming the contrary. Let $g = \sum_{j=1}^{m} \gamma_j \cdot f_j * w_j$ with

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

$$\begin{aligned}
& \sum_{i=1}^{k} \gamma_i \cdot f_i * w_i \\
= & \sum_{i=1}^{k} (\sum_{j=1}^{n} \alpha_{j,i} \cdot \delta_j) \cdot f_i * w_i \\
= & \sum_{j=1}^{n} \delta_j \cdot (\sum_{i=1}^{k} \alpha_{j,i} \cdot f_i * w_i) \qquad (6.1)
\end{aligned}$$

Taking a closer look at the last sum of these transformations in 6.1, we see that we can express the sum of the first k elements of our representation of g by a sum of M-polynomials. Since these M-polynomials belonging to $\{f_1, \ldots, f_k\}$ and t all have head terms smaller than t and are all right reducible to zero using F, we get a new representation of g with a critical term smaller than t, contradicting our assumption that our chosen representation was minimal.
In case $t = \mathsf{HT}(g)$ we know that there exists a finite subset $P \subseteq F$ such that $\mathsf{HC}(g) \in \mathsf{ideal}^{\mathbf{R}}(\{\mathsf{HC}(p) \mid p \in P\})$, and as this ideal is finitely generated it has a G-basis, say G_P. Then $\mathsf{HC}(g)$ is reducible by an element $\alpha \in G_P$. By our assumption now $\alpha \cdot t$ is head monomial of a G-polynomial corresponding to P and t and since this G-polynomial is right reducible to zero using F, in particular there exist polynomials $f_1, \ldots, f_k \in F$ in volved in the reduction of $\alpha \cdot t$ such that $\alpha \Longrightarrow_{\mathsf{HC}(f_1)} \alpha_1 \Longrightarrow_{\mathsf{HC}(f_2)} \cdots \Longrightarrow_{\mathsf{HC}(f_k)} 0$. By lemma 6.0.2 this implies that $\mathsf{HM}(g)$ is right reducible using F.

q.e.d.

In case we additionally require that in $\mathbf{R}$ every ideal is finitely generated we can even show a stronger result in the second part of this proof. Given a set of polynomials F and an element $s \in \mathcal{M}$, let

$$C_F(s) = \{\mathsf{HC}(f) \mid f \in F, s = \mathsf{HT}(f) \circ z \text{ for some } z \in \mathcal{M}, \mathsf{HT}(f * z) = \mathsf{HT}(f) \circ z\}.$$

Notice that if F is finite then $C_F(s)$ is also finite. Then the following lemma holds.

Lemma 6.0.8
Let $\mathbf{R}$ be a reduction ring such that every ideal is finitely generated. Further let F be a saturated set of polynomials fulfilling the conditions of theorem 6.0.7. Then for every $s \in \mathcal{M}$, the corresponding set $C_F(s)$ contains a G-basis of $\mathsf{ideal}^{\mathbf{R}}(C_F(s))$.

Proof :
Since $\mathsf{ideal}^{\mathbf{R}}(C_F(s))$ is finitely generated, there exists a finite set $A \subseteq C_F(s)$ such that $\mathsf{ideal}^{\mathbf{R}}(A) = \mathsf{ideal}^{\mathbf{R}}(C_F(s))$. Let G_A be the finite G-basis of this ideal. Furthermore let $P \subseteq F_s = \{f \in F \mid \text{ there exists an element } z \in \mathcal{M} \text{ such that } \mathsf{HT}(f * z) = \mathsf{HT}(f) \circ z = s\}$ be a finite set of polynomials such that $A = \{\mathsf{HC}(f) \mid f \in P, s = \mathsf{HT}(f) \circ z = \mathsf{HT}(f * z) \text{ for some } z \in \mathcal{M}\}$. Then, as for every $\alpha \in G_A$ there exists a G-polynomial corresponding to P and s, by our assumption there exists a finite set $C \subset C_F(s)$ such that for all $\alpha \in G_A$ we have $\alpha \overset{*}{\Longrightarrow}_C 0$. Moreover, since $C \subseteq C \cup G_A$ and the latter is a G-basis of $\mathsf{ideal}^{\mathbf{R}}(A) = \mathsf{ideal}^{\mathbf{R}}(C_F(s))$, by lemma 6.0.2 C is also a G-basis of the same ideal.

q.e.d.

This lemma also holds in case F is finite as then all ideals $\mathsf{ideal}^{\mathbf{R}}(C_F(s))$ in this proof are finitely generated, namely by the finite sets $C_F(s)$.

Corollary 6.0.9
Let F be a saturated set fulfilling the conditions specified in theorem 6.0.7. In case F is finite or $\mathbf{R}$ is Noetherian, then F is a right G-basis.

Proof :
The inclusion $\overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_F \subseteq \equiv_{\mathsf{ideal}_r(F)}$ is obvious. Hence let us assume $f \equiv_{\mathsf{ideal}_r(F)} g$, i.e., $f - g \in \mathsf{ideal}_r(F)$ and, therefore, $f - g \overset{*}{\longrightarrow}{}^{\mathrm{r}}_F 0$. We show that this implies $f \overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_F g$. In case $f - g = 0$ we are immediately done. Hence let us assume $f - g \neq 0$ and as any polynomial in $\mathsf{ideal}_r(F)$ is right reducible to zero using F, without loss of generality we can assume that the reduction sequence $f - g \overset{*}{\longrightarrow}{}^{\mathrm{r}}_F 0$ uses top-reduction, i.e., all reductions take place at the respective head monomial. Further let $t = \mathsf{HT}(f - g)$ and let γ_1 respectively γ_2 be the coefficients of t in f respectively g. We will now show that $f \overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_F g$ holds by induction on the term $t = \mathsf{HT}(f - g)$. In case $t = \lambda$ we find $f - g = \gamma_1 - \gamma_2 \overset{*}{\longrightarrow}{}^{\mathrm{r}}_F 0$ and as described in lemma 6.0.8 there exists a subset $C \subseteq C_F(\lambda) = \{\mathsf{HC}(f) \mid f \in F, \lambda = \mathsf{HT}(f * z) = \mathsf{HT}(f) \circ z \text{ for some } z \in \mathcal{M}\} \subseteq \mathbf{R}$ which is a G-basis of $\mathsf{ideal}^{\mathbf{R}}(C_F(\lambda))$ and then, as $\gamma_1 - \gamma_2 \in \mathsf{ideal}^{\mathbf{R}}(C_F(\lambda))$, $\gamma_1 - \gamma_2 \overset{*}{\Longrightarrow}_C 0$ implies $\gamma_1 \overset{*}{\Longleftrightarrow}_C \gamma_2$. Using the respective polynomials belonging to the elements in C, we get $f \overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_F g$. Now let us assume $t \succ \lambda$ and $f - g \overset{k}{\longrightarrow}{}^{\mathrm{r}}_F h$ where $k \in \mathbf{N}^+$ is minimal such that $\mathsf{HT}(h) \neq t$. Further let $f_1, \ldots, f_k$ be the polynomials used in the respective reduction steps, i.e., $\gamma_1 - \gamma_2 \overset{*}{\Longrightarrow}_{\{\mathsf{HC}(f_i) \mid 1 \leq i \leq k\}} 0$. Again there exists a set $C \subseteq C_F(t)$ which is a G-basis of $\mathsf{ideal}^{\mathbf{R}}(C_F(t))$ and without loss of generaltity let $\{\mathsf{HC}(f_i) \mid 1 \leq i \leq k\} \subseteq C$. Then $\gamma_1 - \gamma_2 \overset{*}{\Longrightarrow}_C 0$ implies $\gamma_1 \overset{*}{\Longleftrightarrow}_C \gamma_2$. Now applying

the polynomial multiples belonging to the elements of C used in this last sequence $\gamma_1 \overset{*}{\Longleftrightarrow}_C \gamma_2$ to the monomial with term t in f we find an element $\tilde{f} \in \mathbf{R}[\mathcal{M}]$ such that $f \overset{*}{\longleftrightarrow}^{\mathrm{r}}_F \tilde{f}$, $\mathsf{HM}(\tilde{f}) = \gamma_2 \cdot t$, $\tilde{f} - g \in \mathsf{ideal}_r(F)$, and $t \succ \mathsf{HT}(\tilde{f} - g)$. Hence our induction hypothesis yields $g \overset{*}{\longleftrightarrow}^{\mathrm{r}}_F \tilde{f} \overset{*}{\longleftrightarrow}^{\mathrm{r}}_F f$ and we are done.
It remains to show that right reduction using F is confluent. Suppose there is a polynomial g having two distinct normal forms with respect to F, say p_1 and p_2. Let t be the largest term on which p_1 and p_2 differ and let α_1 respectively α_2 be the coefficients of t in p_1 respectively p_2. Since $p_1 - p_2 \in \mathsf{ideal}_r(F)$ we know $p_1 - p_2 \overset{*}{\longrightarrow}^{\mathrm{r}}_F 0$ and $\alpha_1 - \alpha_2 \in \mathsf{ideal}^{\mathbf{R}}(C_F(t)) = \mathsf{ideal}^{\mathbf{R}}(C)$, where $C \subseteq C_F(t)$ is a G-basis. Hence, $\alpha_1 \overset{*}{\Longleftrightarrow}_C \alpha_2$, and either α_1 or α_2 must be reducible using C, i.e., not both p_1 and p_2 can be in normal form with respect to F, contradicting our assumption.

q.e.d.

In [De89] Deiß has shown that in case $\mathbf{R}$ allows the computation of Gröbner bases using pairs of polynomials, then Gröbner bases in commutative polynomial rings over $\mathbf{R}$ can also be characterized by G- and M-polynomials of pairs of polynomials. When working over the integers it is even possible to restrict oneself to *one* special overlap called the s-polynomial. We have done a similar characterization for monoid rings over the integers in [MaRe93a] which is sketched in the following example. Notice, that still a pair of polynomials can give rise to an infinite set of s-polynomials.

Example 6.0.10
We give a definition of $\mathbf{Z}$ as a reduction ring fulfilling the axioms (A1) to (A4) by defining a reduction relation as follows:
First we give a total ordering on $\mathbf{Z}$ by $\alpha <_{\mathbf{Z}} \beta$ if and only if ($\alpha \geq 0$ and $\beta < 0$) or ($\alpha \geq 0$, $\beta > 0$ and $\alpha < \beta$) or ($\alpha < 0$, $\beta < 0$ and $\alpha > \beta$). For $\alpha \in \mathbf{Z}$ we call the elements ρ with $0 \leq \rho < |\alpha|$ the remainders of α. Reduction is now specified as $\alpha \Longrightarrow_\beta \gamma$ if and only if $\alpha \geq_{\mathbf{Z}} \beta$, $\alpha = \delta \cdot \beta + \gamma$ and γ is a remainder of $|\beta|$. The axioms (A1) to (A3) are easily checked. (A4) holds since $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_\gamma \delta$ imply $\alpha \geq_{\mathbf{Z}} \beta \geq_{\mathbf{Z}} \gamma \geq_{\mathbf{Z}} \delta$ and hence α is reducible by γ as well as by δ.

Notice that $\mathbf{Z}$ contains pairs of non-zero associated elements[3] which only differ in sign. We will call the positive element of such a pair the canonical element and define right reduction by restricting ourselves to the use of polynomials with canonical head coefficients for reduction only (compare [KaKa84]).

A polynomial f right reduces a non-zero polynomial p to q at a monomial $\alpha \cdot t$ in p in one step, denoted by $p \longrightarrow^{\mathrm{r}}_f q$, if

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

(b) $\mathsf{HC}(f) > 0$ and $\alpha = \gamma \cdot \mathsf{HC}(f) + \beta$ for $\gamma, \beta \in \mathbf{Z}$, $\gamma \neq 0$, β a remainder of $\mathsf{HC}(f)$.

(c) $q = p - \gamma \cdot f * w$.

[3]We call α and β associated in case there exists a unit ϵ such that $\alpha = \epsilon \cdot \beta$

Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{M}]$ with $HT(p_i) = t_i$, $i = 1, 2$. If there are $w_1, w_2 \in \mathcal{M}$ with $t_1 \circ w_1 = t_2 \circ w_2 = t$, and α_1, α_2 are the non-zero coefficients of t in $p_1 * w_1$ respectively $p_2 * w_2$, then If $\alpha_2 \geq \alpha_1 > 0$ and $\alpha_2 = \beta \cdot \alpha_1 + \gamma$, where $\beta, \gamma \in \mathbf{Z}$, γ a remainder of α_1, we get the following s-polynomial

$$\mathsf{spol}(p_1, p_2, w_1, w_2) = \beta \cdot p_1 * w_1 - p_2 * w_2.$$

Let $U_{\mathsf{HM}(p_1),\mathsf{HM}(p_2)} \subseteq \mathcal{M} \times \mathcal{M}$ be the set containing all pairs $w_1, w_2 \in \mathcal{M}$ as above.

Now we can characterize right Gröbner bases as follows:
For a saturated set of polynomials F in $\mathbf{Z}[\mathcal{M}]$, equivalent are:

1. F is a right Gröbner basis.
2. $\mathsf{ideal}_r(F) \xrightarrow{*}{}^{\mathrm{r}}_F 0$.
3. For all not necessarily different $f_k, f_l \in F, (w_k, w_l) \in U_{\mathsf{HM}(f_k),\mathsf{HM}(f_l)}$ we have $\mathsf{spol}(f_k, f_l, w_k, w_l) \xrightarrow{*}{}^{\mathrm{r}}_F 0$. $\diamond$

The existence of finite Gröbner bases for the special classes of monoids and groups shown in the previous chapters can be transfered to corresponding monoid rings over reduction rings. This is on one hand due to the fact that with respect to prefix, commutative or quasi-commutative reduction, for a finite set of polynomials we can localize the corresponding G- and M-polynomials to finitely many critical situations. On the other hand the property of having a reduction ring as coefficient domain ensures the finiteness of the respective Gröbner bases. Using the necessary procedures for calculations in $\mathbf{R}$ one can modify the given procedures as it has been done for the case of the integers.

Let us close this section with a short remark on other possible definitions of "Gröbner" bases of ideals in reduction rings. Recall that in order to decide the membership or the congruence problem of an ideal $\mathfrak{i}$ in a reduction ring it is sufficient to have a finite basis G of $\mathfrak{i}$ such that for all $\alpha \in \mathfrak{i}$ we have $\alpha \xRightarrow{*}_G 0$. This definition of special ideal bases was used e.g. by Pan ([Pa85]) or Kapur and Narendran ([KaNa85]). Notice that for such a basis $\overset{*}{\Longleftrightarrow}_G = \equiv_{\mathfrak{i}}$ in general need not hold. In case one uses these bases to define G-polynomials, theorem 6.0.7 no longer characterizes right Gröbner bases since we cannot guarantee $\overset{*}{\longleftrightarrow}{}^{\mathrm{r}}_F = \equiv_{\mathsf{ideal}^r(F)}$.

Another type of ideal bases studied in reduction rings are the so-called weak Gröbner bases.

Definition 6.0.11
A finite subset B in $\mathbf{R}$ is called a **weak G-basis** of an ideal $\mathfrak{i}$, if $\overset{*}{\Longleftrightarrow}_B = \equiv_{\mathfrak{i}}$ and every element in the ideal reduces to zero using B. $\diamond$

Example 6.0.12
To give an example for a weak Gröbner basis, let us define reduction using 4 on $\mathbf{Z}$ as follows: For $n > 7$ set $n \Longrightarrow_4 n - 4$, for $n < -4$ set $n \Longrightarrow_4 n + 4$ and further set

$7 \Longrightarrow_4 3$, $7 \Longrightarrow_4 -1$, $6 \Longrightarrow_4 2$, $6 \Longrightarrow_4 -2$, $5 \Longrightarrow_4 1$, $5 \Longrightarrow_4 -3$, $4 \Longrightarrow_4 0$, $-4 \Longrightarrow_4 0$. Then we have that $\stackrel{*}{\Longleftrightarrow}_{\{4\}} = \equiv_{\mathsf{ideal}^{\mathbf{R}}(4)}$ and all elements in $\mathsf{ideal}^{\mathbf{R}}(4)$ reduce to zero. But although $3 - (-1) = 4 \Longrightarrow_4 0$, 3 and -1 are not joinable, i.e., the translation lemma does not hold and $\Longrightarrow_{\{4\}}$ is not confluent. $\diamond$

Although we now have that the weak G-bases in $\mathbf{R}$ describe the ideal congruence, this does not carry over to the monoid ring: when using these bases to define G-polynomials, theorem 6.0.7 does not characterize right Gröbner bases, as lemma 6.0.2 no longer holds. We still have

Lemma 6.0.13
Let $B \subseteq \mathbf{R}$ be a weak G-basis and $B' \subseteq B$ such that for all $\beta \in B$, $\beta \stackrel{*}{\Longrightarrow}_{B'} 0$ holds. Then for all $\alpha \in \mathbf{R}$, $\alpha \stackrel{*}{\Longrightarrow}_B 0$ implies $\alpha \stackrel{*}{\Longrightarrow}_{B'} 0$.

But we cannot show that B' is a weak G-basis, as the axioms, especially (A2) and (A4), do not provide enough information on the reduction step to capture the ideal congruence. Still, special bases can be characterized as in theorem 6.0.7 which allow to solve the membership and congruence problem in case they are finite.

Chapter 7

Concluding Remarks

So eine Arbeit wird eigentlich nie fertig.

GOETHE

The aim of this thesis was to introduce reduction and the concept of Gröbner bases to monoid and group rings.

Since finitely generated ideals in general already do not have finite Gröbner bases in the free monoid or free group ring due to the fact that this would solve the word problem for monoids respectively groups, we have restricted our studies to right ideals except for the class of commutative monoids where right ideals are of course ideals and for the class of nilpotent groups. Furthermore, as general monoid rings need not be right Noetherian, we have tried to localize monoids and groups where finitely generated right ideals have finite Gröbner bases.

In order to introduce reduction to a monoid ring, a well-founded ordering on the monoid elements is needed. Such an ordering in general cannot be compatible with the monoid multiplication and hence one of the main problems turned out to be that monomial right multiples of a polynomial need no longer be reducible to zero by the polynomial itself. Furthermore, Gröbner bases cannot be characterized by head terms as in the case of polynomial rings, solvable polynomial rings or free monoid rings. This phenomenon of having to deal with non-stable orderings influenced the concepts of reduction we studied: strong reduction allowed to use all right multiples of a polynomial as rules, right reduction restricted the right multiples to the "stable" ones and in defining prefix respectively commutative[1] or quasi-commutative[2] reduction additional syntactical restrictions for the multiplication of the head term of the polynomial were added. While the weakenings of strong reduction on one side gave more information on the reduction steps, the expressiveness of the right ideal congruence by the reflexive transitive symmetric closure of such a weaker reduction was lost. To recover this property of reduction the concept of saturation was used to enrich the sets of polynomials used for reduction.

[1]for commutative monoids only

[2]for nilpotent groups only

But in general for none of these reductions $p \xrightarrow{*}_F 0$ implies $\alpha \cdot p * w \xrightarrow{*}_F 0$, which is a crucial lemma in Buchberger's original approach of characterizing Gröbner bases by s-polynomials and in most of the generalizations known in literature. In fact, in defining prefix respectively commutative reduction, a weaker condition to characterize Gröbner bases by corresponding s-polynomials could be proved. These reductions are motivated syntactically and correspond to polynomial multiples, where the multiplication of the head term can be interpreted by a multiplication not only in the monoid but also in the set of syntactical elements from which the representatives for the monoid elements are taken, e.g., a free monoid respectively a free commutative monoid. These monoids now allow admissible well-founded orderings and in using such an ordering to induce the ordering on the respective monoid, we can characterize Gröbner bases by localized s-polynomials. This approach resulted in a procedure to enumerate a prefix Gröbner basis for a finitely generated ideal in a monoid ring. The procedure could be modified to give terminating algorithms for special classes of monoids and groups, e.g., finite monoids, free monoids, free groups, plain groups and context-free groups. Similarly, for commutative monoid rings a terminating algorithm could be provided.

The key idea of introducing reduction and Gröbner bases to other structures used in this work is as follows:

1. Define a weakening of strong reduction, say w-reduction, appropriate to the respective structure in the following sense:
   If for some polynomials $p, g \in \mathbf{K}[\mathcal{M}]$ and a set of polynomials $F \subseteq \mathbf{K}[\mathcal{M}]$ we have $p \longrightarrow^{\mathrm{w}}_g 0$ and $g \xrightarrow{*}^{\mathrm{w}}_F 0$, then there exists a w-representation of p such that one term in this representation equals the head term of p and all other terms are smaller[3].

2. Define saturation with respect to w-reduction.

3. Define s-polynomials with respect to w-reduction.

Then the following holds:

For a w-saturated set $F \subset \mathbf{K}[\mathcal{M}]$ the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}^{\mathrm{w}}_F 0$.*

2. *For all polynomials $f_k, f_l \in F$ we have $\mathsf{spol}_w(f_k, f_l) \xrightarrow{*}^{\mathrm{w}}_F 0$.*

A further application of this approach is given in the section on nilpotent groups, where we define quasi-commutative reduction and show the existence of finite Gröbner bases for right ideals and ideals.

We close by giving possible further points of interest: On the theoretical side, the class of polycyclic groups is a good candidate to extend our approach of generalizing Gröbner bases. It is known from literature that polycyclic groups have solvable subgroup problem [Wi89] and that polycyclic group rings have solvable membership

[3] Variations of this lemma are e.g. the lemmata 4.4.13 and 4.5.15.

problem [Ha59, BaCaMi81]. On the practical side, the algorithms provided in this thesis should be improved, implemented and complexity bounds should be investigated. A possible guide for the latter task can be found in the literature on the subgroup problem for the respective classes of groups [AvMa84, CrOt94, KuMa89].

Bibliography

[Ap88] J. Apel. *Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung.* Dissertation. Universität Leipzig. 1988.

[ApLa88] J. Apel and W. Lassner. *An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras.* Journal of Symbolic Computation(1988) 6. pp 361-370.

[AvMa84] J. Avenhaus and K. Madlener. *The Nielsen Reduction and P-Complete Problems in Free Groups.* Theoretical Computer Science 32(1984), pp. 61-76.

[AvMaOt86] J. Avenhaus, K. Madlener, F. Otto. *Groups Presented by Finite Two-Monadic Church-Rosser Thue Systems.* Transactions of the American Mathematical Society, Volume 297(1986). pp 427-443.

[Ba81] G. Bauer. *Zur Darstellung von Monoiden durch konfluente Reduktionssysteme.* Dissertation. Universität Kaiserslautern. 1981.

[BaCaMi81] G. Baumslag, F. Cannonito and C. Miller, III. *Computable Algebra and Group Embeddings.* Journal of Algebra 69(1981). pp 186-212.

[BeWe92] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer Verlag(1992).

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

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

[Bu85] B. Buchberger. *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.* N. K. Bose (ed). Multidimensional Systems Theory. Chapter 6. 1985. Dordrecht: Reidel. pp 184-232.

[Bu87] B. Buchberger. *Applications of Gröbner Bases in Non-Linear Computational Geometry.* In: R. Janßen (ed.), Trends in Computer Algebra, Springer LNCS 296(1987), pp 52-80.

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

[CoLiOS92] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer Verlag(1992).

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

[De89] T. Deiß. *Berechnung von Gröbnerbasen, effizienzsteigernde Maßnahmen und Restklassenringe als Koeffizientenbereich.* Diplomarbeit. Universität Kaiserslautern. 1989.

[Di86] V. Diekert. *Commutative Monoids Have Complete Presentations by Free (Non-Commutative) Monoids.* Theoretical Computer Science 46(1986), pp 319-327.

[Es86] C. Eschenbach. *Die Verwendung von Zeichenkettenordnungen im Zusammenhang mit Semi-Thue Systemen.* Technischer Bericht. Universität Hamburg. 1986.

[Ga88] T. Gateva-Ivanova and V. Latyshev. *On Recognizable Properties of Associative Algebras.* Journal of Symbolic Computation 6(1988). pp 371-388.

[GeCzLa92] K.O. Geddes, S.R. Czapor and G. Labahn. *Algorithms for Computer Algebra.* Kluwer Academic Publishers. Massachusettes(1992).

[Ha59] M. Hall, Jr. *The Theory of Groups.* Chelsea Publishing Company. New York(1959).

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

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

[He64] I.N. Herstein. *Topics in Algebra.* Xerox College Publishing. Lexington, Massachusetts. Toronto(1964).

[KaKa84] A. Kandri-Rody and D. Kapur. *An Algorithm for Computing the Gröbner Basis of a Polynomial Ideal over an Euclidean Ring.* Technical Information Series General Electric Company Corporate Research and Development Schenectady. NY 12345. Dec. 1984.

[KaKa88] A. Kandri-Rody and D. Kapur. *Computing a Gröbner Basis of a Polynomial Ideal over an Euclidean domain.* Journal of Symbolic Computation 6(1988). pp 37-57.

[KaMa86] D. Kapur and K. Madlener. Private communication.

[KaMa89] D. Kapur and K. Madlener. *A Completion Procedure for Computing a Canonical Basis for a $\mathcal{K}$-Subalgebra.* Proc. of Computers and Mathematics(1989).

[KaMe79] M.I. Kargapolov and Ju.I. Merzljakov. *Fundamentals of the Theory of Groups.* Springer Verlag(1979).

[KaNa85] D. Kapur and P. Narendran. *Constructing a Gröbner Basis for a Polynomial Ring.* Summary in Proceedings of Combinatorial Algorithms in Algebraic Structures. Otzenhausen(1985). Eds J. Avenhaus, K. Madlener. Universität Kaiserslautern.

[KaWe90] A. Kandri-Rody and V. Weispfenning. *Non-Commutative Gröbner Bases in Algebras of Solvable Type.* Journal of Symbolic Computation 9(1990). pp 1-26.

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

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

[Kr93] H. Kredel. *Solvable Polynomial Rings.* Verlag Shaker, Aachen. 1993.

[La85] W. Lassner. *Symbol Representations of Noncommutative Algebras.* EUROCAL'85. Springer LNCS 204, pp. 99-115.

[La76] M. Lauer. *Kanonische Repräsentanten für die Restklassen nach einem Polynomideal.* Diplomarbeit. Universität Kaiserslautern. 1976.

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

[Ma86] K. Madlener. *Existence and Construction of Gröbner Bases for Ideals in Reduction Rings.* Working paper. 1986.

[MaOt89] K. Madlener and F. Otto. *About the Descriptive Power of Certain Classes of Finite String-Rewriting Systems.* Theoretical Computer Science 67(1989). pp 143-172.

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

[MaRe93a] K. Madlener and B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* SEKI Report SR-93-08. Universität Kaiserslautern.

[MaRe93b] K. Madlener and B. Reinert. *Computing Gröbner Bases in Monoid and Group Rings.* Proc. ISSAC'93. pp 254-263.

[MoMoTr92] H.M. Möller, T. Mora and C. Traverso. *Gröbner Bases Computation Using Syzygies.* Proc. ISSAC'92. pp 320-328.

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

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

[NaOD89] P. Narendran and C. Ó'Dúnlaing. *Cancellativity in Finitely Presented Semigroups.* Journal of Symbolic Computation 7(1989). pp 457-472.

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

[Pa85] L. Pan. *On the Gröbner Bases of Ideals in Polynomial Rings over a Prinicipal Ideal Domain.* University of California, Santa Barbara, Department of Mathematics, Internal Manuscript, 1985.

[Ro93] A. Rosenmann. *An Algorithm for Constructing Gröbner and Free Schreier Bases in Free Group Algebras.* Preprint No.3(1993). Institut für Experimentelle Mathematik. Universität GH Essen.

[Ro93] A. Rosenmann. *An Algorithm for Constructing Gröbner and Free Schreier Bases in Free Group Algebras.* Journal of Symbolic Computation 16(1993). pp 523-549.

[Sa90] A. Sattler-Klein. *Divergence Phenomena during Completion.* Interner Bericht 203 \ 90 (1990). Universität Kaiserslautern.

[Se83] D. Segal. *Polycyclic Groups.* Cambridge University Press. 1983.

[Si87] C. Sims. *Verifying Nilpotence.* Journal of Symbolic Computation 3(1987). pp 231-247.

[Si90] C. Sims. *Implementing the Baumslag-Cannonito-Miller Polycyclic Quotient Algorithm.* Journal of Symbolic Computation 9(1990). pp 707-723.

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

[St85] S. Stifter. *Computation of Gröbner Bases over the Integers and in General Reduction Rings.* Diplomarbeit. Johannes Kepler Universität Linz. 1985.

[St87] S. Stifter. *A generalization of Reduction Rings.* Journal of Symbolic Computation 4(1987). pp 351-364.

[St90] T. Stokes. *Gröbner Bases in Exterior Algebras.* Journal of Automated Reasoning 6(1990). pp 233-250.

[We87] V. Weispfenning. *Gröbner Basis for Polynomial Ideals over Commutative Regular Rings.* Proc. EUROCAL'87. Springer LNCS 378. pp 336-347.

[We92] V. Weispfenning. *Finite Gröbner Bases in Non-Noetherian Skew Polynomial Rings.* Proc. ISSAC'92. pp 329-334.

[Wi84] F. Winkler. *The Church-Rosser Property in Computer Algebra and Special Theorem Proving: An Investigation of Critical Pair Completion Algorithms.* Dissertation. Universität Linz. 1984.

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

[Zi87] M. Zimnol. *Beispiele algebraischer Reduktionsstrukturen.* Diplomarbeit. Universität Kaiserslautern. 1987.

Curriculum vitae

Persönliche Daten

Name	Birgit Reinert, geborene Weber
Geburtsdatum	6.11.1964
Geburtsort	Landstuhl
Familienstand	verheiratet
Staatsangehörigkeit	deutsch

Schulausbildung

08/70 – 12/71	Grundschule in El Paso/Texas, USA
01/72 – 03/73	Grundschule in Huntsville/Alabama, USA
04/73 – 07/75	Grundschule in Spesbach/Pfalz
08/75 – 06/84	Staatliches Gymnasium in Landstuhl Abschluß: Abitur

Hochschulstudium

10/84 – 09/89	Mathematik mit Nebenfach Informatik an der Universität Kaiserslautern Abschluß: Diplom-Mathematiker

Berufstätigkeit

10/89 – 03/95	Wissenschaftlicher Mitarbeiter in der Arbeitsgruppe "Grundlagen der Informatik" von Prof. Dr. K. Madlener Universität Kaiserslautern