Computational Improvements for Non-Commutative Gröbner Bases over $\mathbb{Z}/m\mathbb{Z}$

Tobias Metzlaff

vorgelegt dem Fachbereich Mathematik der RWTH Aachen University zur Verleihung des akademischen Grades

Master of Science

Erstgutachter: Priv.-Doz. Dr. Viktor Levandovskyy
Zweitgutachterin: Prof. Dr. Eva Zerz

Lehrstuhl D für Mathematik

Abstract

Commutative Gröbner bases over fields $\mathbb{K}$ have the strong property of yielding canonical reductions, which is equivalent to having Gröbner representations for polynomials. The transition to the free algebra $\mathbb{K}\langle X\rangle$ is essential for the understanding of $\mathbb{K}$-algebras as quotients of the tensor algebra. Furthermore, Gröbner theory inherits properties from the commutative case for finitely generated ideals. This motivates the idea of introducing non-commutative Gröbner bases for the free polynomial ring over the integers $\mathbb{Z}\langle X\rangle$. The main goal is to achieve a version of Buchberger's algorithm that uses criteria to determine zero reductions of pairs. After a revisit on commutative Gröbner bases over fields, we introduce the general case with arbitrary monoids and commutative, unital coefficient rings. This results in important insights concerning the structure of left syzygy modules and justifies the use of S-polynomials. However, to obtain the strength of Gröbner bases over fields we need to introduce new G-polynomials next to S-polynomials, to ensure the divisibility of coefficients. Therefore, we analyze the commutative case first and obtain criteria that resemble the product criterion and the chain criterion. New phenomena arise when dealing with non-commutative polynomials, which lead to infinite Gröbner bases and require adjustments of the criteria. The lack of a general product criterion over rings gives rise to a new definition of S- and G-polynomials, which goes beyond divisibility relations of leading monomials. An implementation of Buchberger's algorithm in the computer algebra system Singular [24] is possible with the Singular:Letterplace subsystem [25] to compute Gröbner bases with a degree-bound.

Kommutative Gröbner Basen über Körpern $\mathbb{K}$ haben die starke Eigenschaft, einen eindeutigen Rest nach Reduktion zu erzeugen, was äquivalent dazu ist, über eine Gröbner Darstellung für Polynome zu verfügen. Der Übergang zur freien Algebra $\mathbb{K}\langle X\rangle$ ist für das Verständnis von $\mathbb{K}$-algebren als Quotienten der Tensoralgebra unerlässlich. Des Weiteren erbt die Gröbner-Theorie Eigenschaften aus dem kommutativen Fall für endlich erzeugte Ideale. Dies motiviert die Idee, nicht-kommutative Gröbner-Basen für freie Polynomringe über den ganzen Zahlen $\mathbb{Z}\langle X\rangle$ einzuführen. Ziel ist es, eine Version des Buchberger Algorithmus zu erhalten, der Kriterien verwendet, um Reduktionen zu Null vorauszusagen. Nach einer Wiederholung von kommutativen Gröbner Basen über Körpern, stellen wir den allgemeinen Fall mit beliebigen Monoiden und kommutativen Koeffizientenringen mit Eins vor. Dies liefert wichtige Erkenntnisse über die Struktur von Links-Syzygienmoduln und rechtfertigt den Gebrauch von S-Polynomen. Um jedoch die Stärke von Gröbner Basen über Körpern zu erhalten, müssen neben S-Polynomen auch neue G-Polynome eingeführt werden, um Teilbarkeit von Koeffizienten zu gewährleisten. Deshalb analysiert man zunächst den kommutativen Fall und erhält Kriterien, die dem Produktkriterium und dem Kettenkriterium ähneln. Die Fortsetzung mit nicht-kommutativen Polynomen führt zu neuen Phänomenen, die es im Allgemeinen nicht möglich machen, endliche Gröbner Basen zu finden, und erfordern eine Anpassung der Kriterien. Das Fehlen eines allgemeinen Produktkriteriums führt zu einer neuen Definition von S- und G-Polynomen, die über Teilbarkeitsrelationen von Leitmonomen hinausgeht. Eine Implementierung des Buchberger Algorithmus mit Gradschranke in das Computeralgebra System Singular [24] ist mit dem Teilsystem Singular:Letterplace [25] möglich.

Statutory Declaration in Lieu of an Oath

I hereby declare in lieu of an oath that I have completed the Master's thesis entitled

Computational Improvements for Non-Commutative Gröbner Bases over $\mathbb{Z}/m\mathbb{Z}$

independently and without illegitimate assistance from third parties (such as academic ghostwriters). I have used no other than the specified sources and aids. In case that the thesis is additionally submitted in an electronic format, I declare that the written and electronic versions are fully identical. The thesis has not been submitted to any examination body in this, or similar, form.

Eidesstattliche Versicherung

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Masterarbeit mit dem Titel

Computational Improvements for Non-Commutative Gröbner Bases over $\mathbb{Z}/m\mathbb{Z}$

selbstständig und ohne unzulässige fremde Hilfe (insbes. akademisches Ghostwriting) erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt. Für den Fall, dass die Arbeit zusätzlich auf einem Datenträger eingereicht wird, erkläre ich, dass die schriftliche und die elektronische Form vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Tobias Metzlaff

Acknowledgements

I would like to take this opportunity to thank my supervisor Viktor Levandovskyy for his time and support as a mentor during the work on this thesis.
Also, I am grateful to Eva Zerz for reviewing this thesis and whose lectures have always been a great source of motivation and fascination.
Furthermore, my thanks go to all coworkers at Lehrstuhl D für Mathematik, especially Karim Abou Zeid, who is working alongside Viktor Levandovskyy on the implementation of the theoretical results.
Last, but definitely not least, I would like to thank my family for the emotional support and care during my studies at the RWTH Aachen University.

Contents

1 Introduction **5**

2 Revisit: Commutative Gröbner bases over fields **7**

3 General setup **11**

4 Non-commutative Gröbner bases and syzygies **13**

5 Commutative Gröbner bases over Euclidean domains **29**

6 Commutative Gröbner bases over principal ideal rings **45**

7 Non-commutative Gröbner bases over Euclidean domains **52**

References **83**

A Appendix **86**

1 Introduction

Gröbner basis theory was introduced by Bruno Buchberger in 1965 for commutative polynomial rings over fields and ever since then it has been used for effective computations. Over the years the theory was extended to both commutative and non-commutative structures such as polynomial algebras or quantum groups and found applications in systems theory, optimization, modelling and theoretical physics. It is one of the most famous and worked-on techniques in computer algebra.
This Master thesis deals with polynomial rings over Euclidean domains such as the integers $\mathbb{Z}$ and principal ideal rings, represented by $\mathbb{Z}/m\mathbb{Z}$. Gröbner bases over fields give rise to canonical reductions and allow us to solve the ideal membership problem which is related to fundamental questions of algebraic mathematics. These canonical reductions give the polynomial ring the structure of a direct sum with respect to a given ideal, which makes it possible to compute quotients and dimensions in multivariate polynomial rings. We give a brief overview on Gröbner basis over fields in the first chapter to point out certain strengths which we desire to maintain over rings.
Several approaches were made for commutative polynomial rings over Euclidean domains, including early publications from Buchberger, Kapur and Kandri-Rody in independent and different ways.
In 1996 F. Leon Pritchard published a paper [7], in which he discussed the ideal membership problem for non-commutative polynomials over principal ideal rings by using critical sequences. His work was included in Teo Mora's "Solving Polynomial Equation Systems, 4" [14] and refered to as Pritchard's Procedure. An important result that we present is the basic structure of left syzygy modules.
However, the strength of Gröbner bases over fields is lost in Pritchards approach. In 2012 Daniel Lichtblau [6] extended the work of Buchberger [19] and Kandri-Rody, Kapur [18] and presented criteria to determine, whether a pair of polynomials needs to be considered in Buchberger's algorithm. Over fields, these are well known as product- and chain criterion. Eder, Pfister, Popescu and Hofmann targeted the problems of coefficient swell and modular techniques using factorizations for which they presented new algorithms in [1], [2] and [3].
The transition from commutative to non-commutative polynomial rings is linked to problems that result from non-Noetherianity. Although an ideal may be finitely generated, it usually does not have a finite Gröbner basis, even if there is such a basis over fields. Therefore, we adopt degree-bounded computations. Over fields, we only need to consider non-trivial overlap relations between leading monomials, because of the product criterion. This is in general not the case, when dealing with non-invertible leading coefficients. It is still possible to have infinite Gröbner bases over fields and we point out here, that the product criterion does not exclude this phenomenon. The only implication that we have is that the existence of a finite Gröbner basis over a ring guarantees the existence of such a basis over its quotient field. To develop an algorithm that computes such a degree-bounded Gröbner basis, it is essential to analyze the behaviour of polynomial pairs and the atomic structure of the ring. This leads to a new definition of S-polynomials.
The Singular:Letterplace subsystem [25], of which the idea was introduced in [5] by Levandovskyy and La Scala, is a tool to compute non-commutative Gröbner bases

over fields with given commutative implementations in computer algebra systems. We extend this to work over Euclidean rings and translate new product and chain criteria to be applied with the SINGULAR:LETTERPLACE subsystem. These algorithms will be implemented into the computer algebra system SINGULAR [24] by my supervisor Viktor Levandovskyy and my colleague Karim Abou Zeid.
Simultaneously to Buchberger, Heisuke Hironaka introduced the term standard basis, which is used today in a more general sense and especially when dealing with localizations of polynomial rings, by means of local or mixed orderings. We focus on global monomial orderings on non-commutative rings, since the approach of Hironaka does not seem to be broadly generalizable.

2 Revisit: Commutative Gröbner bases over fields

In this chapter we will give a revision on Gröbner bases for the well known setting over fields. Let $\mathbb{K}$ be a field and $\mathcal{P} = \mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ the commutative polynomial ring over $\mathbb{K}$ with n indeterminates. Given an ideal of $\mathcal{P}$ by a generating set, we want to decide, if an element of $\mathcal{P}$ is contained in the ideal, the so called ideal membership problem. Finding a solution of this problem yields the answer to a whole collection of further problems concerning equations over algebraically closed fields, dimension theory or computation of generators for intersections of ideals. For $n = 1$ this is easy to achieve via Euclidean division, since $\mathbb{K}[X]$ is a principal ideal domain. This is in general not true, however, there is a property that ensures the solvability of the above problems and the termination of algorithms. Of course we talk about the Noetherian property.

Lemma 2.1. (**Hilbert's basis theorem**, cf. [20], Satz 1.8)
Let $\mathcal{R}$ be a commutative ring with 1. If $\mathcal{R}$ is Noetherian, then so is the commutative polynomial ring with one indeterminate $\mathcal{R}[x]$.

Since fields are Noetherian and $\mathcal{P} = \mathbb{K}[x_1, \ldots, x_{n-1}][x_n]$, we see that $\mathcal{P}$ is Noetherian. More precisely $\mathcal{P}$ is a Noetherian, factorial domain. Therefore, every ideal of $\mathcal{P}$ is generated by finitely many elements and every element has, up to units, a unique factorization.

Definition 2.2.

- An **admissible ordering** $\preceq$ on a commutative monoid $(N, +, e)$ is an ordering, which is agreeable with the monoid structure of N in the sense that
  1. $\preceq$ is reflexive, antisymmetric and transitive,
  2. $\preceq$ is total,
  3. $\mu \preceq \nu$ for $\mu, \nu \in N$ implies $\mu + \lambda \preceq \nu + \lambda$ for all $\lambda \in N$ and
  4. every non-empty subset of N has a smallest element and e, the unitary element of N, is the smallest element of N, i.e. $e \prec \lambda$ for all $\lambda \in N \setminus \{e\}$.
- Let $\preceq$ be an admissible ordering on N and $F \subseteq \mathcal{P} \setminus \{0\}$ finite. A finite linear combination
$$\sum_{f \in F,\, \nu \in N} c_{f,\nu} x_\nu f$$
with $c_{f,\nu} \in \mathbb{K}$, $x_\nu \in X$, is called an **admissible combination** of F, if the leading monomials of $x_\nu f$ w.r.t. $\preceq$ and with $c_{\nu,f} \neq 0$ are pairwise distinct.

Example 2.3.
Consider $N = \mathbb{N}_0^n$ and let $\mu, \nu \in \mathbb{N}_0^n$. The following are global monomial orderings.

- *lexicographical ordering*: We write $\mu \prec_{\text{lex}} \nu$, if there is $1 \leq k \leq n$, such that $\mu_1 = \nu_1, \ldots, \mu_{k-1} = \nu_{k-1}$ and $\mu_k < \nu_k$.

- *graded lexicographical ordering*: We write $\mu \prec_{\text{grlex}} \nu$, if $|\mu| < |\nu|$ or $|\mu| = |\nu|$ and $\mu \prec_{\text{lex}} \nu$. Hereby $|\mu| := \sum_{i=1}^{n} \mu_i$ denotes the length of μ.

Sometimes it is useful to extend a given ordering to compare polynomials in $\mathcal{P}^{1\times p}$ for some $p \in \mathbb{N}$.

Lemma 2.4. (cf. [22], Lemma 5.1)
Let $\preceq$ be an admissible ordering on a monoid $(N, +, e)$. This can be extended to a well ordering on $N \times \{1, \ldots, p\}$ for any $p \in \mathbb{N}$ by term-over-position

$$(\mu, i) \preceq_{\text{top}} (\nu, j), \text{ if } \mu \prec \nu \text{ or } (\mu = \nu \text{ and } i \leq j)$$

or position-over-term

$$(\mu, i) \preceq_{\text{pot}} (\nu, j), \text{ if } i < j \text{ or } (i = j \text{ and } \mu \preceq \nu).$$

Proof.
We need to show that $\preceq_{\text{top}}$ is a well ordering. Consider a descending chain $(\mu_1, i_1) \succeq_{\text{top}} (\mu_2, i_2) \succeq_{\text{top}} \ldots$ in $N \times \{1, \ldots, p\}$. Then we obtain an ascending chain $M_1 \subseteq M_2 \subseteq \ldots$ of submodules of $\mathcal{P}^{1\times p}$ with $M_k := \langle x^{\mu_1} e_{i_1}, \ldots, x^{\mu_k} e_{i_k} \rangle$. But $\mathcal{P}$ is Noetherian and $\mathcal{P}^{1\times p}$ is finitely generated, hence this chain becomes stationary at some k and for all $l \geq k$ there exist $a_j \in \mathcal{P}$ with

$$x^{\mu_l} e_{i_l} = \sum_{j=1}^{k} a_j x^{\mu_j} e_{i_j}$$

or equivalently

$$x^{\mu_l} = \sum_{i_j = i_l} a_j x^{\mu_j}.$$

Then there exists a $\lambda \in N$ with $\mu_l = \mu_j + \lambda \succeq \mu_j$ ($\preceq$ is admissible) for some $j \leq k$ with $i_j = i_l$. Thus $(\mu_l, i_l) \succeq_{\text{top}} (\mu_j, i_j) \succeq_{\text{top}} (\mu_k, i_k) \succeq_{\text{top}} (\mu_l, i_l)$, since $j \leq k \leq l$, but then $(\mu_k, i_k) = (\mu_l, i_l)$ for all $l \geq k$, which means that the original chain becomes stationary. □

For $\mu \in \mathbb{N}_0^n$ we set $x^\mu := x^{\mu_1} \cdots x^{\mu_n}$. Let $f = \sum_\mu r_\mu x^\mu \in \mathcal{P} \setminus \{0\}$ with $r_\mu \in \mathcal{R}$. Then we define $\deg(f) := \max_{\preceq}\{\mu \in \mathbb{N}_0^n \mid r_\mu \neq 0\}$ w.r.t. an admissible ordering on $\mathbb{N}_0^n$. Furthermore, for $\mathcal{G} \subseteq \mathcal{P}$ let $\deg(\mathcal{G}) := \{\deg(\mathcal{G}) \mid f \in \mathcal{G} \setminus \{0\}\} \subseteq \mathbb{N}_0^n$. For an ideal $\mathcal{I} \subseteq \mathcal{P}$ we have $\deg(\mathcal{I}) = \deg(\mathcal{I}) + \mathbb{N}_0^n$. If $\mathcal{G}$ is a generating set for $\mathcal{I}$, then $\deg(\mathcal{G}) + \mathbb{N}_0^n \subseteq \deg(\mathcal{I})$, but "$\supseteq$" is not guaranteed and clearly linked to admissible combinations and the admissible ordering. Assume for example that $f \in \mathcal{I}$ results from a combination of $\mathcal{G}$, such that the leading terms w.r.t. $\preceq$ cancel each other out. Therefore, the combination is not admissible.

Theorem 2.5. (cf. [20], Satz 2.4)
Let $f \in \mathcal{P}$ and $F \subseteq \mathcal{P} \setminus \{0\}$ finite. Then there is an admissible combination g of F with $f = g$ or $\deg(h-g) \notin \deg(F)+\mathbb{N}_0^n$. We call $h-g$ a **remainder** after division of h through $\mathcal{G}$.

Such a remainder is not uniquely determined. We are interested in finite sets with this specific property.

Theorem 2.6. (cf. [20], Satz 2.5, Folgerung 2.6)
Let $\{0\} \neq \mathcal{I} \subseteq \mathcal{P}$ be an ideal, $\mathcal{G} \subseteq \mathcal{I} \setminus \{0\}$ a finite subset and $\preceq$ an admissible ordering on $\mathbb{N}_0^n$. The following are equivalent.

1. $\deg(\mathcal{I}) = \deg(\mathcal{G}) + \mathbb{N}_0^n$.
2. For $f \in \mathcal{I}$, every remainder after division of f through $\mathcal{G}$ is zero.
3. For $f \in \mathcal{I}$, one remainder after division of f through $\mathcal{G}$ is zero.
4. For $\mu \in \deg(\mathcal{G}) + \mathbb{N}_0^n$, we fix $\nu \in \mathbb{N}_0^N$ and $g \in \mathcal{G}$ with $\mu = \nu + \deg(g)$. Then with $g_\mu := x^\nu g$ we have

$$\mathcal{I} = \bigoplus_{\mu \in \deg(\mathcal{G})+\mathbb{N}_0^n} \mathbb{K} g_\mu.$$

If one of the equivalent conditions holds, then $\mathcal{G}$ is called a **Gröbner basis** for $\mathcal{I}$ and we obtain a decomposition of the polynomial ring

$$\mathcal{P} = \mathcal{I} \oplus \bigoplus_{\mu \notin \deg(\mathcal{G})+\mathbb{N}_0^n} \mathbb{K} x^\mu \cong \mathcal{I} \oplus \mathcal{P}/\mathcal{I}$$

as a $\mathbb{K}$-vectorspace. A Gröbner basis can be constructed with Buchberger's algorithm, which we will present later for a more general setup.

Example 2.7.

- *Integral linear programs in optimization*: Find a solution $x \in \mathbb{Z}^q$ for

$$\max_x cx, \text{ s.t. } Ax = b \text{ and } x \geq 0 \text{ (component-wise)}$$

with $A \in \mathbb{N}_0^{g \times q}$, $b \in \mathbb{N}_0^g$. For this problem let $\mathcal{P} = \mathbb{K}[y_1, \ldots, y_n]$. Then $Ax = b$ yields $g \in \mathbb{N}$ equations

$$a_{i,1}x_1 + \ldots + a_{i,q}x_q = b_i$$

or equivalently polynomial equations

$$y_i^{a_{i,1}x_1+\ldots+a_{i,q}x_q} = y_i^{b_i}$$

over $\mathcal{P}$ which can be combined as

$$\prod_{i=1}^{g} y_i^{a_{i,1}x_1+\ldots+a_{i,q}x_q} = \prod_{i=1}^{g} y_i^{b_i}.$$

After rearranging the factors we obtain

$$\prod_{j=1}^{q} (\underbrace{y_1^{a_{1,j}} \ldots y_g^{a_{g,j}}}_{=:z_j})^{x_j} = \prod_{j=1}^{q} z_j^{x_j} = \prod_{i=1}^{g} y_i^{b_i}.$$

Let $\mathcal{I}$ be the ideal of the polynomial ring $\tilde{\mathcal{P}} = \mathbb{K}[z_1, \ldots, z_q, y_1, \ldots, y_g]$ which is generated by the elements $z_j - y_1^{a_{1,j}} \ldots y_g^{a_{g,j}}$ and determine a Gröbner basis $\mathcal{G}$ of $\mathcal{I}$ w.r.t. an admissible ordering. One can show that the linear program has an optimal solution x, if and only if the monomial $y_1^{b_1} \ldots y_g^{b_g}$ has $z_1^{x_1} \ldots z_q^{x_q}$ as a remainder after division through $\mathcal{G}$.

- *Algebraic systems theory*: Let $\mathcal{D} = \mathbb{K}[\sigma_1, \ldots, \sigma_n]$ and $\mathcal{A} = \mathbb{K}^{\mathbb{N}^n}$ a $\mathcal{D}$-left module with $(\sigma_i f)(t_1, \ldots, t_n) = f(t_1, \ldots, t_i + 1, \ldots, t_n)$. We say that an abstract linear system $\mathcal{B} = \{w \in \mathcal{A}^q | Rw = 0\}$ with $R \in \mathcal{D}^{g \times q}$ has a **free variable** w_i, if the canonical projection $\mathcal{B} \to \mathcal{A}$, $w \mapsto w_i$ is surjective. Otherwise $\mathcal{B}$ is called **autonomous**. Since $\mathcal{A}$ is an injective cogenerator over $\mathcal{D}$, it follows that $\mathcal{B}$ is autonomous, if and only if the associated system module $\mathcal{M} = \mathcal{D}^{1\times q}/\mathcal{D}^{1\times g}R$ is torsion (cf. [22], Lemma 3.3). This motivates the idea to measure the autonomy of a system with the **dimension** of $\mathcal{M}$, which is defined as the Krull-dimension of $\mathcal{D}/\mathrm{ann}(\mathcal{M})$. Note that a Gröbner basis for $\mathrm{ann}(\mathcal{M})$ yields a decomposition of $\mathcal{D}/\mathrm{ann}(\mathcal{M})$ as a $\mathbb{K}$-vectorspace. We say that $\mathcal{B}$ has **autonomy degree** at least m, if $\dim(\mathcal{M}) < n - r$. As a polynomial ring over a field, the Krull-dimension of $\mathcal{D}$ is n. Hence $r \in \{-1, \ldots, n\}$ with $r = n$ corresponding to $\mathcal{B} = 0$, $r = n - 1$ corresponding to $\mathcal{B}$ being finite dimensional as a $\mathbb{K}$-space, and $r = 0$ corresponding to $\mathcal{B}$ simply being autonomous (cf. [22], Theorem 5.3).
  To determine the dimension we extend an admissible ordering on $\mathbb{N}_0^n$ to an ordering on $\mathbb{N}_0^n \times \{1, \ldots, p\}$. Then for any element $m \in \mathcal{D}^{1\times p}$ we define the degree as usual. Let $\Gamma := \mathbb{N}_0^n \times \{1, \ldots, p\} \setminus \deg(\mathcal{D}^{1\times p}R)$ and $\Gamma_j := \{\nu \in \mathbb{N}_0^n : (\nu, j) \in \Gamma\}$. We define

  $$d(\Gamma) := \max\{0 \leq k \leq n \mid \exists\, 1 \leq j_1 < \ldots < j_k \leq n,\, 1 \leq j \leq p : \langle e_{j_1}, \ldots, e_{j_k}\rangle_{\mathbb{N}} \subseteq \Gamma_j\}.$$

  One can show that $d(\Gamma)$ corresponds to the dimension of $\mathcal{B}$ (cf. [22], ch. 5.2).

3 General setup

Before we start with Gröbner bases for ideals in non-commutative polynomial rings, we have to fix some notations. The set $\mathbb{N}_0^n$ works fine for the definition of a term ordering on commutative polynomials, but when dealing with non-commutative structures or monoid extensions, a more general setup is required. In this chapter we will give the necessary definitions.
Let $\mathcal{R}$ be a commutative, unital ring and $(X, \cdot, 1)$ a monoid. It is convenient to denote the unitary elements of $\mathcal{R}$ and of X both by 1. A **global monomial ordering** $\preceq$ on X is a well ordering which is agreeable with the monoid structure in the sense that

1. $\preceq$ is reflexive, antisymmetric and transitive,
2. $\preceq$ is total,
3. $\mu \preceq \nu$ for $\mu, \nu \in X$ implies $\lambda_1 \cdot \mu \cdot \lambda_2 \preceq \lambda_1 \cdot \nu \cdot \lambda_2$ for all $\lambda_1, \lambda_2 \in X$ and
4. every non-empty subset of X has a smallest element and 1 is the smallest element of X, i.e. $1 \preceq \lambda$ for all $\lambda \in X$.

Let $\mathcal{P} = \mathcal{R}\langle X \rangle$ be the **monoid ring** of X over $\mathcal{R}$. This is the set of all maps $\phi : X \to \mathcal{R}$ with finite support and can be identified by the set of formal sums $\sum_{x \in X} \phi_x x$ with $\phi_x := \phi(x) = 0$ for all, but finitely many $x \in X$. Clearly this is a ring with addition $(\phi + \psi)_x = \phi_x + \psi_x$ and multiplication $(\phi \cdot \psi)_x = \sum_{yz=x} \phi_y \psi_z$. Furthermore, $\mathcal{P}$ is the finitely presented commutative polynomial ring over $\mathcal{R}$, if and only if X is commutative and based on (i.e. generated by) a finite alphabet. If X is commutative, then we write $\mathcal{P} = \mathcal{R}[X]$.
For $F = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ with $|F| = m$ we consider the left $\mathcal{R}$-module homomorphism $\pi : \mathcal{P}^{1\times m} \to \mathcal{P}$, which is defined by $e_i \mapsto f_i$, where e_i is the i-th standard basis vector of the free left $\mathcal{R}$-module $\mathcal{P}^{1\times m}$. An element $\alpha \in \mathcal{P}^{1\times m}$ with $\overline{\alpha} := \pi(\alpha) = 0$, i.e. $\sum_i \alpha_i f_i = 0$, is called a **left syzygy** of F. Clearly the set of all left syzygies of F is the kernel of π. Note, that it is not necessary to write left $\mathcal{R}$-module, since the definition of the multiplication on $\mathcal{P}$ indicates that elements of $\mathcal{R}$ and $\mathcal{P}$ commute with each other. However, $\mathcal{P}$ is non-commutative in general, hence we must write left (and analogously right) syzygy. The set of all left syzygies of F is denoted by $\mathrm{Syz}(F)$.
With respect to a global monomial ordering there exist unique elements $r \in \mathcal{R} \setminus \{0\}$ and $t \in X$ for any $f \in \mathcal{P} \setminus \{0\}$, such that $f = rt$+l.o.t. (lower order terms) or equivalently $f = \sum_{i=0}^{k} r_i t_i$ where $t_0 \prec t_1 \prec \ldots \prec t_k = t$ and $r_k = r \neq 0$. If $X = \langle x_1, \ldots, x_n \rangle$ is based on a finite alphabet, we can find $\nu^i \in \mathbb{N}_0^n$ for each t_i, such that $t_i = x^{\nu^i} := x_1^{\nu_1^i} \cdots x_n^{\nu_n^i}$ and can write $f = \sum_{i=0}^{k} r_i x^{\nu^i}$ or simply $f = \sum_\nu r_\nu x^\nu$. Then $\mathrm{LT}(f) = r_k x^{\nu^k}$ is called the **leading term**, $\mathrm{LM}(f) = x^{\nu^k}$ is called the **leading monomial**, $\mathrm{LC}(f) = r_k$ is called the **leading coefficient** and $\mathrm{tail}(f) = f - \mathrm{LT}(f)$ is called the **tail** of f with respect to $\preceq$. The **degree** of f is defined as $\deg(f) = \max\{|\nu^i| = \nu_1^i + \ldots + \nu_n^i \mid 0 \leq i \leq k\}$ and the **ecart** of f as $\mathrm{ecart}(f) = \deg(f) - \deg(\mathrm{LM}(f))$. For completeness we set $\mathrm{ecart}(0) = \deg(0) = -\infty$. The **leading ideal** or **ideal of leading terms** of $F \subseteq \mathcal{P}$ is the two sided ideal $\mathrm{L}(F)$ generated by all leading terms of the non-zero elements of F.

Definition 3.1.
Let $f \in \mathcal{P}$ and $\mathcal{G} \subseteq \mathcal{P}$ be a finite and ordered subset. A **weak normal form** of f w.r.t. $\mathcal{G}$ is a map $(f, \mathcal{G}) \mapsto \mathrm{NF}(f, \mathcal{G}) \in \mathcal{P}$ with

1. $\mathrm{NF}(0, \mathcal{G}) = 0$,
2. $\mathrm{NF}(f, \mathcal{G}) \neq 0$ implies $\mathrm{LT}(\mathrm{NF}(f, \mathcal{G})) \notin \mathrm{L}(\mathcal{G})$ and
3. $f - \mathrm{NF}(f, \mathcal{G}) \in \langle \mathcal{G} \rangle$.

Definition 3.2.
Let X be a free monoid on a finite alphabet $\{x_1, \ldots, x_n\}$ that is preordered by $x_1 \prec x_2 \prec \ldots \prec x_n$. Let $x = x_{i_1} \cdots x_{i_k}$, $y = x_{j_1} \cdots x_{j_l}$.

- We say that x is smaller than y in the **left lexicographical ordering**, denoted by $x \prec_{\mathrm{llex}} y$, if either there exists $1 \leq m \leq \min\{k, l\}$ with $x_{i_1} = y_{i_1}, \ldots, x_{i_{m-1}} = x_{i_{m-1}}$ and $x_{i_m} \prec y_{i_m}$, or if otherwise x divides y from the left, i.e. there exists $z \in X$, such that $y = xz$.
  Note, that this is not a monomial ordering in the non-commutative case, because it is not agreeable with the operation of the monoid. If $x \succ y$, then by the left lexicographical ordering we have $x \succ_{\mathrm{llex}} yx$. But, if $\preceq_{\mathrm{llex}}$ would be monomial, then $1 \prec_{\mathrm{llex}} y$ would imply $x \prec_{\mathrm{llex}} yx$, a contradiction.
- We say that x is smaller than y in the **graded left lexicographical ordering** or **degree left lexicographical ordering**, denoted by $x \prec_{\mathrm{grllex}} y$, if $|x| = k < l = |y|$ or $k = l$ and $x \prec_{\mathrm{llex}} y$. This is indeed a global monomial ordering.

Analogously one can define the right and graded/degree right lexicographical ordering.

Example 3.3.

- Let $\mathcal{P} = \mathcal{W}_1 := \mathbb{R}\langle t, \partial | \partial t = t\partial + 1 \rangle$ the first Weyl algebra. Then $\partial t^2 = t\partial t + t$ and thus $(\partial, -t)$ is a left syzygy of $\{t^2, \partial t + 1\}$. However, $t^2\partial - (\partial t + 1)t = -3t \neq 0$. Therefore, it is not a right syzygy.
- Let $f = x_1^2 + x_1 x_2^3 \in \mathbb{Z}[x_1, x_2]$. Then with $x_1 \succ x_2$ in the left lexicographical ordering we have $\deg(f) = 4$, $\deg(\mathrm{LM}(f)) = 2$ and $\mathrm{ecart}(f) = 2$.

4 Non-commutative Gröbner bases and syzygies

In this chapter we will introduce Gröbner basis theory for non-commutative polynomial rings with commutative, unital coefficient rings. The results are mostly based on the work of Pritchard [7]. After a characterization for Gröbner bases, we will present some statements for ring extensions and monomial extensions. Furthermore, we address the ideal membership problem with the result, that the question "$f \in \mathcal{I}$?" can only be determined in finitely many steps, if and only if f is actually contained in the ideal $\mathcal{I}$. This is done with the tool of critical sequences. We will see that having Gröbner basis, that remains a Gröbner basis after monoid extension, is an intrinsic property and independent of the choice of the basis. This leads to a generalized version of the PBW Theorem for Lie algebras.
Let $\mathcal{R}$ be a commutative, unital ring and $\preceq$ a global monomial ordering on a monoid X. We denote the polynomial ring over $\mathcal{R}$ by $\mathcal{P} = \mathcal{R}\langle X\rangle$.

Definition 4.1.
Let $\mathcal{G} \subseteq \mathcal{P}$ and $\mathcal{I} = \langle \mathcal{G}\rangle$ a two-sided ideal of $\mathcal{P}$. Then $\mathcal{G}$ is called **Gröbner basis** for $\mathcal{I}$, if $\mathrm{L}(\mathcal{I}) = \mathrm{L}(\mathcal{G})$.

In the non-commutative case we have to distinguish between multiplying monomials from the left and from the right to generate the two-sided ideal $\mathrm{L}(\mathcal{G})$. Let $\sim$ be the equivalence relation on $\mathcal{P} \otimes_{\mathcal{R}} \mathcal{P}^{\mathrm{opp}}$ that is given by

$$x_1 \otimes y_1 \sim x_2 \otimes y_2 \Leftrightarrow \forall t \in X : \; x_1 t y_1 = x_2 t y_2$$

for x_1, x_2, y_1, $y_2 \in X$. We denote $(\mathcal{P} \otimes_{\mathcal{R}} \mathcal{P}^{\mathrm{opp}})/\sim$ by $\mathcal{P}^e$ and call it the **enveloping polynomial ring**.

Remark 4.2.

- $\mathcal{P}^* := \mathcal{P} \otimes_{\mathcal{R}} \mathcal{P}^{\mathrm{opp}}$ is a unital ring with multiplication $\lambda_1(x_1 \otimes y_1) \cdot \lambda_2(x_2 \otimes y_2) = \lambda_1\lambda_2(x_1x_2 \otimes y_1y_2)$ for $\lambda_i \in \mathcal{R}$ and x_i, $y_i \in X$. Moreover, $\mathcal{P}$ is a left $\mathcal{P}^*$-module via $(x \otimes y)t = xty$. Therefore, ideals of $\mathcal{P}$ can be identified as left $\mathcal{P}^*$-submodules of $\mathcal{P}$. However, $\mathcal{P}$ is not a left $\mathcal{P}^*$-algebra, if X is non-commutative, because then $((x \otimes y)t_1)t_2 = xt_1yt_2 \neq xt_1t_2y = (x \otimes y)(t_1t_2)$ if t_2 and y do not commute. Thus the action of $\mathcal{P}^*$ on $\mathcal{P}$ is not associative.
- Similarly $\mathcal{P}$ is a left $\mathcal{P}^e$-submodule and we can identify ideals of $\mathcal{P}$ as left $\mathcal{P}^e$-submodules of $\mathcal{P}$.
- For $g \in \mathcal{P}$ let $\phi_g : \mathcal{P}^* \to \mathcal{P}$, $f \mapsto fg$ and $\mathcal{I} = \bigcap_{g\in\mathcal{P}} \ker(\phi_g)$. Then $\mathcal{P}^e \cong \mathcal{P}^*/\mathcal{I}$.

For $\mathcal{I} = \langle \mathcal{G}\rangle$ and $f \in \mathcal{I}$ we can find $g_i \in \mathcal{G}$, coefficients $\lambda_{ij} \in \mathcal{R}$ and monomials a_{ij}, $b_{ij} \in X$, such that

$$f = \sum_{i=1}^{m} \sum_{j=1}^{k_i} \lambda_{ij} a_{ij} g_i b_{ij}$$

for some $k_i \in \mathbb{N}$. With the above notation of the enveloping polynomial ring this translates to having polynomials $p_i \in \mathcal{P}^e$ with

$$p_i = \sum_{j=1}^{k_i} \lambda_{ij}(a_{ij} \otimes b_{ij})$$

and $f = \sum_{i=1}^{m} p_i g_i$. The degree, leading coefficient, leading monomial and leading term of $p_i \in \mathcal{P}^e$ is defined via the polynomial $p_i \cdot 1 = \sum_{j=1}^{k_i} \lambda_{ij} a_{ij} b_{ij} \in \mathcal{P}$.
It should be noted that the k_i are not bounded. Since we are interested in two-sided ideals, we need two-sided syzygies. The notation for a syzygy, which has entries in$\mathcal{P}^e$, comes in handy, but should not be confounded with strict left syzygies with entries in $\mathcal{P}$. Since $\mathcal{P}$ is a left $\mathcal{P}^e$-module, we use the term left syzygy.
Now let $f = \sum_{i=0}^{k} r_i t_i$ be an arbitrary element of $\mathcal{P}$ with coefficients $r_i \in \mathcal{R}$ and monomials t_i. We say that f is in **simplified form**, if all coefficients r_i are non-zero and the t_i are pairwise distinct. Analogously we say that an element of $\mathcal{P}^e$ is in simplified form.

Definition 4.3.
Let $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq \mathcal{P} \setminus \{0\}$ and $f \in \mathcal{P} \setminus \{0\}$.

- We say that f has a **Gröbner representation** w.r.t. $\mathcal{G}$, if $f = \sum_{i=1}^{m} p_i g_i$ for some $p_i \in \mathcal{P}^e \setminus \{0\}$ and $\mathrm{LM}(f) \geq \mathrm{LM}(p_i f_i)$ for all $1 \leq i \leq m$.
- We say that f **reduces** to some $h \in \mathcal{P}$ w.r.t. $\mathcal{G}$, if $h = 0$ or $\mathrm{LM}(f) \succ \mathrm{LM}(h)$ and $f - h$ has a Gröbner representation w.r.t. $\mathcal{G}$.
- Let $\alpha \in (\mathcal{P}^e)^{1\times m}$ be a left syzygy of $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq \mathcal{P}$, i.e. $\sum_{i=1}^{m} \alpha_i g_i = 0$. By $\mathrm{Syz}(\mathcal{G})$ we denote the set of all left syzygies of $\mathcal{G}$. Assume that for $\alpha \in \mathrm{Syz}(\mathcal{G})$ with $\alpha_i = \sum_{j=1}^{k_i} r_j^i \tau_j^i$, $\tau_j^i \in X^e$, there exist ρ_j^i such that $\tau_j^i = \rho_j^i t$ for some fixed $t \in X$. Then we call α **homogeneous of degree** t. An X-grading of $\mathrm{Syz}(\mathcal{G})$ is given by $\bigoplus_{t\in X} \mathrm{Syz}_t(\mathcal{G})$ where $\mathrm{Syz}_t(\mathcal{G})$ consists of all homogeneous left syzygies of $\mathcal{G}$ with degree t. Now assume that the left $\mathcal{P}$-module $\mathrm{Syz}(\mathcal{G})$ has a $\mathcal{P}^e$-basis H. We say that H is **homogeneous of degree** t if every element of H is homogeneous of degree t. Note that $\mathrm{Syz}(\mathcal{G})$ is not finitely generated in general.

Remark 4.4.
Under the assumptions of Definition 4.3, reduction is closed under transitivity. Let f reduce to h and let h reduce to $\tilde{h}$, both w.r.t. $\mathcal{G}$. Then $\mathrm{LM}(f) \succ \mathrm{LM}(h) \succ \mathrm{LM}(\tilde{h})$ and there exist $p_i, \tilde{p}_i \in \mathcal{P}^e$ such that $f - h = \sum_{i\in I} p_i g_i$ with $\mathrm{LM}(f - h) = \max\{\mathrm{LM}(p_i g_i)\}_{i\in I}$. Moreover, we have $h - \tilde{h} = \sum_{j\in J} \tilde{p}_j g_j$ with $\mathrm{LM}(h - \tilde{h}) = \max\{\mathrm{LM}(\tilde{p}_i g_i)\}_{j\in J}$. Especially

$$f - \tilde{h} = f - h + h - \tilde{h} = \sum_{i\in I} p_i g_i + \sum_{j\in J} \tilde{p}_j g_j = \sum_{k\in I\cup J} \hat{p}_k g_k$$

with $\hat{p}_k = p_k + \tilde{p}_k$, such that $p_k = 0$, if $k \notin I$, and $\tilde{p}_k = 0$, if $k \notin J$. This is a Gröbner representation of $f - \tilde{h}$ w.r.t. $\mathcal{G}$, because

$$\begin{aligned}\max\{\mathrm{LM}((p_k + \tilde{p}_k)g_k)\}_k &\preceq \max\{\mathrm{LM}(p_i g_i), \mathrm{LM}(\tilde{p}_j g_j)\}_{i,j} \\ &\preceq \max\{\mathrm{LM}(f-h), \mathrm{LM}(h-\tilde{h})\} \\ &= \mathrm{LM}(f-h) \\ &= \mathrm{LM}(f),\end{aligned}$$

because $\mathrm{LM}(f) \succ \mathrm{LM}(h)$. Therefore, we have equality and thus f reduces to $\tilde{h}$ w.r.t. $\mathcal{G}$.

The following is a characterization of Gröbner bases and similar to the commutative field case from chapter 2.

Theorem 4.5. (cf. [7], Theorem 1)
Let $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq \mathcal{P} \setminus \{0\}$, $\mathcal{I} = \langle \mathcal{G} \rangle$ and $M := \{\mathrm{LM}(g_i)\}_i$. Let $H = \{H_j = (h_1^j, \ldots, h_m^j)\}_j$ be a homogeneous basis for $\mathrm{Syz}(M)$ of degree t. The following are equivalent.

1. $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$.
2. Every $f \in \mathcal{I} \setminus \{0\}$ has a Gröbner representation w.r.t. $\mathcal{G}$.
3. Every polynomial $\sum_i h_i^j g_i$ has a Gröbner representation w.r.t. $\mathcal{G}$.
4. Every $f \in \mathcal{I} \setminus \{0\}$ reduces to zero w.r.t. $\mathcal{G}$.
5. Every polynomial $\sum_{i=1}^m h_i^j g_i$ reduces to zero w.r.t. $\mathcal{G}$

Proof.
For "1. $\Rightarrow$ 2." let $f \in \mathcal{I}$. Since $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$, we can write $\mathrm{LT}(f) = \sum_i p_i \mathrm{LT}(g_i)$ for some $p_i \in \mathcal{P}^e$ and we may assume without loss of generality that $\mathrm{LM}(p_i f_i) = \mathrm{LM}(f)$, if $p_i \neq 0$. Then $f' := f - \sum_i p_i g_i$ satisfies $\mathrm{LM}(f') \prec \mathrm{LM}(f)$ and either has a Gröbner representation or we repeat the procedure with $f'' := f' - \sum_i h_i' f_i$ for some $p_i' \in \mathcal{P}^e$. Since $\preceq$ is a well ordering, this process terminates and we obtain a Gröbner representation $f = \sum_i (p_i + p_i' + p_i'' + \ldots) g_i$ of f w.r.t. $\mathcal{G}$.
The implication "2. $\Rightarrow$ 3." is trivial.
We prove "3. $\Rightarrow$ 1." by showing that $\mathrm{LT}(f) \in \mathrm{L}(\mathcal{G})$ for any $f \in \mathcal{I}$. Let $f = \sum_i p_i g_i$ for some $p_i \in \mathcal{P}^e$ and let $t := \max\{\mathrm{LM}(p_i g_i)\}$. In the case where $\mathrm{LM}(f) = t$ we have $\mathrm{LT}(f) \in \mathrm{L}(\mathcal{G})$. Assume now that $\mathrm{LM}(f) \prec t$ and let $p_i = \sum_k r_k^i \tau_k^i$ be in simplified form with $r_k^i \in \mathcal{R}$ and $\tau_k^i \in X^e$. We define

$$\alpha_i := \sum_{\tau_k^i \mathrm{LM}(p_i) = t} r_k^i \tau_k^i.$$

Then by the assumption $\mathrm{LM}(f) \prec t$ we have $\alpha = [\alpha_1, \ldots, \alpha_m] \in \mathrm{Syz}(M)$. Since H is a basis of $\mathrm{Syz}(M)$, we can write $\alpha = \sum_j s_j H_j$ with $s_j \in \mathcal{P}^e$. Let $\sum_i \lambda_i^j g_i$ be a Gröbner

representation of $\sum_i h_i^j g_i$ w.r.t. $\mathcal{G}$ with $\mathrm{LM}(\lambda_i^j g_i) \prec \mathrm{LM}(g_j)$. Then

$$\begin{aligned} f &= \sum_i p_i g_i \\ &= \sum_i p_i g_i + \sum_i \alpha_i g_i - \sum_i \alpha_i g_i \\ &= \sum_i p_i g_i - \sum_i \alpha_i g_i + \sum_j s_j \left(\sum_i h_i^j g_i \right) \\ &= \sum_i p_i g_i - \alpha_i g_i + \left(\sum_j s_j \lambda_i^j \right) g_i \\ &= \sum_i \underbrace{\left(p_i - \alpha_i + \sum_j s_j \lambda_i^j \right)}_{=:p_i'} g_i \end{aligned}$$

is another representation of f with $t' := \max\{\mathrm{LM}(p_i' g_i)\} \prec t$. Since $\preceq$ is a global monomial ordering, this procedure terminates, when we arrive at $\mathrm{LM}(f)$ and we obtain a Gröbner representation of f w.r.t. $\mathcal{G}$. Especially we have $\mathrm{LT}(f) \in \mathrm{L}(\mathcal{G})$ and, therefore, $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$.
The implication "4. $\Rightarrow$ 5." is trivial.
To show "5. $\Rightarrow$ 3." let $h = \sum_i h_i^j g_i$ reduce to zero, which is a transitive process. Then for $h_0 := h$ there exists h_1, such that $\mathrm{LM}(h_1) \prec \mathrm{LM}(h_0)$ and $h_0 - h_1$ has a strong Gröbner representation. Iteratively we get a finite chain of reductions $h_0 - h_1$, $h_1 - h_2$, $\ldots$, $h_k - h_{k+1}$, $h_{k+1} = 0$ and thus $\sum_{i=0}^{k-1} h_i - h_{i+1}$ is a Gröbner representation of h.
Finally the proof of "1. $\Rightarrow$ 4." is analogous to "1. $\Rightarrow$ 2.". □

The polynomials $\sum_{i=1}^m h_i^j g_i$ in the above theorem are sometimes called S-polynomials, since the leading terms are eliminated due to the syzygy-property. We will use the term S-polynomial from chapter 5 on in a more specific sense and not adopt it here yet.

Proposition 4.6. (cf. [9], Theorem 3.6)
Let $\mathcal{S}$ be a ring with a ring homomorphism $\phi : \mathcal{R} \to \mathcal{S}$. We extend ϕ to $\mathcal{P}$. Then the following statements hold.

1. For any ideal $\mathcal{I} \subseteq \mathcal{P}$ we have $\mathrm{L}_{\mathcal{S}}(\langle \phi(\mathcal{I}) \rangle) \supseteq \langle \phi(\mathrm{L}_{\mathcal{R}}(I)) \rangle$.

2. $\mathcal{S}$ is a flat $\mathcal{R}$-module, if and only if for any sequence $\{a_i\}_i \in \mathcal{R}$ and $\{b_i\}_i \in \mathcal{S}$ of length ℓ, such that $\sum_i b_i \phi(a_i) = 0$, we can find $c_{ij} \in \mathcal{R}$ and $d_j \in \mathcal{S}$ with $\sum_i c_{ij} a_i = 0$ and $\sum_j d_j \phi(c_{ij}) = b_i$.

Proof.
For 1. note that $\langle \phi(\mathrm{L}_{\mathcal{R}}(I)) \rangle$ is generated by $\phi(\mathrm{LT}(f))$ for $f \in \mathcal{I}$ and either $\mathrm{LT}(f)$ maps to zero under ϕ (if $\phi(\mathrm{LC}(f)) = 0$) or $\phi(\mathrm{LT}(f)) = \mathrm{LT}(\phi(f)) \in \mathrm{L}_{\mathcal{S}}(\langle \phi(\mathcal{I}) \rangle)$.
In the case of 2. we will show the statement for arbitrary $\mathcal{R}$-modules $\mathcal{M}$ instead of $\mathcal{S}$, starting with $\mathcal{M}$ being flat. Let $\sum_i a_i m_i = 0$ for $a_i \in \mathcal{R}$ and $m_i \in \mathcal{M}$ with $1 \leq i \leq \ell$. The

matrix $R = [a_1, \ldots, a_\ell] \in \mathcal{R}^{1\times\ell}$ induces maps $\psi : \mathcal{R}^\ell \to \mathcal{R}$ and $\psi_\mathcal{M} : \mathcal{M}^\ell \to \mathcal{M}$ such that $\psi_\mathcal{M} = \psi \otimes \mathrm{id}_\mathcal{M}$. Now we consider the exact sequence

$$0 \to \ker(\psi) \xrightarrow{\iota} \mathcal{R}^\ell \xrightarrow{\psi} \mathcal{R}$$

and apply the functor $\bullet \otimes_\mathcal{R} \mathcal{M}$ which yields an exact sequence

$$0 \to \ker(\psi) \otimes_\mathcal{R} \mathcal{M} \xrightarrow{\iota\otimes\mathrm{id}_\mathcal{M}} \mathcal{M}^\ell \xrightarrow{\psi_\mathcal{M}} \mathcal{M},$$

since $\mathcal{M}$ is flat. As $\psi_\mathcal{M}(m_1, \ldots, m_\ell) = R[m_1, \ldots, m_\ell]^{\mathrm{tr}} = 0$ we have $(m_1, \ldots, m_l) \in \ker(\psi_\mathcal{M}) = \mathrm{im}(\iota \otimes \mathrm{id}_\mathcal{M})$ and thus there exist $\gamma_j = (c_{1j}, \ldots, c_{\ell j}) \in \ker(\psi) \subseteq \mathcal{R}^\ell$ and $\tilde{m}_j \in \mathcal{M}$ with $(m_1, \ldots, m_\ell) = \iota \otimes \mathrm{id}_\mathcal{M}(\sum_j \gamma_j \otimes \tilde{m}_j)$. Replacing $m_i \in \mathcal{M}$ with $b_i \in \mathcal{S}$, respectively $\tilde{m}_j \in \mathcal{M}$ with $d_j \in \mathcal{S}$, and $a_i m_i$ with $b_i\phi(a_i)$, respectively $c_{ij}\tilde{m}_j$ with $d_j\phi(c_{ij})$, yields the conclusion.
For the converse we will use a variation of Baer's criterion (cf. [21], Theorem 5.26). This is usually applied to check for injective modules, but can be modified in order to be a criterion for flatness. We claim that $\mathcal{M}$ is a flat $\mathcal{R}$-module, if and only if for every finitely generated ideal $\mathcal{I} \subseteq \mathcal{R}$ the canonical map $\mathcal{I} \otimes_\mathcal{R} \mathcal{M} \to \mathcal{R} \otimes_\mathcal{R} \mathcal{M}$ is injective and especially $\mathcal{I} \otimes_\mathcal{R} \mathcal{M} \cong \mathcal{I}\mathcal{M}$. The proof is given in [10], Theorem 7.7.
Now let $\mathcal{I} = \langle a_1, \ldots, a_\ell\rangle$, which is a finitely generated ideal of $\mathcal{R}$. Then any element of $\mathcal{I} \otimes_\mathcal{R} \mathcal{M}$ can be written as $\sum_i a_i \otimes m_i$. Let $\sum_i a_i m_i = 0 \in \mathcal{M}$. By our assumption there exist $c_{ij} \in \mathcal{R}$ and $\tilde{m}_j \in \mathcal{M}$ with $\sum_i a_i c_{ij} = 0$ and $\sum_j c_{ij}\tilde{m}_j = m_i$. Therefore, we have $\sum_i a_i \otimes m_i = \sum_{ij} a_i \otimes c_{ij}\tilde{m}_j = \sum_j(\sum_i a_i c_{ij}) \otimes \tilde{m}_j = 0$, i.e. the canonical map $\mathcal{I} \otimes_\mathcal{R} \mathcal{M} \to= \mathcal{R} \otimes_\mathcal{R} \mathcal{M} \cong \mathcal{R}\mathcal{M} = \mathcal{M}$ is injective. By Baer's criterion, $\mathcal{M}$ is flat and this of course also holds, if we replace $\mathcal{M}$ with $\mathcal{S}$. □

This proposition leads to the following characterization.

Theorem 4.7.
Let $\mathcal{S}$ be a ring with a ring homomorphism $\phi : \mathcal{R} \to \mathcal{S}$. Let $\mathcal{I}$ be an ideal of $\mathcal{P}$. Then $\mathrm{L}_\mathcal{S}(\langle\phi(\mathcal{I})\rangle) = \langle\phi(\mathrm{L}_\mathcal{R}(I))\rangle$, if and only if $\mathcal{S}$ is a flat $\mathcal{R}$-algebra.

Proof.
Let $\mathcal{S}$ be a flat $\mathcal{R}$-algebra. The inclusion "$\supseteq$" follows from Proposition 4.6. To show that $\mathrm{L}_\mathcal{S}(\langle\phi(\mathcal{I})\rangle) \subseteq \langle\phi(\mathrm{L}_\mathcal{R}(I))\rangle$ let $rx^\nu \in \mathrm{L}_\mathcal{S}(\langle\phi(\mathcal{I})\rangle)$. Then we can write $rx^\nu = \mathrm{LT}(\sum_i b_i\phi(f_i))$ for some $b_i \in \mathcal{S}[x]^e$ and $f_i \in \mathcal{I}$. Since the f_i are not fixed, but elements of an ideal, we can assume without loss of generality that $b_i \in \mathcal{S}$. Let $x^\mu = \max\{\mathrm{LM}(f_i)\}_i$. We choose an expression of rx^ν where x^μ is minimal. Suppose that $x^\mu \succ x^\nu$ and let a_i be the coefficient of x^μ in f_i. Then $\sum_i b_i\phi(a_i) = 0$ and by Proposition 4.6 there exist $c_{ij} \in \mathcal{R}$ and $d_j \in \mathcal{S}$ with $\sum_i c_{ij}a_i = 0$ and $\sum_j d_j\phi(c_{ij}) = b_i$. Then $\tilde{f}_j = \sum_i c_{ij}f_i \in \mathcal{I}$. These satisfy

$$\sum_j d_j\phi(\tilde{f}_j) = \sum_{ij} d_j\phi(c_{ij})\phi(f_i) = \sum_i b_i\phi(f_i)$$

and, therefore, $\mathrm{LT}(\sum_j d_j\phi(\tilde{f}_j)) = rx^\nu$, but in this expression we have $\mathrm{LM}(\tilde{f}_j) \prec x^\mu$, because $\sum_i c_{ij}a_i = 0$ which contradicts the minimality of x^μ. We supposed that $x^m u \succ x^\nu$

and lead this to a contradiction. Therefore, $\mu = \nu$ and for the coefficients a_i of $x^\mu = x^\nu$ in the f_i we have $\sum_i b_i\phi(a_i) = r$. Especially $rx^\nu \in \langle\phi(\mathrm{L}_\mathcal{R}(I))\rangle$.
Now suppose that $\mathcal{S}$ is not flat. Then by Proposition 4.6 there exist $a_i \in \mathcal{R}$ and $b_i \in \mathcal{S}$ with $\sum_i b_i\phi(a_i) = 0$ and no expression $\sum_j d_j\phi(c_{ij}) = b_i$ when simultaneously $\sum_i c_{ij}a_i = 0$ should hold, i.e. $b_i \notin \langle\mathrm{im}(\phi)\rangle$. We choose the length l of the sequences (i.e. $1 \leq i \leq l$) to be minimal. Let $f_i = a_i x^l y + x^{l-i}y^i \in \mathcal{R}[x, y]$ with $x \succ y$ and $\mathcal{I} = \langle f_1, \ldots, f_l\rangle$. Then $\sum_i b_i\phi(f_i) = \sum_i b_i\phi(a_i) + b_i x^{l-i}y^i = \sum_i b_i x^{l-i}y^i$. Note that $\sum_i c_{ij}a_i = 0$ is equivalent to $\sum_i c_{ij}f_i = \sum_i c_{ij}a_i + c_{ij}x^{l-i}y^i = \sum_i c_{ij}x^{l-i}y^i$. The leading coefficient of this expression is given by c_{1j} and by our assumption b_1 is not contained in the ideal $\langle\{c_{1j}\}_j\rangle$ which is generated by the coefficients of $\phi(\mathrm{L}_\mathcal{R}(\mathcal{I}))$. Especially $\mathrm{LT}(b_1\phi(f_1)) \notin \langle\phi(\mathrm{L}_\mathcal{R}(\mathcal{I}))\rangle$ which completes the proof. □

Corollary 4.8.
Let $\mathcal{I}$ be an ideal of $\mathcal{P}$, $S \subseteq \mathcal{R}$ a multiplicatively closed subset and $\mathcal{S} = S^{-1}\mathcal{R}$, the localization of $\mathcal{R}$ on S with canonical ring homomorphism $\iota : \mathcal{R} \to \mathcal{S}$. Then $\mathrm{L}_\mathcal{S}(\iota(\mathcal{I})) = \iota(\mathrm{L}_\mathcal{R}(\mathcal{I}))$.

Proof.
We will show that the functor $S^{-1}\bullet$ is exact. Let

$$A_1 \xrightarrow{\phi} A_2 \xrightarrow{\psi} A_3$$

be an exact sequence of left $\mathcal{R}$-modules. Then $S^{-1}\phi \circ S^{-1}\psi = S^{-1}(\phi \circ \psi) = 0$. Let on the other hand $S^{-1}\psi(\frac{a}{s}) = 0$ for $a \in A_2$ and $s \in S$. Then we can find $\tilde{s} \in S$ with $\tilde{s}\psi(a) = 0$, i.e. $\tilde{s}a \in \ker(\psi) = \mathrm{im}(\phi)$. Let $\phi(\tilde{a}) = \tilde{s}a$. Then we have $\frac{a}{s} = \frac{\tilde{s}a}{\tilde{s}s} = \frac{\phi(\tilde{m})}{\tilde{s}s} = S^{-1}\phi(\frac{\tilde{a}}{\tilde{s}s})$ thus $\ker(S^{-1}\psi) = \mathrm{im}(S^{-1}\phi)$ and

$$S^{-1}A_1 \xrightarrow{S^{-1}\phi} S^{-1}A_2 \xrightarrow{S^{-1}\psi} S^{-1}A_3$$

is an exact sequence.
We showed that $S^{-1}\bullet$ is exact. On the other hand $S^{-1}\bullet$ is functorially isomorphic to $S^{-1}\mathcal{R} \otimes_\mathcal{R} \bullet = \mathcal{S} \otimes_\mathcal{R} \bullet$. Using Theorem 4.7 completes the proof. □

Let $Y \supseteq X$ be a monoid extension of F and let $\prec_X$, $\prec_Y$ be global monomial orders on X, Y respectively, such that $x \prec_X \tilde{x}$ implies $x \prec_Y \tilde{x}$ for all $x, \tilde{x} \in X$. We call Y an **order preserving extension** of X.

Proposition 4.9.
Let $Y \supseteq X$ be an order preserving extension of commutative monoids on finite alphabets, i.e. $\mathcal{P} = \mathcal{R}[x_1, \ldots, x_n]$ and $\mathcal{R}[Y] = \mathcal{R}[x_1, \ldots, x_n, y_1, \ldots, y_{n'}]$. Let $\mathcal{G} \subseteq \mathcal{P}$ and $\mathcal{I} = \langle\mathcal{G}\rangle \subseteq \mathcal{P}$, such that $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$. Then $\mathcal{G}$ is also a Gröbner basis for $\mathcal{J} = \langle\mathcal{G}\rangle \subseteq \mathcal{R}[Y]$.

Proof. Let $f \in \mathcal{J}$. Then there exist monomials $t_i \in Y$ and polynomials $f_i \in \mathcal{I}$ such that $g = \sum_i t_i f_i$. Furthermore, let $\mathrm{LT}(g) = rtx$ with $r \in \mathcal{R}$, $t \in Y$ and $x \in X$. Since the f_i are in $\mathcal{I}$, we can choose the represenation of f such that there is an index i with $t_i = t$ and thus $rtx = \mathrm{LT}(\sum_i t_i f_i) = \mathrm{LT}(\sum_{t_i=t} t_i f_i) = t\mathrm{LT}(\sum_{t_i=t} f_i)$. Hence $\tilde{f} := \sum_{t_i=t} h_i \in \mathcal{I}$ satisfies $\mathrm{LT}(f) = t\mathrm{LT}(\tilde{f}) \in \mathrm{L}_Y(\mathcal{G})$. Therefore, $\mathcal{G}$ is a Gröbner basis for $\mathcal{J}$. □

A similar statement exists for non-commutative monoids over fields and is proven in [15]. Let $\mathcal{R} = \mathbb{K}$ be a field and $Y \supseteq X$ be an order preserving extension. Let $\mathcal{G} \subseteq \mathbb{K}\langle X\rangle$ and $\mathcal{I} = \langle \mathcal{G}\rangle \subseteq \mathbb{K}\langle X\rangle$ such that $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$. Then $\mathcal{G}$ is also a Gröbner basis for $\mathcal{J} = \langle \mathcal{G}\rangle \subseteq \mathbb{K}\langle Y\rangle$.

Theorem 4.10.
Let $Y \supseteq X$ be an order preserving extension. Let $\mathcal{G} \subseteq \mathcal{P}$ such that $\mathcal{G}$ is a Gröbner basis for both $\mathcal{I} = \langle \mathcal{G}\rangle \subseteq \mathcal{P}$ and $\mathcal{J} = \langle \mathcal{G}\rangle \subseteq \mathcal{R}\langle Y\rangle$. Then every Gröbner basis for $\mathcal{I}$ is also a Gröbner basis for $\mathcal{J}$.

Proof.
Let $\tilde{\mathcal{G}}$ be another Gröbner basis for $\mathcal{I}$ and $f \in \mathcal{J}$. Then $\mathrm{LT}(f) \in \mathrm{L}(\mathcal{G})$ and, therefore, there exist $p_i \in \mathcal{R}\langle Y\rangle^e$ and $g_i \in \mathcal{G}$ such that $\mathrm{LT}(f) = \sum_i p_i \mathrm{LT}(g_i)$. Moreover, since $g_i \in \mathcal{G} \subseteq \mathcal{I}$, we have $\mathrm{LT}(g_i) \in \mathrm{L}(\tilde{\mathcal{G}})$ and hence there exist $h_j^i \in \mathcal{P}^e$ and $\tilde{g}_j \in \tilde{\mathcal{G}}$ with $\mathrm{LT}(g_i) = \sum_j h_j^i \mathrm{LT}(\tilde{g}_j)$. Then

$$\mathrm{LT}(f) = \sum_i p_i \mathrm{LT}(g_i) = \sum_{i,\,j} p_i h_j^i \mathrm{LT}(\tilde{g}_j) \in \mathrm{L}(\tilde{\mathcal{G}})$$

and thus $\tilde{\mathcal{G}}$ is a Gröbner basis for $\mathcal{J}$. □

Definition 4.11.
Let $\mathcal{G} = \{g_1, g_2, \ldots\} \subseteq \mathcal{P}$ be a countable subset and let $t_1 \prec t_2 \prec \ldots$ be an ascending sequence in X such that every $t \in X$ is bounded by some t_i. We call this a **partition** of X. An ascending sequence $B_1 \subseteq B_2 \subseteq \ldots \subseteq \mathcal{P}$ of finite sets $B_i = \{b_k^i\}_k$ is called **critical sequence for** $\mathcal{I} = \langle \mathcal{G}\rangle$, if

1. $g_i \in B_i$ for all $i \in \mathbb{N}$ and
2. there is a homogeneous basis H of $\mathrm{Syz}(\{\mathrm{LT}(b_k^i)\}_{k,i})$, such that for each homogeneous $H_j = \sum_k \gamma_k^j e_k \in H$ of degree at most t_i for some i, we have that $\sum_k \gamma_k^j b_k^j$ either reduces to some element of B_{i+1} or to zero.

Lemma 4.12.
Let $t \in X \setminus \{1\}$. Then $t \prec t^2 \prec t^3 \prec \ldots$ is an ascending sequence and every $\tilde{t} \in X$ is bounded by some t^i, thus we have a partition of X.

Proof.
Since $\preceq$ is a global monomial order, we have $e \prec t$ and thus $t^i \prec t^{i+1}$ for all $i \in \mathbb{N}$. Fix some $\tilde{t} \in X$ and let $T := \{x \in X \mid x \prec \tilde{t}\}$ and $T_i := \{x \in X \mid x \prec t^i\}$. These are finite sets. Since $\preceq$ is total, we have for every $i \in \mathbb{N}$ either $T \subseteq T_i$ or $T_i \subseteq T$. Suppose that $t^i \prec \tilde{t}$ for every $i \in \mathbb{N}$. Then $|T_i| < |T|$. But by construction, $|T_1| < |T_2| < \ldots$ is a strictly increasing sequence in $\mathbb{N}$. Hence we have a contradiction and $\tilde{t}$ is contained in some T_i, i.e. is bounded by t^i. □

Theorem 4.13.
Let $B_1 \subseteq B_2 \subseteq \ldots \subseteq \mathcal{P}$ be a critical sequence for $\mathcal{I}$ as in Definition 4.11. Then there exists $N \in \mathbb{N}$ such that every $f \in \mathcal{I}$ has a Gröbner representation w.r.t. B_N.

Proof.
Let $f \in \mathcal{I}$ with $\mathrm{LM}(f) = t$. Then there exists $n \in \mathbb{N}$ such that $f \in \langle f_1, \ldots, f_n \rangle$. For $m \geq n$ we consider the, therefore, non-empty sets

$$T_m := \{\max\{\mathrm{LM}(h_k^m b_k^m)\}_k \mid h_k^m \in \mathcal{P}^e,\, b_k^m \in B_m :\, f = \sum_k h_k^m b_k^m\}.$$

Since $\preceq$ is a global monomial ordering, we know that T_m contains a unique minimal element, say t_m. We claim that $t_m \succ t_{m+1}$ if $t_m \neq t$. To see this, let $p_i \in \mathcal{P}^e$ with $f = \sum_i p_i b_i^m$ and $\max\{\mathrm{LM}(p_i b_i^m)\}_i = t_m$. Now we define α as in the proof of Theorem 4.5. Let $p_i = \sum_k r_k^i \tau_k^i$ be in simplified form with $r_k^i \in \mathcal{R}$ and $\tau_k^i \in X^e$. We set

$$\alpha_i := \sum_{\tau_k^i \mathrm{LM}(b_i^m) = t_m} r_k^i \tau_k^i.$$

and $\alpha := [\alpha_1, \alpha_2, \ldots]$. Then $\max\{\mathrm{LM}((p_i - \alpha_i) b_i^m)\}_i \prec t_m$. Let $H = \{H_j\}_j$ be a homogeneous basis for $\mathrm{Syz}(\mathrm{LT}(b_i^m))$ which exists by the assumption that we have a critical sequence. Note that $\alpha \in \mathrm{Syz}(\mathrm{LT}(b_i^m))$ is homogeneous of degree t_m. Therefore, we may write $\alpha = \sum_j s_j H_j$ with $s_j \in \mathcal{P}^e$. For the rest of the proof we have to set simplicity aside and fix $\mathrm{card}(B_i) = N_i \in \mathbb{N}$. Then $\alpha = [\alpha_1, \ldots, \alpha_{N_m}]$ and with the basis H we have

$$\sum_{i=1}^{N_m} \alpha_i b_i^m = \sum_j s_j \underbrace{\left(\sum_{k=1}^{N_m} \gamma_k^j b_k^m \right)}_{\star}.$$

We have to consider two cases. If the expression $\star$ in brackets reduces to zero w.r.t. B_m then there exist $\tilde{\lambda}_i^j \in \mathcal{P}^e$ such that $\max\{\mathrm{LM}(\tilde{\lambda}_i^j b_i^m)\}_{i=1}^{N_m}$ is equal to the leading monomial of $\star$ and $\star$ equals $\sum_{i=1}^{N_m} \tilde{\lambda}_i^j b_i^m$. If on the other hand $\star$ reduces to some $b_l^{m+1} \in B_{m+1}$ w.r.t. B_m then there exist $\tilde{\lambda}_i^j \in \mathcal{P}^e$ such that $\max\{\mathrm{LM}(\tilde{\lambda}_i^j b_i^m)\}_{i=1}^{N_m}$ is smaller than or equal to the leading monomial of $\star$ and $\star$ equals $b_l^{m+1} + \sum_{i=1}^{N_m} \tilde{\lambda}_i^j b_i^m$. Since $B_m \subseteq B_{m+1}$, we obtain in both cases a representation $\sum_{i=1}^{N_{m+1}} \lambda_i^j b_i^{m+1}$ for $\star$ with $\lambda_i^j \in \mathcal{P}^e$. Then

$$\sum_{i=1}^{N_m} \alpha_i b_i^m = \sum_j s_j \left(\sum_{k=1}^{N_m} \gamma_k^j b_k^m \right) = \sum_j \underbrace{s_j \left(\sum_{i=1}^{N_{m+1}} \lambda_i^j b_i^{m+1} \right)}_{\star\star}$$

where each summand $\star\star$ has leading monomial strictly smaller than t_m. Note that above we already had $\max\{\mathrm{LM}((p_i - \alpha_i)b_i^m)\}_i \prec t_m$ and altogether

$$\begin{aligned} f &= \sum_{i=1}^{N_m}(p_i - \alpha_i)b_i^m + \sum_{i=1}^{N_m}\alpha_i b_i^m \\ &= \sum_{i=1}^{N_m}(p_i - \alpha_i)b_i^m + \sum_j s_j \left(\sum_{i=1}^{N_{m+1}} \lambda_i^j b_i^{m+1}\right) \\ &= \sum_{i=1}^{N_m}(p_i - \alpha_i)b_i^m + \sum_{i=1}^{N_{m+1}} \left(\sum_j s_j \lambda_i^j\right) b_i^{m+1}. \end{aligned}$$

Again we use $B_m \subseteq B_{m+1}$ to write this as one sum $f = \sum_{i=1}^{N_{m+1}} \tilde{p}_i b_i^{m+1}$ with $t_{m+1} \preceq \max\{\mathrm{LM}(\tilde{p}_i b_i^{m+1})\}_{i=1}^{N_{m+1}} \prec t_m$. Therefore, f has a Gröbner representation w.r.t $B_N := B_{m+1}$. □

An obvious consequence is, that we can obtain a Gröbner basis using critical sequences.

Remark 4.14.
Let M be a finite set of terms, for example leading terms of a generating set that we are interested in. Then for $t \in X$ we can construct a basis H^t for $\mathrm{Syz}_t(M)$ as follows. Let $M = \{r_1 t_1, \ldots, r_m t_m\}$ with $r_i \in \mathcal{R}$ and $t_i \in X$. Furthermore, for $1 \leq i \leq m$ let

$$\{p \in \mathcal{P}^e \text{ monomial} \mid pt_i = t\} = \{p_j^i\}_j$$

which is finite and non-empty if and only if t_i divides t. We set $n_i := \mathrm{card}(\{p_j^i\}_j) \in \mathbb{N}$ and $n^s := \sum_{i=1}^s n_i$ for $1 \leq s \leq m$. For every $1 \leq k \leq n^m$ we choose a $1 \leq s \leq m$ such that $n^{s-1} \leq k \leq n^s$. We set $c_k := r_s$. Then we can find a generating set $\tilde{H}$ for

$$\{c_1, \ldots, c_{n^m}\}^\perp = \{v \in \mathcal{R}^{(n^m)} \mid \sum_k c_k v_k = 0\}.$$

Let $(h_1^l, \ldots, h_{n^m}^l) \in \tilde{H}$. For $1 \leq k \leq n^m$ we choose $1 \leq s_k \leq m$ such that $n^{s_k - 1} \leq k \leq n^{s_k}$ and set $\lambda_k := k - n^{s_k - 1}$. We define $H_l := \sum_k h_k^l p_{\lambda_k}^{s_k}$ and $H^t = \bigcup_l \{H_l\}$. Then H^t is a homogeneous basis of $\mathrm{Syz}_t(M)$.
This can be used to compute a critical sequence of an ideal $\mathcal{I} \subseteq \mathcal{P}$, if we have a partition $\tilde{t}_1 \prec \tilde{t}_2 \prec \ldots$ of X (cf. [7], Lemma 12 for a proof).
Finally we can solve the ideal membership problem $f \in \mathcal{I}$ as follows. For $t \in X \setminus \{e\}$ we take the partition $t \prec t^2 \prec \ldots$ of X and compute the critical sequence $B_1 \subseteq B_2 \subseteq \ldots$ as above. Let $f_0 = f$ and for $n \in \mathbb{N}$ let f_n be a normal form of f_{n-1} w.r.t. B_n. Then $f \in \mathcal{I}$ if and only if we have $f_{n'} = 0$ for some $n' \in \mathbb{N}$.

From now on let $\mathcal{R}$ be a principal ideal domain.

Remark 4.15.
There is a procedure to compute a basis for $\mathrm{Syz}(M)$ with $M = \{\mathrm{LT}(g_i)\}_i$ over principal

ideal rings. For every $g_i \in \mathcal{G}$ let $\mathrm{LC}(g_i) = r_i$ and $\mathrm{LM}(g_i) = t_i$. Since $\mathcal{R}$ is a principal ideal ring, we can find a greatest common divisor and a least common multiple of two leading coefficients, based on the Euclidean algorithm. Therefore, let

$$c_{ij} := \frac{r_j}{\gcd(r_i,\, r_j)},$$

thus $\mathrm{lcm}(r_i,\, r_j) = c_{ij} r_i = c_{ji} r_j$. Moreover, let $x_1,\, x_2,\, y_1,\, y_2 \in X$ such that at least one of the following conditions holds

- $x_1 = y_1 = 1$
- $x_2 = y_2 = 1$
- $x_1 = y_2 = 1$
- $x_2 = y_1 = 1$

and there exists no $x \in X$ such that exactly one of the following holds for some fixed $1 \leq i < j \leq m$

- $x_1 = x_2 t_j x$ and $y_2 = x t_i y_1$
- $x_2 = x_1 t_i x$ and $y_1 = x t_j y_2$

We define

$$\mathcal{Z}_{ij} := \{\alpha \in \mathrm{Syz}(M) \mid \forall 1 \leq k \leq m :\ \alpha_k = \begin{cases} c_{ij}(x_1 \otimes y_1), & k = i \\ -c_{ji}(x_2 \otimes y_2), & k = j \\ 0, & \text{else} \end{cases}$$

and for an arbitrary, but fixed $x \in X$, we define

$$\mathcal{Y}_{ij} := \{\alpha \in \mathrm{Syz}(M) \mid \forall 1 \leq k \leq m : \begin{cases} c_{ij}(e \otimes x t_j), & k = i \\ -c_{ji}(t_i x \otimes e), & k = j \\ 0, & \text{else} \end{cases}.$$

Then

$$H := \bigcup_{i,\,j} (\mathcal{Z}_{ij} \cup \mathcal{Y}_{ij})$$

is a $\mathcal{P}^e$-basis for $\mathrm{Syz}(M)$. This is an important fact and we will use it in chapter 7. It tells us that we only need to focus on elements of the syzygy module, that have exactly two non-zero components. Thus it suffices for computations to restrict to syzygies for two elements which we call a pair.

Theorem 4.16.
Let $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq \mathcal{P} \setminus \{0\}$, $\mathcal{I} = \langle \mathcal{G} \rangle$ and H a homogeneous basis of $\mathrm{Syz}(\{\mathrm{LM}(g_i)\}_i)$ such that for all $H_j = (h_1^j, \ldots, h_m^j) \in H$ we have that $\sum_{i=1}^m h_i^j g_i$ has a Gröbner representation w.r.t. $\mathcal{G}$. Then $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$.

Proof.
Let $f \in \mathcal{I}$ and assume that there exists no Gröbner representation of f w.r.t. $\mathcal{G}$. We write $f = \sum_i p_i g_i$ for some $p_i \in \mathcal{P}^e$ such that $t := \max\{\mathrm{LM}(p_i g_i)\}_i$ is minimal amongst all such representations of f. Since there is no Gröbner representation w.r.t. $\mathcal{G}$, we have $t \succ \mathrm{LM}(f)$. The next step is already well known from the proofs of the previous Theorems 4.5 and 4.13. Let $p_i = \sum_k r_k^i \tau_k^i$ be in simplified form with $r_k^i \in \mathcal{R}$ and $\tau_k^i \in X^e$. We set

$$\alpha_i := \sum_{k:\, \tau_k^i \mathrm{LM}(g_i) = t} r_k^i \tau_k^i$$

and obtain $\alpha := [\alpha_1, \ldots, \alpha_m] \in \mathrm{Syz}(\{\mathrm{LM}(g_i)\}_i)$. Using the basis H we can express α as $\alpha = \sum_j s_j H_j$ with $s_j \in \mathcal{P}^e$ and $\sum_i h_i^j g_i = \sum_i \lambda_i^j g_i$ a Gröbner representation such that $\max\{\mathrm{LM}(\lambda_i^j g_i)\}_i \prec \mathrm{LM}(h_i^j)$ (here we use that H_j is homogeneous, thus $\mathrm{LM}(h_i^j)$ does not depend on i). Now

$$\sum_i \alpha_i g_i = \sum_i \left(\sum_j s_j h_i^j \right) g_i = \sum_j s_j \left(\sum_i h_i^j g_i \right) = \sum_j s_j \left(\sum_i \lambda_i^j g_i \right) = \sum_i \left(\sum_j s_j h_i^j \right) g_i$$

and thus

$$f = \sum_i p_i g_i = \sum_i (p_i + \alpha_i - \alpha_i) g_i = \sum_i \underbrace{\left(p_i - \alpha_i + \sum_j s_j h_i^j \right)}_{=: p_i'} g_i$$

with $\max\{\mathrm{LM}(p_i' g_i)\}_i \prec t$, a contradiction to our assumption that t is minimal. Hence f has a Gröbner representation w.r.t. $\mathcal{G}$ and $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$. □

To give another criteria for Gröbner basis we extend the concept of reduction: We say that f has a **monomial Gröbner representation** w.r.t. $\mathcal{G} = \{g_1, \ldots, g_m\}$ if $f = \sum_i h_i g_i$ is a Gröbner representation w.r.t. $\mathcal{G}$ with $h_i \in \mathcal{P}^e$ such that the h_i are either zero or monomials with $\mathrm{LM}(h_i g_i) = \mathrm{LM}(f)$. We say that f **monomially reduces** to h w.r.t. $\mathcal{G}$ if $\mathrm{LM}(h) \prec \mathrm{LM}(f)$ and $f - h$ has a monomial Gröbner representation w.r.t. $\mathcal{G}$. This allows us to give a criteria for monomial extensions.

Theorem 4.17.
Let $Y \supseteq X$ be an order preserving extension of free monoids on finite alphabets, i.e. $\mathcal{P} = \mathcal{R}\langle x_1, \ldots, x_n \rangle$ and $\mathcal{R}\langle Y \rangle = \mathcal{R}\langle x_1, \ldots, x_n, y_0, y_1, \ldots, y_{n'} \rangle$. For $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq \mathcal{P}$ let $\mathcal{J} = \langle \mathcal{G} \rangle \subseteq \mathcal{R}\langle Y \rangle$. Then $\mathcal{G}$ is a Gröbner basis for $\mathcal{J}$, if and only if every polynomial $\sum_i \alpha_i g_i$ monomially reduces to zero w.r.t. $\mathcal{G}$ where $\alpha = [\alpha_1, \ldots, \alpha_m]$ is an element of

$$\mathcal{Z} := \bigcup_{ij} \left(\mathcal{Z}_{ij} \cup \{ \alpha \in \mathrm{Syz}(M) \mid \forall 1 \leq k \leq m : \alpha_k = \begin{cases} c_{ij}(1 \otimes y_0 t_j), & k = i \\ -c_{ji}(t_i y_0 \otimes 1), & k = j \\ 0, & \text{else} \end{cases} \} \right)$$

for M, c_{ij}, t_i, $\mathcal{Z}_{ij}$ as in Remark 4.15 and 1 the unitary element of Y.

Proof.
Let $\mathcal{G}$ be a Gröbner basis for $\mathcal{J}$. We will show that for any homogeneous syzygy α with

$$\alpha_k = \begin{cases} c_{ij}(e \otimes y_0 t_j), & k = i \\ -c_{ji}(t_i y_0 \otimes e), & k = j \\ 0, & \text{else} \end{cases}$$

for $1 \leq k \leq m$ we can find $p_i \in \mathcal{P}^e$ such that $\sum_i \alpha_i g_i = \sum_i p_i g_i$ and $\max\{\mathrm{LM}(p_i g_i)\} \prec t_i y_0 t_j$. Since $\mathcal{G}$ is a Gröbner basis, we know that every polynomial $h_0 := c_{ij} g_i y_0 t_j - c_{ji} t_i y_0 g_j$ monomially reduces to zero w.r.t. $\mathcal{G}$ thus the is a sequence of polynomials $h_0, h_1, \ldots, h_N = 0$ obtained from each other by reduction and with Gröbner representations $h_{i-1} - h_i = \sum_j \lambda_j^i g_j$ such that λ_j^i is a term in $\mathcal{R}\langle Y \rangle^e$. Observe that h_0 consists of terms $r\tau_1 y_0 \tau_2$ with $r \in \mathcal{R}$ and $[\tau_1, \tau_2] \in X^{1\times 2} \setminus \{[t_i, t_j]\}$ such that $\tau_1 \preceq t_i$, $\tau_2 \preceq t_j$. We claim that this is the case for every term occurring in the h_i and in the Gröbner representation of $h_{i-1} - h_i$. Let the claim hold for $i-1$ and let $\mathrm{LM}(h_{i-1}) = \tilde{\tau}_1 y_0 \tilde{\tau}_2$. Since the g_i are polynomials in X, there are x, $x' \in X$ with $\lambda_j^i = c(x \otimes x' y_0 \tilde{\tau}_2)$ or $\lambda_j^i = c(\tilde{\tau}_1 y_0 x \otimes x')$ for some coefficient $c \in \mathcal{R}$. We assume that the first case holds and write $g_j = \sum_l r_l^j x_l^j$ with $r_l^j \in \mathcal{R}$ and $x_l^j \in X$. Then

$$\lambda_j^i g_j = \sum_l c(x \otimes x' y_0 \tilde{\tau}_2) r_l^j x_l^j = \sum_l c r_l^j x x_l^j x' y_0 \tilde{\tau}_2$$

and

$$x x_l^j \begin{cases} = \tilde{\tau}_1, & l = 1 \\ \prec \tilde{\tau}_1, & l \geq 2 \end{cases}$$

which proves the claim for i. Set $\lambda_j := \sum_j \lambda_j^i g_j$. Then $\sum_j \lambda g_j = c_{ij} g_i y_0 t_j - c_{ji} t_i y_0 g_j = \sum_j \alpha_j g_j$ with $\max\{\mathrm{LM}(p_j g_j)\} \prec t_i y_0 t_j$ which was to show. Hence we find another syzygy of degree smaller than α and iteratively α must monomially reduce to zero w.r.t. $\mathcal{G}$.
On the other hand the set $\mathcal{Z}$ contains a basis for $\mathrm{Syz}(M)$ and thus if every element reduces to zero then $\mathcal{G}$ is a Gröbner basis for $\mathcal{J}$. □

Remark 4.18. (**fundamental theorem for finitely generated modules**)
Let $\mathcal{M}$ be a finitely generated $\mathcal{R}$-module. Then there exist a unique $n \in \mathbb{N}$ and up to units unique $r_1, \ldots, r_n \in \mathcal{R}$ with $r_1 \mid \ldots \mid r_n$ and

$$\mathcal{M} = \mathcal{R}/r_1\mathcal{R} \oplus \ldots \oplus \mathcal{R}/r_n\mathcal{R}.$$

For $r_i \neq 0$ we get parts of the torsion submodule, while $r_i = 0$ corresponds to free submodules. Now let $\mathcal{M} = \mathcal{L}$ be a Lie algebra over $\mathcal{R}$ with Lie bracket $[\bullet, \bullet]$ and freely generated by $e_1, \ldots, e_N$, $N \geq n$, such that $\mathcal{L} = \mathcal{R}e_1 \oplus \ldots \oplus \mathcal{R}e_N$ and $\mathrm{ann}(e_i) = \langle r_i \rangle$ for $1 \leq i \leq n$ (especially there are free resolutions of $\mathcal{L}$ of length $N - n$). Then there exist coefficients $c_{ijk} \in \mathcal{R}$ with $[e_i, e_j] = \sum_k c_{ijk} e_k$ and if we have $\tilde{c}_{ijk} \in \mathcal{R}$ with the same

property then $c_{ijk} - \tilde{c}_{ijk} \in \langle r_k \rangle$ for $1 \leq k \leq n$ and $c_{ijk} = \tilde{c}_{ijk}$ for $n+1 \leq k \leq N$.
Let X be a free monoid on a finite alphabet with N letters, i.e. $\mathcal{P} = \mathcal{R}\langle x_1, \ldots, x_N \rangle$. We define

$$\mathcal{G} := \{g_{ij} = x_i x_j - x_j x_i - \sum_k c_{ijk} x_k\}_{i,j} \quad \text{and} \quad \mathcal{H} := \{h_i = r_i x_i\}_i.$$

Then the universal enveloping algebra

$$\mathcal{U} := \frac{\mathcal{L} \oplus (\mathcal{L} \otimes \mathcal{L}) \oplus (\mathcal{L} \otimes \mathcal{L} \otimes \mathcal{L}) \oplus \ldots}{\langle \{v \otimes w - w \otimes v - [v, w] \mid v, w \in \mathcal{L}\} \rangle}$$

is isomorphic to $\mathcal{P}/\langle \mathcal{G} \cup \mathcal{H} \rangle$.

Lemma 4.19.
Let X be a free monoid on a finite alphabet and $\mathcal{L}$ a finitely generated Lie algebra over $\mathcal{R}$ with Lie bracket $[\bullet, \bullet]$. Our global monomial ordering shall be the graded left lexicographical one with $x_N \succ \ldots \succ x_1$. Let $\mathcal{U}$ be the universal enveloping algebra over $\mathcal{L}$. Then $\mathcal{G} \cup \mathcal{H}$, with $\mathcal{G}$, $\mathcal{H}$ as in Remark 4.18, is a Gröbner basis for $\langle \mathcal{G} \cup \mathcal{H} \rangle$ and for every free order preserving extension $Y \supseteq X$ we have that $\mathcal{G} \cup \mathcal{H}$ is a Gröbner basis for $\langle \mathcal{G} \cup \mathcal{H} \rangle \subseteq \mathcal{R}\langle Y \rangle$.

Proof.
We will show that every S-polynomial h resulting from syzygies of elements of $\mathcal{P} \cup \mathcal{H}$ monomially reduces to zero w.r.t. $\mathcal{G} \cup \mathcal{H}$. First of all let h result trivially from elements of $\mathcal{G}$, thus for $i > j$, $k > l$ and $x \in X$ we have

$$\begin{aligned}
h =& x_i x_j x g_{kl} - g_{ij} x x_k x_l \\
=& x_i x_j x \left(x_k x_l - x_l x_k - \sum_s c_{kls} x_s \right) \\
& - \left(x_i x_j - x_j x_i - \sum_s c_{ijs} x_s \right) x x_k x_l \\
=& - x_i x_j x x_l x_k - \sum_s c_{kls} x_i x_j x x_s \\
& + x_j x_i x x_k x_l + \sum_s c_{ijs} x_s x x_k x_l \\
& + (g_{ij} x x_l x_k - x_j x_i g_{kl}) - (g_{ij} x x_l x_k - x_j x_i g_{kl}) \\
=& - x_i x_j x x_l x_k - \sum_s c_{kls} x_i x_j x x_s \\
& + x_j x_i x x_k x_l + \sum_s c_{ijs} x_s x x_k x_l \\
& + x_i x_j x x_l x_k - x_j x_i x x_l x_k - \sum_s c_{ijs} x_s x x_l x_k \\
& - x_j x_i t x_k x_l + x_j x_i x x_l x_k + \sum_s c_{kls} x_j x_i x x_s \\
& - (g_{ij} x x_l x_k - x_j x_i g_{kl}).
\end{aligned}$$

We define

$$h' := -\sum_s c_{kls} x_i x_j x x_s + \sum_s c_{ijs} x_s x x_k x_l - \sum_s c_{ijs} x_s x x_l x_k + \sum_s c_{kls} x_j x_i x x_s.$$

to obtain $h = h' - (g_{ij} x x_l x_k - x_j x_i g_{kl})$. Hence h reduces to h' and the leading terms of h' do not cancel each other out. Then h' monomially reduces to

$$h'' := -\sum_{s,\,s'} c_{kls} c_{ijs'} x_s x x_{s'} + \sum_{s,\,s'} c_{kls'} c_{ijs} x_{s'} x x_s = 0.$$

w.r.t. $\mathcal{H}$ where we use the fact that monomials of type $c_{kls} x_i x_j$ with $i > j$ reduce to $c_{kls} g_{ij}$.
Now let h result non-trivially from an element of $\mathcal{G}$. For $i > j > k$ that is

$$\begin{aligned}
h &= x_i g_{jk} - g_{ij} x_k \\
&= x_i \left(x_j x_k - x_k x_j - \sum_l c_{jkl} x_l \right) - \left(x_i x_j - x_j x_i - \sum_l c_{ijl} x_l \right) x_k \\
&= -x_i x_k x_j - \sum_l c_{jkl} x_i x_l + x_j x_i x_k + \sum_l c_{ijl} x_l x_k
\end{aligned}$$

and h reduces to

$$\begin{aligned}
h' :=& h + g_{ik} x_j - x_j g_{ik} - g_{jk} x_i + x_k g_{ij} \\
=& - x_i x_k x_j - \sum_l c_{jkl} x_i x_l + x_j x_i x_k + \sum_l c_{ijl} x_l x_k \\
&+ \left(x_i x_k - x_k x_i - \sum_l c_{ikl} x_l \right) x_j - x_j \left(x_i x_k - x_k x_i - \sum_l c_{ikl} x_l \right) \\
&- \left(x_j x_k - x_k x_j - \sum_l c_{jkl} x_l \right) x_i + x_k \left(x_i x_j - x_j x_i - \sum_l c_{ijl} x_l \right) \\
=& - \sum_l c_{jkl} x_i x_l + \sum_l c_{ijl} x_l x_k \\
&- \sum_l c_{ikl} x_l x_j + \sum_l c_{ikl} x_j x_l \\
&+ \sum_l c_{jkl} x_l x_i - \sum_l c_{ijl} x_k x_l.
\end{aligned}$$

The leading terms of h' (except those which include squares) do not cancel each other out so

$$h' = -\sum_{l \neq i} c_{jkl} x_i x_l + \sum_{l \neq k} c_{ijl} x_l x_k - \sum_{l \neq j} c_{ikl} x_l x_j + \sum_{l \neq j} c_{ikl} x_j x_l + \sum_{l \neq i} c_{jkl} x_l x_i - \sum_{l \neq k} c_{ijl} x_k x_l.$$

reduces further to

$$\begin{aligned}
h'' :=& \sum_s \left(-\sum_{l<i} c_{jkl} c_{ils} + \sum_{l>i} c_{jkl} c_{lis} + \sum_{l<j} c_{ikl} c_{jlv} - \sum_{l>j} c_{ikl} c_{ljs} + \sum_{l<k} c_{ijl} c_{kls} + \sum_{l>k} c_{ijl} c_{lks} \right) x_s \\
=& \sum_s - \left(\sum_l c_{jkl} c_{ils} + \sum_l c_{kil} c_{jls} + \sum_l c_{ijl} c_{kls} \right) x_s,
\end{aligned}$$

because $c_{ijk} = -c_{jik}$ and $c_{iik} = 0$ for all i, j, k. Moreover, the Jacobi identity yields

$$\begin{aligned}
0 &= [e_i, [e_j, e_k]] + [e_j, [e_k, e_i]] + [e_k, [e_i, e_j]] \\
&= \sum_l [e_i, c_{jkl} e_l] + \sum_l [e_j, c_{kil} e_l] + \sum_l [e_k, c_{ijl} e_l] \\
&= \sum_l c_{jkl} \sum_s c_{ils} e_s + \sum_l c_{kil} \sum_s c_{jls} e_s + \sum_l c_{ijl} \sum_s c_{kls} e_s \\
&= \sum_s \left(\sum_l c_{jkl} c_{ils} + \sum_l c_{kil} c_{jls} + \sum_l c_{ijl} c_{kls} \right) e_s .
\end{aligned}$$

It follows that

$$\sum_l c_{jkl} c_{ils} + \sum_l c_{kil} c_{jls} + \sum_l c_{ijl} c_{kls} = 0$$

for $s > n$ and

$$r_s \mid \sum_l c_{jkl} c_{ils} + \sum_l c_{kil} c_{jls} + \sum_l c_{ijl} c_{kls}$$

for $s \leq n$ if the right hand side is non-zero. Thus h'' monomially reduces to zero w.r.t. $\mathcal{H}$.

Next let h result from a trivial syzygy of an element of $\mathcal{G}$ and an element of $\mathcal{H}$. Then with $i > j$ and $x \in X$ we have

$$\begin{aligned}
h &= h_k x x_i x_j - r_k x_k x g_{ij} \\
&= r_k x_k x x_i x_j - r_k x_k x \left(x_i x_j - x_j x_i - \sum_l c_{ijl} x_l \right) \\
&= r_k x_k x x_j x_i + \sum_l r_k c_{ijl} x_k x x_l
\end{aligned}$$

which reduces to

$$h' = h - h_k x x_j x_i = \sum_l r_k c_{ijl} x_k x x_l$$

and thus monomially reduces to zero as well.

Finally let h result non-trivially from an element of $\mathcal{G}$ and an element of $\mathcal{H}$. Then

$$h = h_i x_j - r_i g_{ij} = r_i x_i x_j - r_i \left(x_i x_j - x_j x_i - \sum_k c_{ijk} x_k \right) = r_i x_j x_i + \sum_k r_i c_{ijk} x_k$$

reduces to

$$h' = h - x_j h_i = \sum_k r_i c_{ijk} x_k = \sum_{k=n+1}^{N} r_i c_{ijk} x_k,$$

because $r_i \sum_k c_{ijk} x_k = r_i [x_i, x_j] = [r_i x_i, x_j] = 0$ and, therefore, $c_{ijk} = 0$ for $k > n$ and $r_k \mid r_i c_{ijk}$ for $k \leq n$ if the right hand side is non-zero. Thus h' monomially reduces to zero w.r.t. $\mathcal{H}$. □

Theorem 4.20.
Let X be a free monoid on a finite alphabet and $\mathcal{L}$ a finitely generated Lie algebra over $\mathcal{R}$ with the notations from Remark 4.18. Our global monomial ordering shall be the graded left lexicographical one. Then $\mathcal{U}$ is generated by the residue classes of $x_1^{m_1} \cdots x_n^{m_n}$ in $\mathcal{P}/\langle \mathcal{G} \cup \mathcal{H} \rangle$ with $m_i \in \mathbb{N}_0$ and the relations in $\mathcal{U}$ are given via $r_i x_i = 0$, i.e.

$$\mathcal{U} \cong \frac{\langle \{\overline{x_1^{m_1} \cdots x_N^{m_N}} \mid \forall 1 \leq i \leq N : \, m_i \in \mathbb{N}_0\} \rangle}{\langle \{\overline{r_i x_i}\}_i \rangle}.$$

Proof.
Suppose that $\mathcal{W} := \langle \{\overline{x_1^{m_1} \cdots x_N^{m_N}} \mid \forall 1 \leq i \leq N : \, m_i \in \mathbb{N}_0\} \rangle$ is a proper submodule of $\mathcal{U}$ with a monomial $t \in X$ of minimal degree such that $\bar{t} \notin \mathcal{W}$. Therefore, $t \notin \{x_1^{m_1} \cdots x_N^{m_N} \mid \forall 1 \leq i \leq N : \, m_i \in \mathbb{N}_0\}$ and thus there exist $\tau = x \otimes y \in X^e$ and $i > j$ such that $t = \tau(x_i x_j) = x x_i x_j y$. Now consider $t' = x x_j x_i y - \sum_l c_{ijl} x x_l y$. Then $\mathrm{LM}(t') \prec \mathrm{LM}(t)$ in the graded left lexicographical ordering and

$$t - t' = x \left(x_i x_j - x_j x_i - \sum_l c_{ijl} x_l \right) y = \tau g_{ij}$$

is a Gröbner representation w.r.t. $\{g_{ij}\}$, hence t reduces to t' w.r.t. $\{g_{ij}\}$. This is a contradiction to t being minimal, and thus $\mathcal{W} = \mathcal{U}$.
Next we assume that there are $t_i \in \{x_1^{m_1} \cdots x_N^{m_N} \mid \forall 1 \leq i \leq N : \, m_i \in \mathbb{N}_0\}$ and non-zero $r_i \in \mathcal{R}$, such that $\sum_i \overline{r_i t_i} = 0 \in \mathcal{U}$. Clearly $\sum_i r_i t_i$ does not reduce any further w.r.t. $\mathcal{G}$, but by our assumptions it reduces to zero w.r.t. $\mathcal{G} \cup \mathcal{H}$. Thus we can only reduce w.r.t. $\mathcal{H}$ and the proof is complete. □

Especially, if $\mathcal{P}$ is commutative, then $U(\mathcal{L}) \cong \mathcal{P}/\langle r_i x_i \rangle$ as a module and if $\mathcal{L}$ is free then $U(\mathcal{L})$ is also free with basis $\{\overline{x_1^{m_1} \cdots x_n^{m_n}} \mid m_i \in \mathbb{N}_0\}$.

5 Commutative Gröbner bases over Euclidean domains

We are especially interested in the case where $\mathcal{R}$ is a Euclidean domain, since implementations in SINGULAR [24] are for $\mathbb{Z}$ or its quotients $\mathbb{Z}/m\mathbb{Z}$. What is missing in our approach from chapter 4 motivated by Pritchard [7] is a canonical form for reductions. To achieve this, we need to extend the definition of a Gröbner basis and will introduce a new type of polynomial. Lichtblau [6] refers to these polynomials also as "syzygy-polynomials", since they correspond to overlap relations of leading monomials. However, on the level of coefficients there is no cancellation taking place and we will refer to this new type of polynomial as a "G-polynomial" as it is done by Eder et al. in [1].
Let $\mathcal{R}$ be a Euclidean domain and $\mathcal{P} = \mathcal{R}[X] = \mathcal{R}[x_1, \ldots, x_n]$. We fix a global monomial ordering $\preceq$ on the commutative monoid $X = \langle x_1, \ldots, x_n \rangle$. Clearly $\mathcal{P}$ is a quotient of the polynomial ring over the free monoid, that is generated by $X_1, \ldots, X_n$. More precisely $\mathcal{P}$ is isomorphic to $\mathcal{R}\langle X_1, \ldots, X_n \rangle$ modulo all commutators $[X_i, X_j] := X_iX_j - X_jX_i$ for $1 \leq i < j \leq n$.

Definition 5.1.
Let $f, g \in \mathcal{P} \setminus \{0\}$, $\mathcal{G} = \{g_1, \ldots, g_m\} \subseteq \mathcal{P} \setminus \{0\}$ be a finite set and $\mathcal{I} \subseteq \mathcal{P}$ be an ideal.

- We say that g **LM-reduces** f, if $\mathrm{LM}(g) \mid \mathrm{LM}(f)$ and there are $a \neq 0$ and $b < \mathrm{LC}(f)$ (in the Euclidean norm), such that $\mathrm{LC}(f) = a\,\mathrm{LC}(g) + b$. Then the **LM-reduction** of f by g is given by
$$h := f - a\frac{\mathrm{LM}(f)}{\mathrm{LM}(g)}g.$$
If t is a monomial occurring in f with coefficient c, such that $\mathrm{LM}(g) \mid t$ and $c = a\mathrm{LC}(g) + b$ with a, b as above, then we say that g **reduces** f.
Extending this to sets we say that f **reduces** to some $r \in \mathcal{P}$ w.r.t. $\mathcal{G}$, if there is a finite sequence of reductions of f by $g_i \in \mathcal{G}$ that ends at r.

- We say that f has a **weak Gröbner representation** w.r.t. $\mathcal{G}$ if $f = \sum_{i=1}^{m} h_i g_i$ for some $h_i \in \mathcal{P}$ and $\mathrm{LM}(f) \geq \mathrm{LM}(h_i g_i)$ for all $1 \leq i \leq m$ with $h_i \neq 0$.

- We say that f has a **strong Gröbner representation** w.r.t. $\mathcal{G}$, if $f = \sum_{i=1}^{m} h_i g_i$ for some $h_i \in \mathcal{P}$ and there exists a unique $1 \leq j \leq m$ such that $\mathrm{LM}(f) = \mathrm{LM}(h_j g_j)$ and $\mathrm{LM}(f) \succ \mathrm{LM}(h_i g_i)$ for all $i \neq j$ with $h_i \neq 0$.

- $\mathcal{G}$ is called **weak Gröbner basis** for $\mathcal{I}$, if $\mathcal{G} \subseteq \mathcal{I}$ and $\mathrm{L}(\mathcal{G}) = \mathrm{L}(\mathcal{I})$.

- $\mathcal{G}$ is called **strong Gröbner basis** for $\mathcal{I}$, if $\mathcal{G}$ is a weak Gröbner basis for $\mathcal{I}$, such that for all $f \in \mathcal{I} \setminus \{0\}$ there exists $g \in \mathcal{G}$ with $\mathrm{LT}(g) \mid \mathrm{LT}(f)$.

Note, that the LM-reduction in the above case is given by
$$h = b\mathrm{LM}(f) + \underbrace{\mathrm{tail}(f) - a\frac{\mathrm{LM}(f)}{\mathrm{LM}(g)}\mathrm{tail}(g)}_{\text{l.o.t.}}.$$

This is a "smaller" polynomial, either in terms of the monomial ordering of leading monomials (if $b = 0$) or in terms of the Euclidean norm of leading coefficients ($|b| < |\mathrm{LC}(f)|$).
In the field case every Gröbner basis is a strong Gröbner basis. To see this, let $\mathcal{I} \subseteq \mathbb{K}[X]$ with weak Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_m\}$ and $f \in \mathcal{I}$. Suppose, that without loss of generality f and all g_i are normalized. Otherwise we divide each polynomial by its leading coefficient. Then $t := \mathrm{LM}(f) = \sum_i p_i \mathrm{LM}(g_i) =: \sum_i p_i t_i$ for some $p_i \in \mathbb{K}[X]$. Let $p_i = \sum_j \lambda_j^i t_j^i$ and $M_w := \{(i, j) \in \mathbb{N}^{1\times 2} \mid t_j^i t_i = w\}$ for $w \in X$. Then $t = \sum_{i,j} \lambda_j^i t_j^i t_i$ and thus $M_t \neq \emptyset$. Therefore, there is $(i, j) \in M_t$, such that $t_j^i \mathrm{LM}(g_i) = t_j^i t_i = t = \mathrm{LM}(f)$, i.e. $\mathcal{G}$ is strong.
However, this does not hold over $\mathbb{Z}$, since we cannot divide by leading coefficients.

Example 5.2.
Let $\mathcal{R} = \mathbb{Z}$, $\mathcal{P} = \mathbb{Z}[x]$ and $\mathcal{I} = \langle x \rangle$. Then $\mathcal{G} = \{4x, 5x\}$ is a Gröbner basis for $\mathcal{I}$, because $5x - 4x = x \in \mathrm{L}(\mathcal{G})$. But $\mathrm{LT}(4x) \nmid \mathrm{LT}(x)$ and $\mathrm{LT}(5x) \nmid \mathrm{LT}(x)$, thus $\mathcal{G}$ is not a strong Gröbner basis.

Lemma 5.3.
Every ideal $\mathcal{I} \subseteq \mathcal{P}$ has a weak Gröbner basis.

Proof.
Since $\mathcal{P}$ is Noetherian according to Hilbert's basis theorem 2.1, there is a finite generating set $\mathcal{G}_1$ of $\mathcal{I}$ and clearly $\mathrm{L}(\mathcal{G}_1) \subseteq \mathrm{L}(\mathcal{I})$. If we have equality, then $\mathcal{G}_1$ is a weak Gröbner basis for $\mathcal{I}$. Otherwise there exists $g_1 \in \mathcal{G}$ such that $\mathrm{LT}(g_0) \notin \mathrm{L}(\mathcal{G}_0)$. We define $\mathcal{G}_2 := \mathcal{G}_1 \cup \{g_1\}$ and see that $\mathrm{L}(\mathcal{G}_1) \subsetneq \mathrm{L}(\mathcal{G}_2) \subseteq \mathrm{L}(\mathcal{I})$. If the latter inclusion is also strict, we repeat the procedure and iteratively construct a sequence $\{\mathcal{G}_i\}_i$ with

$$\mathrm{L}(\mathcal{G}_1) \subsetneq \mathrm{L}(\mathcal{G}_2) \subsetneq \mathrm{L}(\mathcal{G}_3) \subsetneq \ldots \subseteq \mathrm{L}(\mathcal{I}).$$

Since $\mathcal{P}$ is Noetherian, this ideal chain becomes stationary, thus $\mathrm{L}(\mathcal{G}_k) = \mathrm{L}(\mathcal{I})$ for some $k \in \mathbb{N}$, and hence $\mathcal{G} := \mathcal{G}_k$ is a weak Gröbner basis for $\mathcal{I}$. □

We note at this point that it is possible to obtain a Strong Gröbner basis from a weak Gröbner or more precisely from any generating set, but to do this constructively we need some preparation. We do not give a theoretical proof of this statement, but present an algorithm with the desired outcome.

Theorem 5.4.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $\{0\} \neq \mathcal{I} \subseteq \mathcal{P}$ be an ideal. The following are equivalent.

1. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$.
2. Every $f \in \mathcal{I} \setminus \{0\}$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.
3. Every $f \in \mathcal{P} \setminus \{0\}$ has a unique remainder after reduction by $\mathcal{G}$, i.e. if f reduces to r_1 and r_2 w.r.t. $\mathcal{G}$ and both r_1 and r_2 cannot be any further reduced, then $r_1 = r_2$.

In the case of "3." we say that f has a **canonical reduction** w.r.t. $\mathcal{G}$. As a convention, we say that $0 \in \mathcal{I}$ always has a strong Gröbner representation and that $0 \in \mathcal{P}$ always reduces uniquely to zero.

Proof. (cf. [6], Theorem 9)
For "1. $\Rightarrow$ 2." let $f \in \mathcal{I}$. Since $\mathcal{G}$ is a strong Gröbner basis, there exists $g_1 \in \mathcal{G}$ with $\mathrm{LT}(g_1) \mid \mathrm{LT}(f)$. Then we can find $h_1 \in \mathcal{P}$ such that $\mathrm{LT}(h_1 g_1) = \mathrm{LT}(f)$ and $f_1 := f - h_1 g_1$ has a smaller leading monomial w.r.t. our global monomial ordering than f. On the other hand $f_1 \in \mathcal{I}$ and we can repeat the procedure iteratively with

$$f_i := f_{i-1} - \underbrace{\frac{\mathrm{LT}(f_{i-1})}{\mathrm{LT}(g_i)}}_{=:h_i} g_i.$$

Since $\preceq$ is a well ordering, we stop at some $k \in \mathbb{N}$ and obtain $f = \sum_{i=1}^{k} h_i g_i$. Without loss of generality we choose the g_i to be pairwise distinct, otherwise we simply collect h_i and rearrange. Then $\mathrm{LM}(h_1 g_1) \succ \mathrm{LM}(h_j g_j)$ for $j \geq 2$ and we have a strong Gröbner representation of f w.r.t. $\mathcal{G}$.
For the converse note that, if $f \in \mathcal{I}$ has a strong Gröbner representation $\sum_i h_i g_i$ w.r.t. $\mathcal{G}$, then $\mathrm{LT}(f) = \mathrm{LT}(h_i g_i)$ for exactly one i and thus $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$.
For "2. $\Rightarrow$ 3." let r_1 and r_2 be remainders as in 3. Then $r_1 - r_2$ has a strong Gröbner representation w.r.t. $\mathcal{G}$, for instance $r_1 - r_2 = \sum h_i g_i$ with $ct := \mathrm{LT}(r_1 - r_2) = \mathrm{LM}(h_j g_j)$ (recall that j is uniquely determined). Let c_1, c_2 be the coefficients of t in r_1, r_2 respectively. Suppose that $c_1 = 0$. Then $\mathrm{LT}(r_2) = ct$ and thus g_j reduces r_2 which contradicts the assumption that r_2 is fully reduced w.r.t. $\mathcal{G}$. Therefore, c_1, $c_2 \neq 0$, but then $\mathrm{LC}(g_j) \mid (c_1 - c_2)$, because $(c_1 - c_2)t$ must be reducible, while $c_1 t$, $c_2 t$ are not. Hence $c_1 \equiv c_2 \,(\mathrm{mod}\, \mathrm{LC}(g_j))$ (i.e. by reduction $c_1 = c_2$) and so $\mathrm{LT}(r_1 - r_2) = 0$ which means that $r_1 = r_2$.
To show "3. $\Rightarrow$ 2." let $f \in \mathcal{I}$ be reducing uniquely to zero w.r.t. $\mathcal{G}$. Thus we can write $f = \sum_i h_i g_i$ with $\max_{i,\preceq}\{\mathrm{LM}(h_i g_i)\} = t := \mathrm{LM}(f)$. This is a Gröbner representation and we need to show that $\mathrm{card}(\{i \mid \mathrm{LM}(h_i g_i) = t\}) = 1$. Suppose it is bigger than one. Since $\preceq$ and the Euclidean norm are well orderings, we can assume additionally that t is minimal among all monomials $\tilde{t}$ with the property $\mathrm{card}(\{i \mid \mathrm{LM}(h_i g_i) = \tilde{t}\}) > 1$ and $c := \mathrm{LC}(f)$ is minimal among all coefficients for which there is no strong Gröbner representation with leading monomial t. Also without loss of generality let $\{i \mid \mathrm{LM}(h_i g_i) = t\} = \{1, \ldots, k\}$ and $b = \sum_i \lambda_i \mathrm{LC}(g_i)$ the Bézout identity for the greatest common divisor of all leading coefficients which can be obtained from the extended Euclidean algorithm. Especially we have $b \mid c$, say $c = db$. Let $s_i = \dfrac{t}{\mathrm{LM}(g_i)}$ for $1 \leq i \leq k$ and $g = \sum_i s_i \lambda_i g_i$. By this construction we have $\mathrm{LT}(g) = bt$. Suppose $b = c$. But, since $b \leq \mathrm{LC}(h_i g_i) \leq c$, this implies $k = 1$, thus $b < c$. As c was chosen to be minimal there is a strong Gröbner representation of g, say $g = \sum_i \tilde{h}_i g_i$ with $\mathrm{LM}(\tilde{h}_j g_j) = t$. Since $c = db$, we have $\mathrm{LM}(f - dg) \prec t$ and, therefore, $(f - dg)$ has a strong Gröbner representation. In particular f has a strong Gröbner representation. □

The condition "Every element of $\mathcal{I}$ has a strong Gröbner representation" is not a useful

criterion for an algorithm to terminate. Therefore, we introduce polynomials, which we want to check for zero-reductions in order to obtain a strong Gröbner basis constructively. S-polynomials are well known from the field case, but do not suffice over rings. Hence a new type of polynomial is defined as in [1] or similarly in [6].

Definition 5.5.
Let $f, g \in \mathcal{P} \setminus \{0\}$. We set

- $t := \operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))$, $t_f := \dfrac{t}{\operatorname{LM}(f)}$, $t_g := \dfrac{t}{\operatorname{LM}(g)}$,
- $a := \operatorname{lcm}(\operatorname{LC}(f), \operatorname{LC}(g))$, $a_f := \dfrac{a}{\operatorname{LC}(f)}$, $a_g := \dfrac{a}{\operatorname{LC}(g)}$ and
- $b := \gcd(\operatorname{LC}(f), \operatorname{LC}(g))$ with coefficients $b_f, b_g \in \mathcal{R}$ such that $b = b_f \operatorname{LC}(f) + b_g \operatorname{LC}(g)$.

Then the **S-polynomial** of f and g is defined as

$$\operatorname{spoly}(f, g) := a_f t_f f - a_g t_g g$$

and a **G-polynomial** of f and g is defined as

$$\operatorname{gpoly}(f, g) := b_f t_f f + b_g t_g g.$$

Example 5.6.
We reconsider our previous example with $f = 4x$ and $g = 5x$. Then

- $t = x$, $t_f = t_g = 1$,
- $a = 20$, $a_f = 5$, $a_g = 4$ and
- $b = 1 = (-1) \cdot 4 + 1 \cdot 5$ with $b_f = -1$, $b_g = 1$.

We optain $\operatorname{spoly}(f, g) = 5 \cdot 1 \cdot 4x - 4 \cdot 1 \cdot 5x = 0$ and $\operatorname{gpoly}(f, g) = (-1) \cdot 1 \cdot 4x + 1 \cdot 1 \cdot 5x = x$. In fact, $\{4x, 5x, x\}$ is a strong Gröbner basis for $\mathcal{I}$. When computing the S-polynomial the leading terms cancel each other out. The G-polynomial clearly has the advantage of reducing the leading coefficients whilst keeping the leading monomial.
However, a G-polynomial is not unique. Take for example $f = 4x + 1$ and $g = 6y + 3$. Then $\gcd(\operatorname{LC}(f), \operatorname{LC}(g)) = 2 = (-1) \cdot 4 + 1 \cdot 6 = 2 \cdot 4 + (-1) \cdot 6$ and we obtain $\operatorname{gpoly}_1(f, g) = 2xy + 3x - y \neq 2xy - 3x + 2y = \operatorname{gpoly}_2(f, g)$. So to speak of "the" G-polynomial we fix one algorithm to compute the greatest common divisor and coefficients of the Bézout identity, well known as the extended Euclidean algorithm (ExtGcd). Note that if we speak of a Euclidean norm, we mean a total ordering, thus over $\mathbb{Z}$ we have $|0| < |1| < |-1| < |2| < |-2| < \dots$, etc.

Algorithm 5.7. (**Extended Euclidean algorithm**)
The following algorithm is well known and computes for two elements of a Euclidean domain the greatest common divisor plus coefficients for their Bézout identity.

ExtGcd

input: $a, b \in \mathcal{R}$
output: $(x, y, c) \in \mathcal{R}^{1\times 3}$ with $c = \gcd(a, b) = ax + by$
01: $r = b$, $r' = a$, $s = 0$, $s' = 1$, $t = 0$
02: **while** $r \neq 0$ **do**
03: determine $q \in \mathcal{R}$ such that $|r' - qr| < |r|$ is minimal
04: $(r, r', s, s') = (r' - qr, r, s' - qs, s)$
05: **end while**
06: **if** $b \neq 0$ **then**
07: $t = \dfrac{r' - s'a}{b}$
08: **end if**
09: **return** (s', t, r')

Correctness and termination follow from the uniqueness of division with remainder in Euclidean domains (q is uniquely determined) and the fact that the Euclidean norm of r decreases strictly. If $b \mid a$ then the algorithm returns $(0, 1, b)$ thus one coefficient of the corresponding G-polynomial is always zero.

Definition 5.8.
Let $\mathfrak{G}$ be the set of all finite subsets of $\mathcal{P}$, that are partially ordered w.r.t. $\preceq$. A map NF: $\mathcal{P} \times \mathfrak{G} \to \mathcal{P}$ is called **strong normal form**, if for all $f \in \mathcal{P}$ and $\mathcal{G} \in \mathfrak{G}$ we have

1. $\mathrm{NF}(0, \mathcal{G}) = 0$,
2. $\mathrm{NF}(f, \mathcal{G}) = 0$ or no $g \in \mathcal{G}$ LM-reduces $\mathrm{NF}(f, \mathcal{G})$ and
3. $\mathrm{NF}(f, \mathcal{G}) = f$ or $\mathrm{NF}(f, \mathcal{G}) - f$ has a strong Gröbner representation w.r.t. $\mathcal{G}$ for $f \neq 0$.

From now on we will refer to strong normal forms simply as normal forms.

Algorithm 5.9. (**Normal Form Algorithm over** $\mathcal{R}[X]$)
The following algorithm computes a normal form using LM-reductions.

NormalForm

input: $f \in \mathcal{P}$, $\mathcal{G} \subseteq \mathcal{P}$ finite and partially ordered
output: normal form of f w.r.t. $\mathcal{G}$
01: $h = f$
02: **while** $h \neq 0$ **and** $\mathcal{G}_h = \{g \in \mathcal{G} \mid g \text{ LM-reduces } h\} \neq \emptyset$ **do**
03: choose $g \in \mathcal{G}_h$
04: choose $a \in \mathcal{R} \setminus \{0\}$ with $\mathrm{LC}(h) = a\mathrm{LC}(g) + b$ for $b < \mathrm{LC}(h)$
05: $h = h - a\dfrac{\mathrm{LM}(h)}{\mathrm{LM}(g)}g$ LM-reduction of h by g
06: **end while**
07: **return** h

The algorithm terminates, because both the Euclidean norm and $\preceq$ are well-orderings. If $f = 0$, then clearly the procedure returns 0. If $h = \mathrm{NormalForm}(f, \mathcal{G}) \neq 0$, then there exists no $g \in \mathcal{G}$ such that g LM-reduces h. Furthermore, if $f \neq \mathrm{NormalForm}(f, \mathcal{G})$, then there is an element $g \in \mathcal{G}$ that LM-reduces f. If the $h_0, \ldots, h_m$ are the elements computed throughout the while loop, then the sum $\sum_i a_i \dfrac{\mathrm{LM}(h_i)}{\mathrm{LM}(g_i)} g_i$ is finite and has a strong Gröbner representation w.r.t. $\mathcal{G}$.

Theorem 5.10.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$. The following are equivalent.

1. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I} := \langle \mathcal{G} \rangle$.
2. For all $f, g \in \mathcal{G}$ both their S-polynomial and G-polynomial reduce to zero w.r.t. $\mathcal{G}$.
3. Let $f, g \in \mathcal{G}$. If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$ or $\mathrm{LC}(g) \mid \mathrm{LC}(f)$, then $\mathrm{spoly}(f, g)$ reduces to zero w.r.t. $\mathcal{G}$. Otherwise if $\mathrm{LC}(f) \nmid \mathrm{LC}(g)$ and $\mathrm{LC}(g) \nmid \mathrm{LC}(f)$, then $\mathrm{gpoly}(f, g)$ reduces to zero w.r.t. $\mathcal{G}$.

Proof.
The implication "1. $\Rightarrow$ 2." follows immediately from Theorem 5.4.
For "2. $\Rightarrow$ 1." let $\mathcal{G} = \{g_1, \ldots, g_m\}$. Let $f \in \mathcal{I}$ with $t := \mathrm{LM}(f)$ and $f = \sum_i p_i g_i$ a weak Gröbner representation for some $p_i \in \mathcal{P}$. We choose a representation of f where $\tilde{t} := \max\{\mathrm{LM}(p_i g_i)\}_i \succeq t$ is minimal and need to show that the set $\{1 \leq i \leq m \mid \mathrm{LM}(p_i g_i) = \tilde{t}\}$ contains exactly one element. Then we have a strong Gröbner representation of f w.r.t. $\mathcal{G}$. Now suppose for a contradiction that after rearranging indices we have $\mathrm{LM}(p_i g_i) = \tilde{t}$ (eventually after rearranging indices). We choose $\sum_i |\mathrm{LC}(p_i)\mathrm{LC}(g_i)|$ to be minimal in the Euclidean norm w.r.t. $\tilde{t}$ and set

$$t_{ij} := \frac{\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LM}(g_i)} \quad \text{and} \quad w := \frac{\tilde{t}}{\mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}$$

for $1 \leq i, j \leq k$. Furthermore, for the Bézout identity $d := \gcd(\mathrm{LC}(g_1), \mathrm{LC}(g_2)) = b_1\mathrm{LC}(g_1) + b_2\mathrm{LC}(g_2)$ with $b_1, b_2 \in \mathcal{R}$ we set

$$c_{12} := \frac{\mathrm{lcm}(\mathrm{LC}(g_1), \mathrm{LC}(g_2))}{\mathrm{LC}(g_1)} \quad \text{and} \quad c_{21} := \frac{\mathrm{lcm}(\mathrm{LC}(g_2), \mathrm{LC}(g_1))}{\mathrm{LC}(g_2)}.$$

Then

$$\mathrm{spoly}(g_1, g_2) = c_{12}t_{12}g_1 - c_{21}t_{21}g_2 \quad \text{and} \quad \mathrm{gpoly}(g_1, g_2) = b_1t_{12}g_1 + b_2t_{21}g_2,$$

which reduce to zero by our hypothesis. Note that d divides $\mathrm{LC}(p_1)\mathrm{LC}(g_1)+\mathrm{LC}(p_2)\mathrm{LC}(g_2)$, thus there exists $a \in \mathcal{R} \setminus \{0\}$, such that

$$\mathrm{LC}(p_1)\mathrm{LC}(g_1) + \mathrm{LC}(p_2)\mathrm{LC}(g_2) = ad = ab_1\mathrm{LC}(g_1) + ab_2\mathrm{LC}(g_2)$$

or equivalently

$$\mathrm{LC}(p_1)\mathrm{LC}(g_1) = ab_1\mathrm{LC}(g_1) + ab_2\mathrm{LC}(g_2) - \mathrm{LC}(p_2)\mathrm{LC}(g_2),$$

i.e. $\mathrm{LC}(p_1) = ab_1 + bc_{12}$ for some $b \in \mathcal{R} \setminus \{0\}$ and analogously $\mathrm{LC}(p_2) = ab_2 + bc_{21}$. Therefore, with $|a_1\mathrm{LC}(g_1) + a_2\mathrm{LC}(g_2)| > 0$ and by the triangle inequality we have

$$\begin{aligned}
&|\mathrm{LC}(p_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(p_2)\mathrm{LC}(g_2)| \\
=&|(ab_1 + bc_{12})\mathrm{LC}(g_1)| + |(ab_2 + bc_{21})\mathrm{LC}(g_2)| \\
\geq&|ab_1\mathrm{LC}(g_1)| + |bc_{12}\mathrm{LC}(g_1)| + |ab_2\mathrm{LC}(g_2)| + |bc_{21}\mathrm{LC}(g_2)| \\
>&|ab_1\mathrm{LC}(g_1)| + |ab_2\mathrm{LC}(g_2)| \\
\geq&|ab_1\mathrm{LC}(g_1) + ab_2\mathrm{LC}(g_2)| \\
=&|ad|,
\end{aligned}$$

thus $|ad| < |\mathrm{LC}(p_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(p_2)\mathrm{LC}(g_2)|$. Furthermore, we have

$$\begin{aligned}
p_1g_1 + p_2g_2 &= \mathrm{LC}(p_1)\mathrm{LM}(p_1)g_1 + \mathrm{tail}(p_1)g_1 + \mathrm{LC}(p_2)\mathrm{LM}(p_2)g_2 + \mathrm{tail}(p_2)g_2 \\
&= \mathrm{LC}(p_1)\frac{\tilde{t}}{\mathrm{LM}(g_1)}g_1 + \mathrm{tail}(p_1)g_1 + \mathrm{LC}(p_2)\frac{\tilde{t}}{\mathrm{LM}(g_2)}g_2 + \mathrm{tail}(p_2)g_2 \\
&= \mathrm{LC}(p_1)t_{12}wg_1 + \mathrm{tail}(p_1)g_1 + \mathrm{LC}(p_2)t_{21}wg_2 + \mathrm{tail}(p_2)g_2 \\
&= aw\,\mathrm{gpoly}(g_1, g_2) + bw\,\mathrm{spoly}(g_1, g_2) + \underbrace{\mathrm{tail}(p_1)g_1 + \mathrm{tail}(p_2)g_2}_{\text{l.o.t.}}.
\end{aligned}$$

This yields a new representation for f with polynomials $p'_j \in \mathcal{P}$. But, since $\mathrm{LM}(\tau\,\mathrm{spoly}(g_1, g_2)) \prec \tilde{t}$, $\mathrm{LM}(\mathrm{tail}(h_1)g_1) \prec \tilde{t}$, $\mathrm{LM}(\mathrm{tail}(h_2)g_1) \prec \tilde{t}$ and $|ad| < |\mathrm{LC}(p_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(p_2)\mathrm{LC}(g_2)|$, we have

$$\begin{aligned}
&\sum_j |\mathrm{LC}(p'_j)\mathrm{LC}(g_j)| \\
=&\sum_j |\mathrm{LC}(p'_jg_j)| \\
=&|\mathrm{LC}(d\tau\,\mathrm{gpoly}(g_1, g_2))| \\
=&|ad| \\
<&|\mathrm{LC}(p_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(p_2)\mathrm{LC}(g_2)|,
\end{aligned}$$

which contradicts our assumption that the leading coefficient of our original representation are minimal. Therefore, we have a strong Gröbner representation of f w.r.t. $\mathcal{G}$, i.e. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$.
Clearly "2. $\Rightarrow$ 3." holds.
To show "3. $\Rightarrow$ 2." we assume without loss of generality that $|\mathrm{LC}(f)| \leq |\mathrm{LC}(g)|$ in the Euclidean norm. If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$, then by Lemma 5.13 $\mathrm{gpoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$ and by 3. also $\mathrm{spoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$. Next we assume that $\mathrm{LC}(f) \nmid \mathrm{LC}(g)$. Let $d = \gcd(\mathrm{LC}(f), \mathrm{LC}(g))$. We write $\mathrm{spoly}(f, g) = a_f t_f \,\mathrm{tail}(f) - a_g t_g \,\mathrm{tail}(g)$ and $\mathrm{gpoly}(f, g) = dt + b_f t_f \,\mathrm{tail}(f) + b_g t_g \,\mathrm{tail}(g)$ with the usual notation. Then with

$$a_g d = \frac{\mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g))}{\mathrm{LC}(g)} \gcd(\mathrm{LC}(f), \mathrm{LC}(g)) = \frac{\mathrm{LC}(g)\mathrm{LC}(f)}{\mathrm{LC}(g)} = \mathrm{LC}(f)$$

and

$$\begin{aligned} a_g b_f + a_f b_g &= \mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g)) \left(\frac{b_f}{\mathrm{LC}(g)} + \frac{b_g}{\mathrm{LC}(f)} \right) \\ &= \mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g)) \left(\frac{b_f \mathrm{LC}(f) + b_g \mathrm{LC}(g)}{\mathrm{LC}(g)\mathrm{LC}(f)} \right) \\ &= \frac{d}{d} = 1 \end{aligned}$$

we have

$$\begin{aligned} \mathrm{spoly}(f, \mathrm{gpoly}(f, g)) &= t_f f - a_g \,\mathrm{gpoly}(f, g) \\ &= \mathrm{LC}(f)t + t_f \,\mathrm{tail}(f) - a_g(dt + b_f t_f \,\mathrm{tail}(f) + b_g t_g \,\mathrm{tail}(g)) \\ &= t_f \,\mathrm{tail}(f) - a_g b_f t_f \,\mathrm{tail}(f) - a_g b_g t_g \,\mathrm{tail}(g) \\ &= (1 - a_g b_f) t_f \,\mathrm{tail}(f) - b_g a_g t_g \,\mathrm{tail}(g) \\ &= b_g a_f t_f \,\mathrm{tail}(f) - b_g a_g t_g \,\mathrm{tail}(g) \\ &= b_g \,\mathrm{spoly}(f, g). \end{aligned}$$

Analogously $\mathrm{spoly}(\mathrm{gpoly}(f, g), g) = b_f \,\mathrm{spoly}(f, g)$. Therefore,

$$\begin{aligned} &\mathrm{gpoly}(\mathrm{spoly}(f, \mathrm{gpoly}(f, g)), \mathrm{spoly}(\mathrm{gpoly}(f, g), g)) \\ =&\mathrm{gpoly}(b_g \,\mathrm{spoly}(f, g), b_f \,\mathrm{spoly}(f, g)) \\ =&\mathrm{spoly}(f, g), \end{aligned}$$

because b_g, b_f are coprime. Hence we can obtain the S-polynomial of f and g iteratively. This completes the proof. □

When computing a strong Gröbner basis, then this criterion tells us to stop, when all S- and G-polynomials reduce to zero by the second condition. On the other hand we could use the third of the three equivalent conditions by only considering S-polynomials when one leading coefficient divides the other. Then it makes sense to choose pairs by their leading coefficients, when computing their S- and G-polynomials.

Algorithm 5.11. (**Buchberger's algorithm for strong Gröbner bases over $\mathcal{R}[X]$**) The following algorithm computes a strong Gröbner $\mathcal{G}$ basis for an ideal $\mathcal{I}$ given by a set of input polynomials.

SBBA

---

input: $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subseteq \mathcal{P}$, NormalForm
output: strong Gröbner basis $\mathcal{G}$ for $\mathcal{I}$
01: $\mathcal{G} = \{f_1, \ldots, f_m\}$
02: $\mathcal{L} = \{\text{spoly}(f_i, f_j), \text{gpoly}(f_i, f_j) \mid i < j\}$
03: **while** $\mathcal{L} \neq \emptyset$ **do**
04: choose $h \in \mathcal{L}$
05: $\mathcal{L} = \mathcal{L} \setminus \{h\}$
06: $h = \text{NF}(h, \mathcal{G})$
07: **if** $h \neq 0$ **then**
08: $\mathcal{L} = \mathcal{L} \cup \{\text{spoly}(g, h), \text{gpoly}(g, h) \mid g \in \mathcal{G}\}$
09: $\mathcal{G} = \mathcal{G} \cup \{h\}$
10: **end if**
11: **end while**
12: **return** $\mathcal{G}$

The correctness of the algorithm follows from Theorem 5.10, "1. $\Leftrightarrow$ 2.". At the beginning $\mathcal{G}$ consists of the input polynomials and all S- and G-polynomials of possible pairs are constructed. Each such element h goes through a sequence of LM-reduction by elements of $\mathcal{G}$ in shape of the normal form procedure. Once h is fully reduced it is either zero or added to $\mathcal{G}$ and for every new pair the S- and G-polynomial is constructed. Once all S- and G-polynomials reduce to zero we can apply Buchberger's Criterion 5.10 to see that $\mathcal{G}$ is indeed a strong Gröbner basis for $\mathcal{I}$. Termination of the algorithm is analogous to the proof of 5.3, where we used the fact that $\mathcal{P}$ is Noetherian.

The above algorithm completely suffices to compute a strong Gröbner basis. At least in theory. We are interested in speeding up the process by looking at the steps of the algorithm and see whether we can improve them. First of all note that the core of the algorithm is the normal form which is based on the idea of LM-reductions. These reductions take place if one leading monomial divides another regardless of the leading coefficient. If we can reduce the number of elements of the set $\mathcal{G}_h$ in Algorithm 5.11 that LM-reduce h, then we are in a situation similar to the field case as the following Lemma shows.

Lemma 5.12.
For $g, h \in \mathcal{P} \setminus \{0\}$ we say that g **LT-reduces** h, if $\text{LM}(g) \mid \text{LM}(h)$ and $\text{LC}(g) \mid \text{LC}(h)$. Especially in the definition of LM-reductions we have $a = \dfrac{\text{LC}(h)}{\text{LC}(g)}$ and $b = 0$. Then the

LT-reduction of h by g is given by

$$h - \frac{\mathrm{LC}(h)}{\mathrm{LC}(g)} \frac{\mathrm{LM}(h)}{\mathrm{LM}(g)} g.$$

These are precisely the type of reductions that take place in the field case. Now, if we replace the set $\mathcal{G}_h$ in Algorithm 5.9 by

$$\mathcal{G}_h := \{g \in \mathcal{G} \mid g \text{ LT-reduces } h\}$$

then Algorithm 5.11 still terminates and computes a strong Gröbner basis for the given input ideal $\mathcal{I}$.

Proof.
Let $h \in \mathcal{P} \setminus \{0\}$ be an element obtained during Algorithm 5.11 by LT-reductions. We assume, that there exists a $g \in \mathcal{G}$ that LM-reduces h, but does not LT-reduce it, i.e. $\mathrm{LM}(g) \mid \mathrm{LM}(h)$ and $\mathrm{LC}(g) \nmid \mathrm{LC}(h)$ with $|\mathrm{LC}(g)| < |\mathrm{LC}(h)|$. Then $\mathrm{gpoly}(g, h) = b_g t_g g + b_h t_h h$ with $t_h = 1$, $t_g = \dfrac{\mathrm{LM}(h)}{\mathrm{LM}(g)}$ and $\gcd(\mathrm{LC}(g), \mathrm{LC}(h)) = b_g \mathrm{LC}(g) + b_h \mathrm{LC}(h)$. If $b_h = 1$, then $\mathrm{LC}(h) = -b_g \mathrm{LC}(g) + \gcd(\mathrm{LC}(g), \mathrm{LC}(h))$ with $|\gcd(\mathrm{LC}(g), \mathrm{LC}(h))| < |\mathrm{LC}(h)|$ and the LM-reduction of h by g is given by

$$h - (-b_g)\frac{\mathrm{LM}(h)}{\mathrm{LM}(g)} g = b_g t_g g + h = \mathrm{gpoly}(g, h).$$

Otherwise if $b_h \neq 1$, then let $\tilde{h} = h - a\dfrac{\mathrm{LM}(h)}{\mathrm{LM}(g)} g$ be a LM-reduction of h by g with $a \in \mathcal{R} \setminus \{0\}$. If $\tilde{h}$ is further LM-reducible by some $\tilde{g}$ then $\tilde{g} \neq g$, because $|\mathrm{LC}(\tilde{h})| < |\mathrm{LC}(g)|$, i.e. g cannot LM-reduce $\tilde{h}$ any further by definition. Let the LM-reduction of $\tilde{h}$ by $\tilde{g}$ be given by

$$\tilde{h} - \tilde{a}\frac{\mathrm{LM}(\tilde{h})}{\mathrm{LM}(\tilde{g})}\tilde{g} = h - a\frac{\mathrm{LM}(h)}{\mathrm{LM}(g)} g - \tilde{a}\frac{\mathrm{LM}(\tilde{h})}{\mathrm{LM}(\tilde{g})}\tilde{g}$$

for some $\tilde{a} \in \mathcal{R} \setminus \{0\}$ and

$$a\frac{\mathrm{LM}(h)}{\mathrm{LM}(g)} g + \tilde{a}\frac{\mathrm{LM}(\tilde{h})}{\mathrm{LM}(\tilde{g})}\tilde{g}$$

is either a multiple of $\mathrm{spoly}(g, \tilde{g})$ or of $\mathrm{gpoly}(g, \tilde{g})$, because the leading monomials of the two summands are equal. Since the algorithm terminates if and only if $\mathcal{G}$ is a strong Gröbner basis, we find strong Gröbner represenations for the S- and G-polynomial and thus h will be eventually replaced by the above LM-reduction of $\tilde{h}$. However, this sequence of LM-reductions will stop after finitely many steps, because the leading monomial decreases in the global monomial ordering and thus we may assume without loss of generality that $\tilde{h}$ does not LM-reduce any further. Then we compute the G-polynomial of g and $\tilde{h}$. Note that $\mathrm{LM}(h) = \mathrm{LM}(\tilde{h})$ and the LM-reduction corresponds to the first step in the Euclidean algorithm. Therefore, we have

$$\mathrm{gpoly}(g, \tilde{h}) - a\frac{\mathrm{LM}(h)}{\mathrm{LM}(g)} g + h = \mathrm{gpoly}(g, h).$$

In both cases we showed that the LM-reduction is not necessary, because it is obtained through a G-polynomial, which is added to the set $\mathcal{L}$ in the later steps of the algorithm. This completes the proof. □

Another point of improvement is finding criteria to predict zero reductions before S- or G-polynomials are computed and unnecessarily added to $\mathcal{L}$ in Algorithm 5.11.

Lemma 5.13.
Let $f, g \in \mathcal{P} \setminus \{0\}$ with $\mathrm{LC}(f) \mid \mathrm{LC}(g)$. Then $\mathrm{gpoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$.

Proof.
In the definition of the G-polynomial we have $b = \gcd(\mathrm{LC}(f), \mathrm{LC}(g)) = \mathrm{LC}(f)$ and thus we can choose (or compute with ExtGcd) $b_f = 1$ and $b_g = 0$. Then $\mathrm{gpoly}(f, g) = t_f f$ is by f reducible to zero. □

The next criteria are due to Buchberger. The first one is known as Buchberger's product criterion.

Lemma 5.14.
Let $f, g \in \mathcal{P} \setminus \{0\}$ with $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ coprime and $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ coprime. Then $\mathrm{spoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$.

Proof.
Under the above assumptions we have $\mathrm{spoly}(f, g) = \mathrm{LC}(g)\mathrm{LM}(g)f - \mathrm{LC}(f)\mathrm{LM}(f)g = (g - \mathrm{tail}(g))f - (f - \mathrm{tail}(f))g = \mathrm{tail}(f)g - \mathrm{tail}(g)f$, but, since $\mathrm{LM}(f)$ divides $\mathrm{LT}(\mathrm{tail}(g)f)$ while $\mathrm{LM}(g)$ does not and vice versa, the two leading terms $\mathrm{LT}(\mathrm{tail}(g)f)$ and $\mathrm{LT}(\mathrm{tail}(f)g)$ do not cancel each other out. To see this, suppose otherwise that $\mathrm{LT}(\mathrm{tail}(f)g) = \mathrm{LT}(\mathrm{tail}(g)f)$. Since $\mathcal{R}$ is a domain, we have that $\mathrm{LT}(\mathrm{tail}(f)g) = \mathrm{LT}(\mathrm{tail}(f))\mathrm{LT}(g)$ and $\mathrm{LT}(\mathrm{tail}(g)f) = \mathrm{LT}(\mathrm{tail}(g))\mathrm{LT}(f)$. But then $\mathrm{lcm}(\mathrm{LT}(f), \mathrm{LT}(g)) = \mathrm{LT}(f)\mathrm{LT}(g)$ divides $\mathrm{LT}(\mathrm{tail}(f))\mathrm{LT}(g)$, which contradicts the fact that $\mathrm{LM}(\mathrm{tail}(f)) \prec \mathrm{LM}(f)$.
On the other hand $\mathrm{tail}(g)f$ reduces to zero w.r.t. $\{f\}$ and $\mathrm{tail}(f)g$ reduces to zero w.r.t. $\{g\}$, thus we have that $\mathrm{spoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$. □

The next two lemmata are versions of Buchberger's chain criterion, one for S-polynomials and one for G-polynomials, but we first need the following remark.

Remark 5.15.

- Let $\{a, b, c\} \subseteq \mathcal{R} \setminus \{0\}$ or $\{a, b, c\}$ a set of non-zero monomials. If a divides $\mathrm{lcm}(b, c)$ then $\mathrm{lcm}(a, b)$ divides $\mathrm{lcm}(b, c)$. To see this, let $ad = \mathrm{lcm}(b, c)$. Then ad is a multiple of a as well as of b. Thus $\mathrm{lcm}(a, b)$ divides $ad = \mathrm{lcm}(b, c)$.
- Let $f, g \in \mathcal{P} \setminus \{0\}$, $\{g_1, g_2, g_3\} \subseteq \mathcal{G} \setminus \{0\}$ and $t := \mathrm{lcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$ with $\mathrm{LM}(g_3) \mid t$. If both f and g have strong Gröbner representations w.r.t. $\mathcal{G}$ and $\mathrm{LM}(f) \prec t$, $\mathrm{LM}(g) \prec t$, then so does $f + g$ inductively.

Lemma 5.16.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and f, g, $h \in \mathcal{G}$ with

1. $\mathrm{LM}(f) \mid \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h))$,
2. $\mathrm{LC}(f) \mid \mathrm{lcm}(\mathrm{LC}(g), \mathrm{LC}(h))$ and
3. both $\mathrm{spoly}(f, g)$ and $\mathrm{spoly}(f, h)$ have a strong Gröbner representation w.r.t. $\mathcal{G}$.

Then $\mathrm{spoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.

Proof.
Our goal is to write $\mathrm{spoly}(g, h)$ as a sum of $\mathrm{spoly}(f, g)$ and $\mathrm{spoly}(f, h)$ such that the leading terms do not cancel each other out. Then $\mathrm{spoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$. For this we define

$$c_{ab} := \frac{\mathrm{lcm}(\mathrm{LC}(a), \mathrm{LC}(b))}{\mathrm{LC}(a)} \quad \text{and} \quad t_{ab} := \frac{\mathrm{lcm}(\mathrm{LM}(a), \mathrm{LM}(b))}{\mathrm{LM}(a)}$$

with a, $b \in \{f, g, h\}$. We recognize these as the factors in the definition of S-polynomials. By Remark 5.15 and assumptions 1., respectively 2., we have $t_{hf} \mid t_{hg}$ and $t_{gf} \mid t_{gh}$, respectively $c_{hf} \mid c_{hg}$ and $c_{gf} \mid c_{gh}$. Also note that $\mathrm{LC}(a)c_{ab} = \mathrm{LC}(b)c_{ba}$ and we have the analogous symmetry relation for t_{ab}. Thus

$$\begin{aligned}
&\frac{c_{hg}}{c_{hf}}\frac{t_{hg}}{t_{hf}}\,\mathrm{spoly}(f, h) - \frac{c_{gh}}{c_{gf}}\frac{t_{gh}}{t_{gf}}\,\mathrm{spoly}(f, g)\\
=&\frac{c_{hg}}{c_{hf}}\frac{t_{hg}}{t_{hf}}(c_{fh}t_{fh}f - c_{hf}t_{hf}h) - \frac{c_{gh}}{c_{gf}}\frac{t_{gh}}{t_{gf}}(c_{fg}t_{fg}f - c_{gf}t_{gf}g)\\
=&c_{gh}t_{gh}g - c_{hg}t_{hg}h + \left(\frac{c_{hg}c_{fh}}{c_{hf}}\frac{t_{hg}t_{fh}}{t_{hf}}f - \frac{c_{gh}c_{fg}}{c_{gf}}\frac{t_{gh}t_{fg}}{t_{gf}}f\right)\\
=&\,\mathrm{spoly}(g, h) + \underbrace{\left(\frac{c_{hg}c_{fh}}{c_{hf}}\frac{t_{hg}t_{fh}}{t_{hf}} - \frac{c_{gh}c_{fg}}{c_{gf}}\frac{t_{gh}t_{fg}}{t_{gf}}\right)}_{\star} f
\end{aligned}$$

and the above symmetry relation for c_{ab} yields

$$\frac{c_{hg}c_{fh}}{c_{hf}} = \frac{\mathrm{LC}(h)}{\mathrm{LC}(h)}\frac{c_{hg}c_{fh}}{c_{hf}} = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)}\frac{c_{gh}c_{fh}}{c_{fh}} = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)}c_{gh} = \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)}c_{hg}.$$

Analogously we have $\frac{c_{gh}c_{fg}}{c_{gf}} = \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)}c_{hg}$ and $\frac{t_{hg}t_{fh}}{t_{hf}} = \frac{\mathrm{LM}(h)}{\mathrm{LM}(f)}t_{hg} = \frac{t_{gh}t_{fg}}{t_{gf}}$. Therefore, the expression $\star$ in brackets vanishes and we have

$$\mathrm{spoly}(g, h) = \frac{c_{hg}}{c_{hf}}\frac{t_{hg}}{t_{hf}}\,\mathrm{spoly}(f, h) - \frac{c_{gh}}{c_{gf}}\frac{t_{gh}}{t_{gf}}\,\mathrm{spoly}(f, g).$$

From Remark 5.15 it follows that $\mathrm{spoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$. □

Lemma 5.17.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $f, g, h \in \mathcal{G}$ with

1. $\mathrm{LM}(f) \mid \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h))$ and
2. $\mathrm{LC}(f) \mid \gcd(\mathrm{LC}(g), \mathrm{LC}(h))$.

Then $\mathrm{gpoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.

Proof.
We use the notation for t_{ab} from the proof of Lemma 5.16 with $a, b \in \{f, g, h\}$. Let $\gcd(\mathrm{LC}(g), \mathrm{LC}(h)) = b_g \mathrm{LC}(g) + b_h \mathrm{LC}(h)$. Then

$$\begin{aligned}\mathrm{gpoly}(g, h) &= b_g t_{gh} g + b_h t_{hg} h \\ &= \gcd(\mathrm{LC}(g), \mathrm{LC}(h)) \,\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LC}(h)) + b_g t_{gh} \,\mathrm{tail}(g) + b_h t_{hg} \,\mathrm{tail}(h)\end{aligned}$$

and by the second assumption we especially have that $\mathrm{LC}(f)$ divides both $\mathrm{LC}(g)$ and $\mathrm{LC}(h)$. Therefore, we have

$$\mathrm{spoly}(f, g) = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} t_{fg} f - t_{gf} g = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} t_{fg} \,\mathrm{tail}(f) - t_{gf} \,\mathrm{tail}(g)$$

and

$$\mathrm{spoly}(f, h) = \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} t_{fh} f - t_{hf} h = \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} t_{fh} \,\mathrm{tail}(f) - t_{hf} \,\mathrm{tail}(h).$$

Furthermore, note that

$$w := \frac{t_{gh} t_{fg}}{t_{gf}} = \frac{\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h))}{\mathrm{LM}(f)} = \frac{t_{hg} t_{fh}}{t_{hf}}$$

is a monomial by our first assumption, and

$$d := b_g \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} + b_h \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} = \frac{b_g \mathrm{LC}(g) + b_h \mathrm{LC}(h)}{\mathrm{LC}(f)} = \frac{\gcd(\mathrm{LC}(g), \mathrm{LC}(h))}{\mathrm{LC}(f)} \in \mathcal{R}$$

is an element of $\mathcal{R}$ by our second assumption. Then

$$dw\mathrm{LT}(f) = \gcd(\mathrm{LC}(g), \mathrm{LC}(h)) \,\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LC}(h))$$

and altogether we obtain

$$\begin{aligned}&\mathrm{gpoly}(g, h) - dwf + b_g \frac{t_{gh}}{t_{gf}} \mathrm{spoly}(f, g) + b_h \frac{t_{hg}}{t_{hf}} \mathrm{spoly}(f, h) \\ &= \gcd(\mathrm{LC}(g), \mathrm{LC}(h)) \,\mathrm{lcm}(\mathrm{LM}(g), \mathrm{LC}(h)) + b_g t_{gh} \,\mathrm{tail}(g) + b_h t_{hg} \,\mathrm{tail}(h) \\ &\quad - (dw\mathrm{LT}(f) + dw \,\mathrm{tail}(f)) \\ &\quad - \left(b_g t_{gh} \,\mathrm{tail}(g) - b_g \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \frac{t_{gh} t_{fg}}{t_{gf}} \,\mathrm{tail}(f) \right) \\ &\quad - \left(b_h t_{hg} \,\mathrm{tail}(h) - b_h \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} \frac{t_{hg} t_{fh}}{t_{hf}} \,\mathrm{tail}(f) \right) \\ &= \left(b_g \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \frac{t_{gh} t_{fg}}{t_{gf}} + b_h \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} \frac{t_{hg} t_{fh}}{t_{hf}} - dw \right) \mathrm{tail}(f) \\ &= 0.\end{aligned}$$

Hence we obtain a strong Gröbner representation

$$\text{gpoly}(g,\, h) = dwf - b_g \frac{t_{gh}}{t_g f}\,\text{spoly}(f,\, g) - b_h \frac{t_{hg}}{t_{hf}}\,\text{spoly}(f,\, h)$$

w.r.t. $\mathcal{G}$, because the leading term is given by $dw\text{LT}(f)$. □

Example 5.18. (cf. [6], Example 16)
Let $\mathcal{I} = \langle f_1 = 7x^2y^2 + 8xy^2 + 3xz - 11,\, f_2 = 11y^2z + 4x^2y + xyz^2 + 2,\, f_3 = 5x^2yz + x^2 + 2z^2 + 5z,\, f_4 = 7xyz + 3xy + 5x + 4y + 7\rangle \subseteq \mathbb{Z}[x,\, y,\, z]$ with graded lexicographical ordering $x \succ y \succ z$. A strong Gröbner basis for $\mathcal{I}$ is given by

$$\begin{aligned} G = \{&x - 1476098719963760109045215409621051259372 1,\\ &y - 6355322887725405337810105619887333184234,\\ &z + 1089845251315182396260633050875076267021 9,\\ &34475640417355562336236396270436281195926\}. \end{aligned}$$

When computing over fields one can achieve efficiency with lifting methods like Hensel lifting or the Chinese remainder theorem. We will address these methods in chapter 6, but it should be mentioned that lifting usually leads to a loss of information on coefficients. However, it can be useful to know about the existence of constants contained in the ideal or small polynomials, meaning small number of terms. We can use computations over quotient fields to find these elements.

Lemma 5.19.
Let $\mathcal{K} := \text{quot}(\mathcal{R})$ be the quotient field of $\mathcal{R}$. Let $\mathcal{I} = \langle f_1, \ldots, f_m\rangle \subseteq \mathcal{P}$ and $\tilde{\mathcal{I}} = \langle f_1, \ldots, f_m\rangle \subseteq \mathcal{K}[x_1, \ldots, x_n] =: \mathcal{K}[x]$ be the corresponding ideal generated over $\mathcal{K}[x]$. If $1 \in \tilde{\mathcal{I}}$ (i.e. $\{1\}$ is a Gröbner basis for $\tilde{\mathcal{I}}$ or in other words $\tilde{\mathcal{I}} = \mathcal{K}[x_1, \ldots, x_n]$), then $\mathcal{I} \cap \mathcal{R} \neq \{0\}$ (i.e. $\mathcal{I}$ contains a constant).

Proof.
Let $\pi : \mathcal{K}[x]^{m+1} \to \mathcal{K}[x]$ with $e_1 \mapsto f_1$, $e_m \mapsto f_m$ and $e_{m+1} \mapsto 1$. Since $1 \in \tilde{\mathcal{I}}$, there is an element α in the kernel of π with $\alpha = p_1e_1 + \ldots + p_me_m + e_{m+1}$ for some $p_i \in \mathcal{K}[x]$. Then $\pi(\alpha) = 0$ or equivalently $\pi(e_{m+1}) = -\sum_{i=1}^m p_i\pi(e_i)$. Let $c \in \mathcal{R}$ be a least common multiple of all denominators of all the coefficients occurring in the p_i. Then $cp_i \in \mathcal{P}$ and hence $c = c \cdot 1 = c\pi(e_{m+1}) = -\sum_{i=1}^m cp_i\pi(e_i) = -\sum_{i=1}^m cp_if_i \in \mathcal{I}$. □

Algorithm 5.20. (**Precheck for Constants**)
The following algorithm is based on the proof of Lemma 5.19 and returns an ideal equal to the original one, but given by a different generating set.

PreConst

input: $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subseteq \mathcal{P}$
output: $\mathcal{J} \subseteq \mathcal{P}$ ideal with $\mathcal{J} = \mathcal{I}$
01: compute a Gröbner basis $\mathcal{G}$ for $\langle f_1, \ldots, f_m \rangle \subseteq \mathcal{K}[x]$
02: **if** $1 \in \mathcal{G}$ **do**
03: compute $\mathcal{Z} = \mathrm{Syz}(\{f_1, \ldots, f_m, 1\}) \subseteq \mathcal{K}[x]^{m+1}$
04: choose $\alpha = p_1 e_1 + \ldots + p_m e_m + e_{m+1} \in \mathcal{Z}$
05: $c = \mathrm{lcm}(\{d \mid d \text{ is a denominator of a coefficient occurring in one of the } p_i\})$
06: $\mathcal{J} = \langle c, f_1, \ldots, f_m \rangle$
07: **end if**
08: **return** $\mathcal{J}$

If we find a Gröbner basis for the ideal over $\mathcal{K}$ that contains a monomial $x \in X$, then we can clearly replace 1 in the above proof by x. We construct the homomorphism π such that $e_{m+1} \mapsto x$.

Example 5.21. (cf. [1], Example 21)
Let $\mathcal{I} = \langle f_1 = x + 4, f_2 = xy + 9, f_3 = x - y + 8 \rangle \subseteq \mathbb{Z}[x, y]$ with the lexicographical ordering $x \succ y$. Then

$$f_4 := \mathrm{spoly}(f_1, f_2) = yf_1 - f_2 = 4y - 9,$$
$$f_5 := \mathrm{spoly}(f_1, f_3) = f_1 - f_2 = y - 4$$

and

$$\mathrm{spoly}(f_4, f_5) = f_4 - 4f_5 = 7.$$

On the other hand a consideration of the syzygy module $\mathrm{Syz}(\{f_1, f_2, f_3, 1\})$ over $\mathbb{Q}$ yields

$$(y - 4)f_1 - f_2 + 4f_3 - 7 = 0.$$

A strong reduced Gröbner basis for $\mathcal{I}$ is given by $\{x + 4, y - 4, 7\}$.

Lemma 5.22.
Let $f, g \in \mathcal{P} \setminus \{0\}$ with $\mathrm{LM}(f) = \mathrm{LM}(g)$. Then $\langle f, g \rangle = \langle \mathrm{spoly}(f, g), \mathrm{gpoly}(f, g) \rangle$.

Proof.
We write $\gcd(\mathrm{LC}(f), \mathrm{LC}(g)) = b_f \mathrm{LC}(f) + b_g \mathrm{LC}(g) =: d$. Then

$$\begin{aligned} \mathrm{spoly}(f, g) &= \frac{\mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g))}{\mathrm{LC}(f)} f - \frac{\mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g))}{\mathrm{LC}(g)} g \\ &= \frac{\mathrm{LC}(g)}{d} f - \frac{\mathrm{LC}(f)}{d} g \end{aligned}$$

and $\mathrm{gpoly}(f, g) = b_f f + b_g g$. By this we obtain a coefficient matrix

$$R = \begin{bmatrix} \mathrm{LC}(g)/d & -\mathrm{LC}(f)/d \\ b_f & b_g \end{bmatrix} \in \mathcal{R}^{2\times 2}$$

with $[\mathrm{spoly}(f, g), \mathrm{gpoly}(f, g)]^{\mathrm{tr}} = R[f, g]^{\mathrm{tr}}$. This shows the fact that $\langle f, g\rangle \supseteq \langle \mathrm{spoly}(f), \mathrm{gpoly}(g)\rangle$ (which is trivial). On the other hand note that

$$\det(R) = b_g \frac{\mathrm{LC}(g)}{d} - \left(-b_f \frac{\mathrm{LC}(f)}{d}\right) = \frac{b_f \mathrm{LC}(f) + b_g \mathrm{LC}(g)}{d} = \frac{d}{d} = 1$$

which shows that R is invertible and thus $R^{-1}[\mathrm{spoly}(f, g), \mathrm{gpoly}(f, g)]^{\mathrm{tr}} = [f, g]^{\mathrm{tr}}$, i.e. $\langle f, g\rangle \subseteq \langle \mathrm{spoly}(f), \mathrm{gpoly}(g)\rangle$. This completes the proof. □

This statement becomes irrelevant when $\mathrm{LC}(f) \mid \mathrm{LC}(g)$ or $\mathrm{LC}(g) \mid \mathrm{LC}(f)$, because then by Lemma 5.13 the G-polynomial of f and g reduces to zero w.r.t. $\{f, g\}$. If this is not the case, then we can go on and replace $g \in \mathcal{G}$ by $g' := \mathrm{gpoly}(f, g)$ to obtain a polynomial with the same leading monomial, but with a smaller leading coefficient in the Euclidean norm. This does not change the generated ideal since $\langle f, g\rangle = \langle f, g'\rangle$ by Lemma 5.22. We hereby increase the number of elements that are LM- or even LT-reducible by g, especially the G-polynomials that were already computed using g. Next we replace f with $\mathrm{spoly}(f, g')$ and continue with the regular procedure.

6 Commutative Gröbner bases over principal ideal rings

Let $\mathcal{P} = (\mathbb{Z}/m\mathbb{Z})[x_1, \ldots, x_n] = (\mathbb{Z}/m\mathbb{Z})[X]$. When m is prime, then the base ring is the finite field $\mathbb{F}_m$. When $m = 0$, then it is the Euclidean domain $\mathbb{Z}$. We covered these cases in the previous chapters. In any other case $\mathbb{Z}/m\mathbb{Z}$ is a finite principal ideal ring. Especially every element is either a unit or a zero divisor. To see this, let $\mathcal{S}$ be an arbitrary finite commutative ring and $r \in \mathcal{S}$ a non-zero-divisor. Then $\phi : \mathcal{S} \to \mathcal{S}$, $s \mapsto rs$ is injective. But, since injective maps from finite sets to themselves are bijective, there exists $s \in \mathcal{S}$ such that $rs = 1$, i.e. r is a unit.
Can we use our results for Euclidean domains and fields to compute over $\mathbb{Z}/m\mathbb{Z}$? Here is a naive approach. Let $\overline{\mathcal{I}} = \langle \overline{f_1}, \ldots, \overline{f_k} \rangle$ be an ideal of $(\mathbb{Z}/m\mathbb{Z})[X]$ and pick representatives $f_i \in \mathbb{Z}[X]$ of $\overline{f_i}$. Consider the ideal $\mathcal{I} = \langle f_1, \ldots, f_k, m \rangle$ of $\mathbb{Z}[x_1, \ldots, x_n]$ and compute a Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_l\}$ for $\mathcal{I}$. We mentioned the advantages of having a constant as an element of the Gröbner basis in Lemma 5.19. Consider the set of residue classes $\overline{\mathcal{G}} = \{\overline{g}_1, \ldots, \overline{g}_l\} \subseteq \mathcal{P}$ and let $\overline{f} \in \overline{\mathcal{I}} \setminus \{0\}$. Then there exist $\overline{p}_i \in (\mathbb{Z}/m\mathbb{Z})[X]$ such that $\overline{f} = \sum_i \overline{p}_i \overline{f}_i$. Hence

$$f - \sum_i p_i f_i \in \langle m \rangle \subseteq \mathbb{Z}[X]$$

is included in the ideal of $\mathbb{Z}[X]$ that is generated by m. So we see that $F := \{f_1, \ldots, f_k\} \cup \{m\}$ is indeed a generating set, such that $f \in \langle F \rangle = \mathcal{I}$. This is essential. If $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$, then there exists $g \in \mathcal{G}$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(f)$. Especially $\mathrm{LM}(g) = \mathrm{LM}(f)$ and $m \nmid \mathrm{LC}(g)$, because otherwise $m \mid \mathrm{LC}(f)$ which contradicts $\mathrm{LC}(\overline{f}) \neq 0$ in $\mathbb{Z}/m\mathbb{Z}$. Thus $\mathrm{LT}(\overline{g}) = \overline{\mathrm{LT}(g)}$ and, therefore, $\mathrm{LT}(\overline{g}) \mid \mathrm{LT}(\overline{f})$ in $(\mathbb{Z}/m\mathbb{Z})[X]$. Since $\overline{f}$ is arbitrary, we see that $\overline{\mathcal{G}}$ is indeed a strong Gröbner basis for $\overline{\mathcal{I}}$.
In theory this is all what is needed to compute Gröbner bases over $\mathbb{Z}/m\mathbb{Z}$. But we do not use any properties of the element m or the fact that the base ring is finite. It might be even more useful to turn the above method around, i.e. to compute a Gröbner basis over $\mathbb{Z}/m\mathbb{Z}$ and then lifting to $\mathbb{Z}$, which clearly should involve requirements for the leading coefficients in regards to m. For computational improvements we will attempt to find statements that use factorizations. Eder and Hofmann developed an algorithm in [3] for which we present the theoretical background in this chapter.

Example 6.1.
Let $\overline{f} = \overline{3}x + \overline{4} \in \mathbb{Z}/6\mathbb{Z}[x]$. Since we only have one generator, we cannot compute any S-polynomials, but, since $\overline{f} + \overline{f} = \overline{2} \in \langle \overline{f} \rangle$ and $\mathrm{LT}(\overline{f}) \nmid \mathrm{LT}(\overline{2})$, we see that $\{\overline{f}\}$ is not a Gröbner basis of $\langle \overline{f} \rangle$. However, the S-polynomial of $3x+4$ and 6 over $\mathbb{Z}[x]$ is 4 and indeed $\{\overline{f}, \overline{4}\}$ is a Gröbner basis for $\langle \overline{f} \rangle$.

From now on let $\mathcal{R}$ be a principal ideal domain and $\mathcal{P} = \mathcal{R}[X] = \mathcal{R}[x_1, \ldots, x_n]$. For $m \in \mathcal{R}$ we set $\overline{\mathcal{R}} := \mathcal{R}/m\mathcal{R}$ and $\overline{\mathcal{P}} = \overline{\mathcal{R}}[X]$. As we saw in the previous chapter, it was useful to introduce G-polynomials whose leading coefficient was (up to a unit) uniquely determined by the greatest common divisor and the other coefficients were determined by our choice of the Euclidean algorithm. Over principal ideal rings the greatest common divisor is

not uniquely determined. Also, as we have seen in the previous example, the leading coefficient could be a zero divisor. Therefore, we introduce a new type of polynomial.

Definition 6.2.
Let $f, g \in \overline{\mathcal{P}}$. S-polynomials and G-polynomials of f and g are defined similarly to Definition 5.5. Let $\mathrm{LC}(f)\overline{\mathcal{R}} \cap \mathrm{LC}(g)\overline{\mathcal{R}} = d\overline{\mathcal{R}}$. Then d is a least common multiple of $\mathrm{LC}(f)$ and $\mathrm{LC}(g)$. On the other hand a generator of $\mathrm{LC}(f)\overline{\mathcal{R}} + \mathrm{LC}(g)\overline{\mathcal{R}} =: c\overline{\mathcal{R}}$ is given by a greatest common divisor c of $\mathrm{LC}(f)$, $\mathrm{LC}(g)$. We fix $a_f, a_g, b_f, b_g \in \mathcal{R}$ such that $a_f\mathrm{LC}(f) = a_g\mathrm{LC}(g) = d$ and $b_f\mathrm{LC}(f) + b_g\mathrm{LC}(g) = c$. Furthermore, let $t = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ and $t_f = \dfrac{d}{\mathrm{LM}(f)}$, $t_g = \dfrac{d}{\mathrm{LM}(g)}$. Then an **S-polynomial** of f and g is defined as

$$\mathrm{spoly}(f, g) := a_f t_f f - a_g t_g g$$

and a **G-polynomial** of f and g is defined as

$$\mathrm{gpoly}(f, g) := b_f t_f f + b_g t_g g.$$

Let $\mathrm{ann}(\mathrm{LC}(f)) = a\overline{\mathcal{R}}$. Then an **A-polynomial** of f is defined as

$$\mathrm{apoly}(f) := af.$$

Since a annihilates $\mathrm{LC}(f)$, this is the tail of f multiplied with a, i.e. $\mathrm{apoly}(f) = a(f - \mathrm{LT}(f))$.

Clearly if $\mathrm{ann}(\mathrm{LC}(f)) = \{0\}$, then $\mathrm{apoly}(f) = 0$. But we also know that $\mathrm{LC}(f)$ is a unit and thus f can be normalized. As a consequence of Lemma 5.13 every G-polynomial of f reduces to zero.

Algorithm 6.3. (**Buchberger's algorithm for strong Gröbner bases over** $\overline{\mathcal{R}}[X]$)
The following procedure is analogous to Algorithm 5.11 and involves A-polynomials.

SBBA2

---

input: $\mathcal{I} = \langle f_1, \ldots, f_k \rangle \subseteq \overline{\mathcal{P}}$, NormalForm
output: strong Gröbner basis $\mathcal{G}$ for $\mathcal{I}$
01: $\mathcal{G} = \{f_1, \ldots, f_k\}$
02: $\mathcal{L} = \{\mathrm{spoly}(f_i, f_j), \mathrm{gpoly}(f_i, f_j)\}_{i<j}$
03: $\mathcal{L} = \mathcal{L} \cup \{\mathrm{apoly}(f_i)\}_i$
04: **while** $\mathcal{L} \neq \emptyset$ **do**
05: choose $h \in \mathcal{L}$
06: $\mathcal{L} = \mathcal{L} \setminus \{h\}$
07: $h = \mathrm{NormalForm}(h, \mathcal{G})$
08: **if** $h \neq 0$ **then**
09: $\mathcal{L} = \mathcal{L} \cup \{\mathrm{spoly}(g, h), \mathrm{gpoly}(g, h) \mid g \in \mathcal{G}\}$
10: $\mathcal{L} = \mathcal{L} \cup \{\mathrm{apoly}(h)\}$

11: $\mathcal{G} = \mathcal{G} \cup \{h\}$
12: **end if**
13: **end while**
14: **return** $\mathcal{G}$

The theoretical background for correctness and termination is given by our considerations at the start of the chapter and Theorem 5.4, Theorem 5.10. Note that if $\mathrm{LC}(f)$ is a non-trivial zero divisor, then there exists $r \in \mathcal{R}$, such that $\overline{r} = \mathrm{LC}(f)$ and $m \nmid r \mid m$. Let $ra = m$ for some $a \in \mathcal{R}$, such that $\overline{a}\overline{\mathcal{R}} = \mathrm{ann}(\mathrm{LC}(f))$. Let $f' \in \mathcal{P}$ be a representative with $\overline{f'} = f$. Then we compute the S-polynomial of f' and m over $\mathcal{R}$ and obtain

$$\mathrm{spoly}(f', m) = af' - \mathrm{LM}(f)m = a\,\mathrm{tail}(f').$$

Then $\overline{\mathrm{spoly}(f', m)} = \overline{a}\,\mathrm{tail}(f) = \mathrm{apoly}(f)$ is an A-polynomial of f.

If $\mathcal{R}$ is a principal ideal ring, which is not necessarily a domain, then we have the two following very useful theorems, that allow us to lift results of computations over the finite ring $\mathbb{Z}/m\mathbb{Z}$. This is in general not possible, because information of coefficients is lost when computing over fields. Therefore, the Chinese remainder theorem or Hensel lifting cannot be applied. Clearly we need further assumptions on the leading coefficients of the generating polynomials.

Theorem 6.4.
Let $m \in \mathcal{R}\backslash\{0\}$ and $\mathcal{I}$ an ideal of $\mathcal{P} = \mathcal{R}[X]$. Let $\mathcal{G} \subseteq \mathcal{P}$ such that $\pi(\mathcal{G})$ is a strong Gröbner basis of $\pi(\mathcal{I})$ where $\pi : \mathcal{P} = \mathcal{R}[X] \to \overline{\mathcal{P}} = (\mathcal{R}/m\mathcal{R})[X]$ is the canonical surjection. Additionally we assume that $m \nmid \mathrm{LC}(g) \mid m$ for every $g \in \mathcal{G}$ (this means that $\pi(\mathrm{LC}(g))$ is a non-trivial zero divisor in $\overline{\mathcal{R}}$). Then $\mathcal{G} \cup \{m\}$ is a strong Gröbner basis for $\mathcal{I} + m\mathcal{P}$.

Proof. (cf. [3], Theorem 10)
Clearly $\mathcal{G} \cup \{m\}$ is a subset of $\mathcal{I} + m\mathcal{P}$. Let $f \in \mathcal{I}$. If $\overline{f} := \pi(f) = 0$, then $m \mid \mathrm{LT}(f)$. So we may assume $\overline{f} \neq 0$ and $m \nmid \mathrm{LC}(f)$. Then $\mathrm{LM}(\overline{f}) = \mathrm{LM}(f)$ and there exists $g \in \mathcal{G}$ such that $\mathrm{LT}(\overline{g}) \mid \mathrm{LT}(\overline{f})$, because $\pi(\mathcal{G})$ is a Gröbner basis and we can find a term $h \in \mathcal{P}$ with $\overline{h}\mathrm{LT}(\overline{g}) = \mathrm{LT}(\overline{f})$. Thus $\mathrm{LM}(h)\mathrm{LM}(g) = \mathrm{LM}(f)$ and $\pi(h\mathrm{LT}(g) - \mathrm{LT}(f)) = 0$. Therefore, we have $h\mathrm{LT}(g) - \mathrm{LT}(f) = \lambda \mathrm{LM}(f)$ for some $\lambda \in m\mathcal{R}$ and hence $\mathrm{LT}(g) \mid \mathrm{LT}(f)$, because $\mathrm{LC}(g) \mid m$ by our additional assumption and $\mathrm{LM}(g) \mid \mathrm{LM}(f)$. In other words $\mathcal{G} \cup \{m\}$ is a strong Gröbner basis for $\mathcal{I} + m\mathcal{P}$. □

Remark 6.5.
We have the following implications for unitary commutative rings.

$$\text{field} \Rightarrow \text{Euclidean ring} \Rightarrow \text{PIR} \Rightarrow \text{factorial ring}$$

Especially every irreducible element in a principal ideal ring is prime and we have a unique prime factorization.

Theorem 6.6.
Let $\mathcal{I}$ be an ideal of $\mathcal{P}$ and a, b, r, $s \in \mathcal{R}$ such that $ab = 0$ and a, b coprime with $ar + bs = 1$. Let $\mathcal{G}_a$, $\mathcal{G}_b$ be Gröbner bases for $\mathcal{I} + a\mathcal{P}$, $\mathcal{I} + b\mathcal{P}$ respectively, such that for every $g_{a,i} \in \mathcal{G}_a \setminus \mathcal{R}$ we have $a \nmid \mathrm{LC}(g_{a,i}) \mid a$. Suppose, that the same holds for $\mathcal{G}_b$. For $g_{a,i} \in \mathcal{G}_a$ and $g_{b,j} \in \mathcal{G}_b$ we define

$$f_{i,j} := ar\mathrm{LC}(g_{a,i})\frac{\mathrm{lcm}(\mathrm{LM}(g_{a,i}),\, \mathrm{LM}(g_{b,j}))}{\mathrm{LM}(g_{b,j})}g_{b,j} + bs\mathrm{LC}(g_{b,j})\frac{\mathrm{lcm}(\mathrm{LM}(g_{a,i}),\, \mathrm{LM}(g_{b,j}))}{\mathrm{LM}(g_{a,i})}g_{a,i}.$$

Additionally we assume that $\mathrm{LC}(g_{a,i})\mathrm{LC}(g_{b,j}) \neq 0$ for all i, j. Then $\mathcal{G} := \{f_{i,j}\}_{i,j}$ is a strong Gröbner basis for $\mathcal{I}$.

Proof. (cf. [3], Theorem 12)
By our assumptions we have $\mathcal{I} = ar\mathcal{I} + bs\mathcal{I} = ar(\mathcal{I} + b\mathcal{P}) + bs(\mathcal{I} + a\mathcal{P}) = ar\langle\mathcal{G}_b\rangle + bs\langle\mathcal{G}_a\rangle$. Since a and b are coprime and $\mathrm{LC}(g_{a,i}) \mid a$, $\mathrm{LC}(g_{b,j}) \mid b$, we see that $\mathrm{LC}(g_{a,i})$ and $\mathrm{LC}(g_{b,j})$ are coprime as well. Furthermore, we have $\mathrm{LC}(g_{a,i})\mathrm{LC}(g_{b,j})\mathcal{R} = \mathrm{LC}(g_{a,i})\mathcal{R} \cap \mathrm{LC}(g_{b,j})\mathcal{R} \supsetneq a\mathcal{R} \cap b\mathcal{R} = \{0\}$ and thus $\mathrm{LT}(f_{i,j}) = \mathrm{lcm}(\mathrm{LM}(g_{a,i}), \mathrm{LM}(g_{b,j}))\mathrm{LC}(g_{a,i})\mathrm{LC}(g_{b,j})$. Now let $f \in \mathcal{I} \subseteq (\mathcal{I} + a\mathcal{P}) \cap (\mathcal{I} + b\mathcal{P})$. Then there exist $g_{a,i} \in \mathcal{G}_a$ and $g_{b,j} \in \mathcal{G}_b$, such that $\mathrm{LT}(g_{a,i}) \mid \mathrm{LT}(f)$ and $\mathrm{LT}(g_{b,j}) \mid \mathrm{LT}(f)$. Especially $\mathrm{lcm}(\mathrm{LM}(g_{a,i}), \mathrm{LM}(g_{b,j})) \mid \mathrm{LM}(f)$ and $\mathrm{LC}(g_{a,i})\mathrm{LC}(g_{a,i}) = \mathrm{lcm}(\mathrm{LC}(g_{a,i}), \mathrm{LC}(g_{b,j})) \mid \mathrm{LC}(f)$. Thus $\mathrm{LT}(f_{i,j}) \mid \mathrm{LT}(f)$ and $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$. □

Remark 6.7.
Theorem 6.4 and Theorem 6.6 hold over any principal ideal ring $\mathcal{R}$, but we are especially interested in the case $\mathcal{R} = \mathbb{Z}/m\mathbb{Z}$.

The point is that if we have $\mathcal{R} = \mathbb{Z}/m\mathbb{Z}$ in Theorem 6.6, then $ab = 0$ is equivalent to $m \mid a'b'$ for $\overline{a'} = a$, $\overline{b'} = b$. The consequence is the following corollary.

Corollary 6.8.
Let $\mathcal{I}$ be an ideal of $\overline{\mathcal{P}}$ with $m = ab$ such that a and b are coprime in $\mathcal{R}$. Then $m\mathcal{R} \cong a\mathcal{R} \cap b\mathcal{R}$ and we have canonical projections $\pi : \mathcal{R}[X] \to (\mathcal{R}/m\mathcal{R})[X]$, as well as

$$\pi_a : (\mathcal{R}/m\mathcal{R})[X] \cong (a\mathcal{R} + b\mathcal{R})/m\mathcal{R}[X] \to (\mathcal{R}/a\mathcal{R})[X]$$

and

$$\pi_b : (\mathcal{R}/m\mathcal{R})[X] \cong (a\mathcal{R} + b\mathcal{R})/m\mathcal{R}[X] \to (\mathcal{R}/b\mathcal{R})[X].$$

Assume that we have a finite set $\mathcal{G}_a \subseteq \overline{\mathcal{P}}$, such that $\pi(a) \in \mathcal{G}_a$, $\pi_a(\mathcal{G}_a)$ is a strong Gröbner basis for $\pi_a(\mathcal{I})$ and $\pi(a) \nmid \mathrm{LC}(g_{a,i}) \mid \pi(a)$ for all $g_{a,i} \in \mathcal{G}_a \setminus \{\pi(a)\}$. Let analogously $\mathcal{G}_b \subseteq \overline{\mathcal{P}}$, such that $\pi(b) \in \mathcal{G}_b$, $\pi_b(\mathcal{G}_b)$ is a strong Gröbner basis for $\pi_b(\mathcal{I})$ and $\pi(b) \nmid \mathrm{LC}(g_{b,j}) \mid \pi(b)$ for all $g_{b,j} \in \mathcal{G}_b \setminus \{\pi(b)\}$. We define $f_{i,j}$ similar to Theorem 6.6 over $\overline{\mathcal{P}}$ by

$$f_{i,j} := \pi(ar)\mathrm{LC}(g_{a,i})\frac{\mathrm{lcm}(\mathrm{LM}(g_{a,i}),\, \mathrm{LM}(g_{b,j}))}{\mathrm{LM}(g_{b,j})}g_{b,j} + \pi(bs)\mathrm{LC}(g_{b,j})\frac{\mathrm{lcm}(\mathrm{LM}(g_{a,i}),\, \mathrm{LM}(g_{b,j}))}{\mathrm{LM}(g_{a,i})}g_{a,i}.$$

Then $\mathcal{G} = \{f_{i,j}\}_{i,j}$ is a strong Gröbner basis for $\mathcal{I}$.

Proof.
First of all note that by the second isomorphism theorem we have

$$\overline{\mathcal{R}}/\overline{a}\overline{\mathcal{R}} = (\mathcal{R}/m\mathcal{R})/(\pi(a)(\mathcal{R}/m\mathcal{R})) \cong \mathcal{R}/a\mathcal{R}$$

and

$$\overline{\mathcal{R}}/\overline{b\mathcal{R}} = (\mathcal{R}/m\mathcal{R})/(\pi(b)(\mathcal{R}/m\mathcal{R})) \cong \mathcal{R}/b\mathcal{R}.$$

From this and Theorem 6.4 it follows that $\mathcal{G}_a \cup \{\overline{a}\} = \mathcal{G}_a$, $\mathcal{G}_b \cup \{\overline{b}\} = \mathcal{G}_b$ are strong Gröbner basis of $\mathcal{I} + \overline{a}\overline{\mathcal{P}}$, $\mathcal{I} + \overline{b\mathcal{P}}$ respectively. Then again using the isomorphism theorem all conditions of Theorem 6.6 are satisfied and it follows that $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$. □

Given such a factorization of m, we can improve Buchberger's algorithm with the following procedure.

Algorithm 6.9. (Mixing two Gröbner bases)
The following algorithm computes a strong Gröbner basis $\mathcal{G}$ as in Corollary 6.8, if the input sets $\mathcal{G}_a$, $\mathcal{G}_b$ satisfy the assumptions.

MIX

---

input: $\mathcal{G}_a = \{g_{a,1}, \ldots, g_{a,k}\} \subseteq (\mathcal{R}/m\mathcal{R})[X]$, $\mathcal{G}_b = \{g_{b,1}, \ldots, g_{b,l}\} \subseteq (\mathcal{R}/m\mathcal{R})[X]$ with $m = ab$, $\pi : \mathcal{P} \to \overline{\mathcal{P}}$
output: $\mathcal{G} \subseteq (\mathcal{R}/m\mathcal{R})[X]$
01: $\mathcal{G} = \emptyset$
02: **for** $1 \leq i \leq k$, $1 \leq j \leq l$ **do**
03: $$f_{i,j} := \pi(au)\mathrm{LC}(g_{a,i})\frac{\mathrm{lcm}(\mathrm{LM}(g_{a,i}), \mathrm{LM}(g_{b,j}))}{\mathrm{LM}(g_{b,j})}g_{b,j} + \pi(bv)\mathrm{LC}(g_{b,j})\frac{\mathrm{lcm}(\mathrm{LM}(g_{a,i}), \mathrm{LM}(g_{b,j}))}{\mathrm{LM}(g_{a,i})}g_{a,i}$$
04: $\mathcal{G} = \mathcal{G} \cup \{f_{i,j}\}$
05: **end do**
06: **return** $\mathcal{G}$

This is used iteratively in the following version of Buchberger's algorithm. We also use the fact that principal ideal rings are factorial.

Algorithm 6.10. (**Buchberger's algorithm for strong Gröbner bases over** $(\mathcal{R}/m\mathcal{R})[X]$ **with known prime factorization**)
We can apply Corollary 6.8 iteratively, when we have a prime factorization of m.

SBBA3

input: $\mathcal{I} = \langle f_1 (\mathrm{mod}\ m), \ldots, f_k (\mathrm{mod}\ m) \rangle \subseteq (\mathcal{R}/m\mathcal{R})[X]$, SBBA2, NormalForm
output: strong Gröbner basis $\mathcal{G}$ for $\mathcal{I}$
01: $m = p_1^{e_1} \cdots p_r^{e_r}$ prime factorization of m
02: **for** $1 \leq k \leq r$ **do**
03: $\quad \mathcal{I}_k = \langle f_1 (\mathrm{mod}\ p_k^{e_k}), \ldots, f_k (\mathrm{mod}\ p_k^{e_k}) \rangle \subseteq (\mathcal{R}/p_k^{e_k}\mathcal{R})[X]$
04: $\quad \mathcal{G}_k = \mathrm{SBBA2}(\mathcal{I}_k, \mathrm{NormalForm})$
05: **end do**
06: $\ell = 1$
07: **while** $1 \leq \ell \leq r-1$ **do**
08: $\quad \mathcal{G}_{\ell+1} = \mathrm{Mix}(\mathcal{G}_\ell, \mathcal{G}_{\ell+1})$
09: $\quad \ell = \ell + 1$
10: **end while**
11: **return** $\mathcal{G}_\ell$

The algorithm is correct, if the Gröbner bases $\mathcal{G}_k$ computed in line 04 only contain elements $g_{k,i}$ such that $p_k^{e_k} \nmid \mathrm{LC}(g_{k,i}) \mid p_k^{e_k}$. This holds by the definition of the canonical projection $\pi_i : (\mathcal{R}/m\mathcal{R})[X] \to (\mathcal{R}/p_k^{e_k}\mathcal{R})[X]$ and if we assume, that the leading coefficients of the elements in $\mathcal{I}$ are zero divisors. Additionally we need that the $p_i^{e_i}$ are coprime, when the p_i are coprime. Assume that $p_i^{e_i}$, $p_j^{e_j}$ have a non-trivial common divisor p. Then, since $\mathcal{R}$ is a unique factorization domain, there are ℓ_i, $\ell_j \in \mathbb{N}$, such that $p = p_i^{\ell_i} = p_j^{\ell_j}$. Then $p_i \mid p_j$ and $p_j \mid p_i$, because p_i, p_j are prime. Therefore we can find u, $v \in \mathcal{R}$, with $up_i = p_j$ and $vp_j = p_i$, i.e. $uvp_j = p_j$ or equivalently, because $\mathcal{R}$ is a domain and primes are not zero divisors, $uv = 1$. Thus p_i and p_j are associated and without loss of generality equal. Altogether we see that the $p_i^{e_i}$ are coprime. Then all assumptions of Corollary 6.8 are satisfied and we obtain a strong Gröbner basis for $\mathcal{I}$ iteratively.

If we are interested in a different factorization of m or cannot obtain a prime factorization, then we can still compute a Gröbner basis as follows.
Let $\mathcal{I} = \langle f_1 (\mathrm{mod}\ m), \ldots, f_k (\mathrm{mod}\ m) \rangle \subseteq (\mathcal{R}/m\mathcal{R})[X]$ be an ideal. We apply SBBA2 to $\mathcal{I}$ and stop at a non-invertible leading coefficient in $\mathcal{R}/m\mathcal{R}$. Then there exists $c \in \mathcal{R}$ such that $m \nmid c \mid m$ and $c (\mathrm{mod}\ m)$ is such a non-invertible leading coefficient of some $f_i (\mathrm{mod}\ m)$. If we can compute $d \in \mathcal{R}$ and $2 \leq \ell \in \mathbb{N}$, such that $m = d^\ell$ and $d \mid c$, then we continue with SBBA2. Otherwise, especially when m is squarefree, we can, according to [3], find a factorization $m = ab$ with a, b coprime. Then we compute Gröbner bases over $\mathcal{R}/a\mathcal{R}$, $\mathcal{R}/b\mathcal{R}$ with SBBA2 and obtain a Gröbner basis for $\mathcal{I}$ using Mix and Corollary 6.8.

SBBA4

input: $\mathcal{I} = \langle f_1 (\mathrm{mod}\ m), \ldots, f_k (\mathrm{mod}\ m) \rangle \subseteq (\mathcal{R}/m\mathcal{R})[x]$, SBBA2, NormalForm
output: strong Gröbner basis $\mathcal{G}$ for $\mathcal{I}$
01: apply SBBA2 to $\mathcal{I}$; stop at non-invertible leading coefficient in $\mathcal{R}/m\mathcal{R}$

02: **if** SBBA in step 1 does not stop **then**
03: $\mathcal{G} = \text{SBBA2}(\mathcal{I}, \text{NormalForm})$
04: **else**
05: choose $c \in \mathcal{R}$, such that $c \pmod m$ is a non-invertible leading coefficient
06: **if** $\exists\, d \in \mathcal{R}, l \in \mathbb{N} : m = d^l, d \mid c$ **then**
07: $\mathcal{G} = \text{SBBA2}(\mathcal{I}, \text{NormalForm})$
08: **else**
09: $m = ab$ for $a, b \in \mathcal{R}$ coprime
10: $\mathcal{I}_a = \langle f_1 \pmod a, \ldots, f_k \pmod a \rangle \subseteq (\mathcal{R}/a\mathcal{R})[X]$
11: $\mathcal{G}_a = \text{SBBA2}(\mathcal{I}_a, \text{NormalForm})$
12: $\mathcal{I}_b = \langle f_1 \pmod b, \ldots, f_k \pmod b \rangle \subseteq (\mathcal{R}/b\mathcal{R})[X]$
13: $\mathcal{G}_b = \text{SBBA2}(\mathcal{I}_b, \text{NF})$
14: $\mathcal{G} = \text{Mix}(\mathcal{G}_a, \mathcal{G}_b)$
15: **end if**
16: **end if**
17: **return** $\mathcal{G}$

Example 6.11. (cf. [6], Example 17)
Let $m = 5072012170009$ and $\mathcal{I} = \langle f_1 = -4984359602099 + x^2 - 3y2 - 9xz \pmod m, f_2 = -1780431462965 + 7xy + 5y^3 + z^2 \pmod m, f_3 = -4585397367278 + x^3 - 3y^2 + z - 12z^3 \pmod m \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})[x, y, z]$ with lexicographical ordering $x \prec y \prec z$. The prime factorization of m is given by $m = 541^2 \cdot 17329489$. Computing a Gröbner basis for $\mathcal{J} = \langle m, f_1, f_2, f_3 \rangle$ with SBBA yields

$$
\begin{aligned}
G = \{&5072012170009,\\
&1174872829454 + 12173501962z - 1363165624472z^2 + 1654998137452z^3\\
&+ 928181308002z^4 - 239795324199z^5 - 1646238538583z^6 - 982686930325z^7\\
&- 1734356432441z^8 - 1928316724538z^9 + 2384106829761z^{10} - 2266219400230z^{11}\\
&- 139245405743z^{12} + 895384068341z^{13} + 161928956428z^{14} + 2194204640034z^{15}\\
&- 1243172466690z^{16} - 1196909984892z^{17} + z^{18},\\
&2247545052503 + y + 788535951374z + 2214230166342z^2 + 955710141543z^3\\
&+ 2160238766386z^4 - 2474194692542z^5 - 1684716364278z^6 + 2157370757916z^7\\
&- 1072725791722z^8 + 1173330106507z^9 - 1057647942280z^{10} - 1511353993603z^{11}\\
&+ 1327624312048z^{12} - 581007814126z^{13} + 1772345363132z^{14} - 185000519654z^{15}\\
&- 1538648034589z^{16} - 456160565195z^{17},\\
&- 899617339822 + x + 2209081769554z - 509675450156z^2 + 566438534091z^3\\
&+ 1828943883971z^4 - 1778487828359z^5 - 1120529181700z^6 + 1238816552216z^7\\
&- 1898793743218z^8 + 1286010808749z^9 + 893019914153z^{10} + 172896055599z^{11}\\
&+ 1872411543380z^{12} + 1420313673322z^{13} - 880454763764z^{14} - 1202867057825z^{15}\\
&- 1977589465047z^{16} - 2210999439349z^{17}\}.
\end{aligned}
$$

Alternatively this basis modulo m (which simply deletes m from $\mathcal{G}$) can be computed over finite rings using the procedure Mix with $a = 541^2$, $b = 17329489$.

7 Non-commutative Gröbner bases over Euclidean domains

In this chapter we will consider non-commutative polynomials over Euclidean domains. Our main goal is to transfer properties from chapter 5. We are especially interested in a basic idea for an algorithm, finding or adjusting criteria for critical pairs and giving an effective method to implement Buchberger's algorithm in the computer algebra system SINGULAR [24]. The problem of applying the statements of the previous chapters for commutative Gröbner basis over Euclidean domains and principal ideal rings are divisibility conditions of type $\mathrm{LM}(f) \mid \mathrm{LM}(g)$. We start with the construction of S- and G-polynomials.
Let $\mathcal{R}$ be a Euclidean domain and X a free monoid. We define $\mathcal{P} = \mathcal{R}\langle X\rangle$ and $\mathcal{P}^e := \mathcal{P} \otimes_{\mathcal{R}} \mathcal{P}^{\mathrm{opp}}$. Then $\mathcal{P}$ is a left $\mathcal{P}^e$-module as we know from chapter 4. The relation $\sim$ is not needed, since X is free. Let $\preceq$ be a global monomial ordering on X.

Definition 7.1.
Let $x, y \in X$ be monomials. We say that x and y have an **overlap**, if there exist monomials $a_1, a_2 \in X$ such that at least one of the following cases holds.

1. $xa_1 = a_2y$
2. $a_1x = ya_2$
3. $a_1xa_2 = y$
4. $x = a_1ya_2$

Additionally we say that x and y have a **non-trivial overlap**, if in the first two cases $|a_1| < |y|$ and $|a_2| < |x|$ where $|\bullet|$ denotes the length of a word (the empty word 1 which is the unitary element of X has length zero). In the third, respectively fourth case, we say that x **divides** y, respectively y **divides** x. The set of all elements which are divisible by both x and y will be denoted by $\mathrm{cm}(x, y)$. The set of all minimal, non-trivial elements which are divisible by both x and y will be denoted by $\mathrm{lcm}(x, y)$, i.e. $t \in \mathrm{lcm}(x, y)$, if and only if there exist $\tau_x, \tau_y \in \mathcal{P}^e$ such that $t = \tau_x x = \tau_y y$, representing non-trivial overlaps of x and y, and if $t, \tilde{t} \in \mathrm{lcm}(x, y)$ with $\tilde{t} = \tau t$ for some $\tau \in \mathcal{P}^e$, then $t = \tilde{t}$ and $\tau = 1 \otimes 1$. If there are only trivial overlaps, then $\mathrm{lcm}(x, y) = \emptyset$.

Example 7.2.
Let X be the free monoid on the alphabet $\{a, b, c, d, e, f\}$.

1. $x = abcd$ and $y = bcde$ have non-trivial overlap in bcd (blue) and we have $a_1 = e$, $a_2 = a$:

a	b	c	d	
	b	c	d	e

2. $x = bcde$ and $y = abcd$ have non-trivial overlap bcd (blue) and we have $a_1 = a$, $a_2 = e$:

	b	c	d	e
a	b	c	d	

3. $x = bcd$ and $y = abcde$ have non-trivial overlap bcd (blue) and $a_1 = a$, $a_2 = e$:

	b	c	d	
a	b	c	d	e

4. $x = abcde$ and $y = bcd$ have non-trivial overlap bcd (blue) and we have $a_1 = a$, $a_2 = e$:

a	b	c	d	e
	b	c	d	

By the above definition $x = y$ have non-trivial overlap, in fact, the least trivial overlap there is, with $a_1 = a_2 = 1$. Two monomials can have more than one overlap, for example $x = abcdcd$ and $y = cdcdef$ have non-trivial overlaps in cd (blue) and $cdcd$ (red)

a	b	c	d	c	d				
				c	d	c	d	e	f

a	b	c	d	c	d		
		c	d	c	d	e	f

which are both contained in $\operatorname{lcm}(x, y)$.

We already defined reduction, Gröbner representations and Gröbner bases for non-commutative polynomial rings. Here are the "strong" versions for $\mathcal{R}\langle X\rangle$.

Definition 7.3.
Let $f, g \in \mathcal{P} \setminus \{0\}$, $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ be a countable set and $\mathcal{I} \subseteq \mathcal{P}$ be an ideal. The following definitions are w.r.t. $\preceq$.

- We say that g **LM-reduces** f, if $\operatorname{LM}(g)$ divides $\operatorname{LM}(f)$ with $\operatorname{LM}(f) = \tau\operatorname{LM}(g)$ for some $\tau \in \mathcal{P}^e$ and there are $a \neq 0$ and $b < \operatorname{LC}(f)$ (in the Euclidean norm) such that $\operatorname{LC}(f) = a\operatorname{LC}(g) + b$. Then the **LM-reduction** of f by g is given by

$$f - a\tau g.$$

- We say that f has a **strong Gröbner representation** w.r.t. $\mathcal{G}$, if $f = \sum_{i=1}^{m} h_i g_i$ with $m \in \mathbb{N}$, $g_i \in \mathcal{G}$, $h_i \in \mathcal{P}^e$ and there exists a unique $1 \leq j \leq m$ such that $\operatorname{LM}(f) = \operatorname{LM}(h_j g_j)$ and $\operatorname{LM}(f) \succ \operatorname{LM}(h_i g_i)$ for all $i \neq j$ with $h_i \neq 0$.

- $\mathcal{G}$ is called a **strong Gröbner basis** for $\mathcal{I}$, if $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}$ and for all $f' \in \mathcal{I} \setminus \{0\}$ there exists $g' \in \mathcal{G}$, such that $\operatorname{LT}(g')$ divides $\operatorname{LT}(f')$.

Definition 7.4.
Let $f, g \in \mathcal{P} \setminus \{0\}$. There exist monomial elements $\tau_f, \tau_g \in \mathcal{P}^e$ such that $\tau_f \mathrm{LM}(f) = \tau_g \mathrm{LM}(g) \in \mathrm{cm}(\mathrm{LM}(f), \mathrm{LM}(g))$. Let $a_f, a_g, b_f, b_g \in \mathcal{R}$ be defined as in 5.5. Then an **S-polynomial** of f and g is defined as

$$\mathrm{spoly}(f, g) := a_f \tau_f f - a_g \tau_g g$$

and a **G-polynomial** of f and g is defined as

$$\mathrm{gpoly}(f, g) := b_f \tau_f f + b_g \tau_g g.$$

Theorem 7.5.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $\{0\} \neq \mathcal{I} \subseteq \mathcal{P}$. The following are equivalent.

1. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$.
2. Every $f \in \mathcal{I} \setminus \{0\}$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.
3. Every $f \in \mathcal{P} \setminus \{0\}$ has a unique remainder after reduction by $\mathcal{G}$.

Proof.
The proof is analogous to Theorem 5.4 for the commutative case but with the replacement of h_i in "1. $\Rightarrow$ 2." by $h_i \in \mathcal{P}^e$ such that $\mathrm{LM}(h_i)\mathrm{LM}(g_i) = \mathrm{LM}(f_{i-1})$. Moreover, we replace $s_i \in \mathcal{P}$ by $\sigma_i \in \mathcal{P}^e$ for "3. $\Rightarrow$ 2." and, therefore, we go through this part again.
Let $f \in \mathcal{I}$ be reducing uniquely to zero w.r.t. $\mathcal{G}$. Thus we can write $f = \sum_i h_i g_i$ with $\max_{i,\preceq}\{\mathrm{LM}(h_i g_i)\} = t := \mathrm{LM}(f)$. This is a Gröbner representation and we need to show that $\mathrm{card}(\{i \mid \mathrm{LM}(h_i g_i) = t\}) = 1$. Suppose it is bigger than one. Since $\preceq$ and the Euclidean norm are well orderings, we can assume additionally that t is minimal among all monomials $\tilde{t}$ with the property $\mathrm{card}(\{i \mid \mathrm{LM}(h_i g_i) = \tilde{t}\}) > 1$ and $c := \mathrm{LC}(f)$ is minimal among all coefficients for which there is no strong Gröbner representation with leading monomial t. Also without loss of generality let $\{i \mid \mathrm{LM}(h_i g_i) = t\} = \{1, \ldots, k\}$ and $b = \sum_i \lambda_i \mathrm{LC}(g_i)$ the Bézout identity for the greatest common divisor of all leading coefficients which can be obtained from the extended Euclidean algorithm. Especially we have $b \mid c$, say $c = db$. Let $\sigma_i \in \mathcal{P}^e$ with $\sigma_i \mathrm{LM}(g_i) = t$ for $1 \leq i \leq k$ and $g = \sum_i \sigma_i \lambda_i g_i$. By this construction we have $\mathrm{LT}(g) = bt$. Suppose $b = c$. But since $|b| \leq |\mathrm{LC}(h_i g_i)| \leq |c|$ this implies $k = 1$, thus $|b| < |c|$. As c was chosen to be minimal there is a strong Gröbner representation of g, say $g = \sum_i \tilde{h}_i g_i$ with $\mathrm{LM}(\tilde{h}_j g_j) = t$. Since $c = db$ we have $\mathrm{LM}(f - dg) \prec t$ and, therefore, $(f - dg)$ has a strong Gröbner representation. In particular f has a strong Gröbner representation. □

So far everything seems to work out as in chapter 5. We consider some examples to see significant differences.

Example 7.6.
Let $f = 2xy$, $g = 3yz \in \mathbb{Z}\langle x, y, z\rangle$ where $X = \langle x, y, z\rangle$ is a free monoid. Usually we would compute an S-polynomial (which is zero) and a G-polynomial

$$\mathrm{gpoly}(f, g) := (-1) \cdot 2xy \cdot z + 1 \cdot x \cdot 3yz = xyz$$

and add them to $\{f, g\}$ to obtain a strong Gröbner basis for $\mathcal{I} = \langle f, g\rangle \subseteq \mathcal{P}$. But clearly

$$\text{gpoly}'(f, g) := (-1) \cdot 2xy \cdot w \cdot yz + 1 \cdot xy \cdot w \cdot 3yz = xywyz$$

is also a G-polynomial of f, g for every $w \in X$ and must be added to the basis. In other words there is no finite Gröbner basis for $\mathcal{I}$ and we have to be satisfied with computing up to a fixed maximal leading monomial. Note that in the first case we computed a G-polynomial in the canonical way by looking for a non-trivial overlap of xy and yz. In the case of gpoly$'$ we ignored this overlap. In the commutative case this is irrelevant, because then gpoly$(f, g) \mid$ gpoly$'(f, g)$. In the field case this is also irrelevant, because then LT$(f) \mid$ LT(gpoly$'(f, g)$). A similar problem occurs with S-polynomials. Let $f = 2xy + x$, $g = 3yz + z$. Then spoly$(f, g) = 3fz - 2xg = 3xz - 2xz = xz$ is an S-polynomial of f and g but so is

$$\text{spoly}'(f, g) := 3fwyz - 2xywg = 3xwyz - 2xywz$$

as well for any monomial $w \in X$. Now we can reduce spoly$'(f, g)$ with f and g to

$$(\text{spoly}'(f, g) - xwg) + fwz = -2xywz + fwz = xwz$$

which does not reduce any further w.r.t $\{f, g\}$ and also w.r.t. spoly$(f, g) = xz$ in general. Therefore, we have to add spoly$'(f, g)$ to the basis.
But this is not enough. For $f = 2xy + x$ we also see that

$$\text{spoly}'(f, f) := fwxy - xywf = xwxy - xywx \neq 0$$

is an S-polynomial of f with itself and does not reduce any further, because the leading coefficient of f is not a unit and we need $\text{LM}(f)w\text{LM}(f) \in \text{cm}(\text{LM}(f), \text{LM}(f))$, although it is clearly not contained in lcm(LM(f), LM(f)). So even principal ideals do not have finite strong Gröbner bases in general. This case of S-polynomials does not occur over fields as well and is completely new for non-commutative polynomials over $\mathcal{R}$.
Also note that we do not consider any further extensions of the leading monomials, meaning that the S- and G-polynomial where we construct $\text{LM}(f)w\text{LM}(g)$ make any further overlaps $a\text{LM}(f)w\text{LM}(g)b$ for $a, b \in X$ redundant. Therefore, in the definition of lcm(x, y) we attached importance to the minimality which is of course motivated by the definition of a least common multiple in the commutative case.

The previous example shows that we have to consider all possible S- and G-polynomials which are infinitely many. Moreover, the set cm(LM(f), LM(g)) contains too many elements that are redundant whereas the set lcm(LM(f), LM(g)) is too small for overlap relations of leading monomials. The following definition is made to distinguish two types of S- and G-polynomials.

Definition 7.7.
Let $f, g \in \mathcal{P} \setminus \{0\}$ and a_f, a_g, b_f, b_g as in Definition 5.5. We consider the following cases.

1. If $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ have a non-trivial overlap, then there exist $t \in \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ and $\tau_f, \tau_g \in \mathcal{P}^e$, such that $t = \tau_f \mathrm{LM}(f) = \tau_g \mathrm{LM}(g)$. Furthermore, we require that $\tau_f = 1 \otimes t_f$, $\tau_g = t_g \otimes 1$ or $\tau_f = 1 \otimes 1$, $\tau_g = t_g \otimes t'_g$ for monomials $t_f, t_g, t'_g \in X$ with $|t_f| < |\mathrm{LM}(g)|$, $|t_g|, |t'_g| < |\mathrm{LM}(f)|$. We define a **first type S-polynomial** of f and g w.r.t. t as

$$\mathrm{spoly}_1^t(f, g) := a_f \tau_f f - a_g \tau_g g$$

and a **first type G-polynomial** of f and g w.r.t. t as

$$\mathrm{gpoly}_1^t(f, g) := b_f \tau_f f + b_g \tau_g g.$$

If such t_f, t_g do not exist then we set $\mathrm{spoly}_1^t(f, g) := \mathrm{gpoly}_1^t(f, g) := 0$. Since two monomials may have several non-trivial overlaps, these t_f, t_g, t'_g are not unique. To be more precise, this results from $\mathcal{P}$ not being a unique factorization domain.

2. For any $w \in X$ we define the **second type S-polynomial** of f and g w.r.t. w by

$$\mathrm{spoly}_2^w(f, g) := a_f f w \mathrm{LM}(g) - a_g \mathrm{LM}(f) w g$$

and the **second type G-polynomial** of f and g w.r.t. w as

$$\mathrm{gpoly}_2^w(f, g) := b_f f w \mathrm{LM}(g) + b_g \mathrm{LM}(f) w g.$$

Remark 7.8.
Clearly, it only makes sense to consider first type S- and G-polynomials if there is a non-trivial overlap of the leading monomials. However, as Example 7.6 shows we always need to consider second type S- and G-polynomials. For any $w \in X$ we have $\mathrm{LM}(f)w\mathrm{LM}(g) \in \mathrm{cm}(\mathrm{LM}(f), \mathrm{LM}(g))$ and $\mathrm{LM}(g)w\mathrm{LM}(f) \in \mathrm{cm}(\mathrm{LM}(f), \mathrm{LM}(g))$, which are distinct in general. Therefore, we need to consider both $\mathrm{spoly}_2^w(f, g)$ and $\mathrm{spoly}_2^w(g, f)$ and the same holds for second type G-polynomials. Also note that the set of first type S- and G-polynomials is finite, because our monomial ordering is a well ordering, whereas the set of second type S- and G-polynomials is infinite, at least on the free monoid. Therefore, we need to fix an upper bound for computations.
It is also important to point out that the elements τ_f, τ_g are not uniquely determined. Take for example $f = 2xyx + y$, $g = 3x + 1$. Then $t := \mathrm{LM}(f) = xy\mathrm{LM}(g)$ but also $t = \mathrm{LM}(g)yx$ and thus $\mathrm{spoly}_1^t(f, g) = -3f + 2gyx = 2yx - 3y$ and $(\mathrm{spoly}_1^t)'(f, g) = -3f + 2xyg = 2xy - 3y$ are both first type S-polynomials with different leading monomials.

In the following we will recall the criteria for critical pairs from chapter 5 and see which can be applied over $\mathcal{R}\langle X \rangle$ and which can not.

Remark 7.9.
First of all we should consider the case where $t := \mathrm{LM}(f)$ is divisible by (or is even equal to) $\mathrm{LM}(g)$. Then $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ contains exactly one element, namely t, because it is the only minimal element that is divisible by both leading monomials. Therefore, $\mathrm{spoly}_1^t(f, g)$ and $\mathrm{gpoly}_1^t(f, g)$ are the only first type S- and G-polynomials. However, these are not uniquely determined, we might have more overlap relations of $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ and we still need second type S-polynomials.

Remark 7.10.
Lemma 5.13 can be applied to both first and second type G-polynomials. Recall that $\mathrm{gpoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$ in the commutative case if $\mathrm{LC}(f) \mid \mathrm{LC}(g)$. In the non-commutative case we also see that since $b_f = 1$, $b_g = 0$ we have that $\mathrm{gpoly}_1^t(f, g) = \tau_f f$ and $\mathrm{gpoly}_2^w(f, g) = fw\mathrm{LM}(g)$ reduce to zero w.r.t f for any $t \in \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ and $w \in X$.

Remark 7.11.
Lemma 5.14 is expected to be applicable to second type S-polynomials. Recall that in the commutative case $\mathrm{spoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$ if $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ are coprime and $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ are coprime. Now let $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ be coprime and $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ have only trivial overlaps. Then for any $w \in X$ we have

$$\begin{aligned}\mathrm{spoly}_2^w(f, g) &= \mathrm{LC}(g)fw\mathrm{LM}(g) - \mathrm{LC}(f)\mathrm{LM}(f)wg \\ &= fw(g - \mathrm{tail}(g))wf - (f - \mathrm{tail}(f))wg \\ &= \mathrm{tail}(f)wg - fw\,\mathrm{tail}(g).\end{aligned}$$

Now we write $r := \mathrm{tail}(f)$, $s := \mathrm{tail}(g)$ and suppose that we have cancellation of leading terms, i.e.

$$\mathrm{LM}(rwg) = \mathrm{LM}(r)w\mathrm{LM}(g) = \mathrm{LM}(f)w\mathrm{LM}(s) = \mathrm{LM}(fws).$$

$\mathrm{LM}(r)$	w	$\mathrm{LM}(g)$
$\mathrm{LM}(f)$	w	$\mathrm{LM}(s)$

By definition we have that $\mathrm{LM}(f) \succ \mathrm{LM}(r)$ and thus $|\mathrm{LM}(f)| > |\mathrm{LM}(r)|$ for global monomial orderings, since in the above case $\mathrm{LM}(r)$ divides $\mathrm{LM}(f)$ from the left. Moreover, we require that $\ell_f := |\mathrm{LM}(f)| - |\mathrm{LM}(r)| = |\mathrm{LM}(g)| - |\mathrm{LM}(s)| =: \ell_g$ and thus with $\ell := \ell_f = \ell_g$, if $|w| < \ell$ then we would have a non-trivial overlap, a contradiction. Thus $\mathrm{spoly}_2^w(f, g)$ only reduces not to zero if ℓ is well-defined, $|w| \geq \ell$, w has non-canonical self-overlap of length $|w| - \ell$, there exist monomials $x, y \in X$, such that $|x| = |y|$, $\mathrm{LM}(r)x = \mathrm{LM}(f)$, $\mathrm{LM}(g) = y\mathrm{LM}(f)$ and $\mathrm{LC}(rg) = \mathrm{LC}(fs)$. Furthermore, the latter demands that $\mathrm{LC}(f) \mid \mathrm{LC}(r)$ and $\mathrm{LC}(g) \mid \mathrm{LC}(s)$, because $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ are coprime.

Example 7.12.
Let $f = 2xyz + 4xy + 1$, $g = 3zxy + 6xy$ and $w = 1$. We choose the graded left lexicographical ordering. Then $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ are coprime and thus

$$\mathrm{spoly}_2^1(f, g) = 3zxy,$$

which LM-reduces to $6xy \neq 0$ w.r.t. g and can not be any further LM-reduced w.r.t. $\{f, g\}$. So if $|w| < \ell_f = \ell_g$, we need that $\mathrm{LM}(f), \mathrm{LM}(g)$ have no overlap. Now take $w = z$. Then $|w| = \ell_f = \ell_g = 1$ and

$$\mathrm{spoly}_2^z(f, g) = 3zzxy,$$

which LM reduces to $12xy \neq 0$ w.r.t g and can not be any further LM-reduced w.r.t. $\{f, g\}$. However, it reduces to zero w.r.t. $\mathrm{spoly}_2^1(f, g)$.

We consider further situation where we might find applications for criteria.

Example 7.13.
If $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ do not overlap and the leading coefficients are not coprime, i.e. $\mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g)) \neq 1$, then we can make no statement about reduction. This only applies to second type S- and G-polynomials. Take for example $f = 4xy + x$, $g = 6zy + z \in \mathbb{Z}\langle X\rangle = \mathbb{Z}\langle x, y, z\rangle$ in the graded left lexicographical ordering with $x \succ y \succ z$. Then $\mathrm{spoly}_2^1(f, g) = 3fzy - 2xyg = 3xzy - 2xyz$ and $\mathrm{gpoly}_2^1(f, g) = (-1)fzy + 1xyg = 2xyzy + xyz - xzy$ both do not reduce any further and thus must be added to the Gröbner basis just as any other second type S- and G-polynomial.

Example 7.14.
Also for first type S- and G-polynomials there can be no statement made if the leading coefficients are not coprime. For example in the case of $f = 4xy + y$, $g = 6yz + y$ we have $\mathrm{spoly}_1^{xyz}(f, g) = 3fz - 2xg = 3yz - 2xy$ and $\mathrm{gpoly}_1^{xyz}(f, g) = (-1)fz + 1xg = 2xyz - yz + xy$ which do not reduce any further.

Remark 7.15.
A special case occurs if one of the polynomials is normalized. Then according to Remark 7.10 every G-polynomial reduces to zero, but by Remark 7.11 not every second type S-polynomial must reduce to zero.

Remark 7.16.
We can also use Lemma 5.22. Recall that the pair $\{f, g\}$ can be replaced in the commutative case by $\{\mathrm{spoly}(f, g), \mathrm{gpoly}(f, g)\}$ if $t = \mathrm{LM}(f) = \mathrm{LM}(g)$. Now if $\mathrm{LM}(f) = \mathrm{LM}(g)$ then in the definition of first type S- and G-polynomials we have $\tau_f = \tau_g = 1 \otimes 1$ and, therefore, $\mathrm{spoly}_1^t(f, g) = a_f f - a_g g$ and $\mathrm{gpoly}_1^t(f, g) = b_f f + b_g g$. The rest of the proof is analogous to Lemma 5.22, because the hereby constructed matrix is an invertible $\mathcal{R}$-matrix.

Remark 7.17.
What about the chain criterion for S-polynomials? Essential for the proof of Lemma 5.16 was Remark 5.15. For a, b, $c \in \mathcal{P}$ monomials let a divide $t \in \mathrm{cm}(b, c)$. Then there exists $\delta \in \mathcal{P}^e$ with $\delta a = t$ and especially a and b divide $\mathrm{lcm}(b, c)$. We have to consider two cases. If a and b have non-trivial overlap then t is divisible by some $s \in \mathrm{cm}(a, b)$. Therefore, the chain criterion can only be applied to first type S-polynomials in this case. If on the other hand a and b only have trivial overlap then there exists a unique monomial $w \in \mathcal{P}$ and $\tau \in \mathcal{P}^e$ with $\tau awb = t$ or $\tau bwa = t$. Thus in the second case the chain criterion can only be applied to second type S-polynomials w.r.t. w. This covers the conditions for the following.
Now let $\mathcal{G} \subseteq \mathcal{P}$ and f, g, $h \in \mathcal{G}$. For a, $b \in \{f, g, h\}$ we fix $T_{ab} \in \mathrm{lcm}(\mathrm{LM}(a), \mathrm{LM}(b))$ and choose $\tau_{ab} \in \mathcal{P}^e$ with $\tau_{ab}\mathrm{LM}(a) = T_{ab}$. There exists $\tau_{ba} \in \mathcal{P}^e$ such that $\tau_{ba}\mathrm{LM}(b) = T_{ab}$, i.e. we need $T_{ab} = T_{ba}$. Furthermore, let

1. $T_{hg} = T_{gh}$ overlap both T_{hf} and T_{gf} with $\delta_{gf}T_{hf} = T_{hg}$ and $\delta_{hf}T_{gf} = T_{gh}$ for some δ_{gf}, $\delta_{hf} \in \mathcal{P}^e$,
2. $\mathrm{LC}(f) \mid \mathrm{lcm}(\mathrm{LC}(g), \mathrm{LC}(g))$ and
3. $\mathrm{spoly}_1^{T_{fg}}(f, g)$ and $\mathrm{spoly}_1^{T_{fh}}(f, h)$ have strong Gröbner representations w.r.t. $\mathcal{G}$.

Then with c_{ab} as in the proof of Lemma 5.16 we have

$$\begin{aligned}
&\frac{c_{hg}}{c_{hf}}\delta_{gf}\,\mathrm{spoly}_1^{T_{fh}}(f, h) - \frac{c_{gh}}{c_{gf}}\delta_{hf}\,\mathrm{spoly}_1^{T_{fg}}(f, g)\\
=&\frac{c_{hg}}{c_{hf}}\delta_{gf}(c_{fh}\tau_{fh}f - c_{hf}\tau_{hf}h) - \frac{c_{gh}}{c_{gf}}\delta_{hf}(c_{fg}\tau_{fg}f - c_{gf}\tau_{gf}g)\\
=&c_{gh}\delta_{hf}\tau_{gf}g - c_{hg}\delta_{gf}\tau_{hf}h + \left(\frac{c_{hg}c_{fh}}{c_{hf}}\delta_{gf}\tau_{fh} - \frac{c_{gh}c_{fg}}{c_{gf}}\delta_{hf}\tau_{fg}\right)f
\end{aligned}$$

and with $\tau_{hg}\mathrm{LM}(h) = T_{hg} = \delta_{gf}T_{hf} = \delta_{gf}\tau_{hf}\mathrm{LM}(h)$ we have $\delta_{gf}\tau_{hf} = \tau_{hg}$ in $\mathcal{P}^e$. Analogously $\delta_{hf}\tau_{gf} = \tau_{gh}$ and thus the first term equals $\mathrm{spoly}_1^{T_{gh}}(g, h)$. Moreover, we already know from the proof of Lemma 5.16 that

$$\frac{c_{hg}c_{fh}}{c_{hf}} = \frac{c_{gh}c_{fg}}{c_{gf}}.$$

Finally

$$\delta_{gf}\tau_{fh}\mathrm{LM}(f) = \delta_{gf}T_{fh} = \delta_{gf}T_{hf} = T_{hg} = T_{gh} = \delta_{hf}T_{gf} = \delta_{hf}T_{fg} = \delta_{hf}\tau_{fg}\mathrm{LM}(f)$$

implies $\delta_{gf}\tau_{fh} = \delta_{hf}\tau_{fg}$ in $\mathcal{P}^e$ and, therefore,

$$\frac{c_{hg}}{c_{hf}}\delta_{gf}\,\mathrm{spoly}_1^{T_{fh}}(f, h) - \frac{c_{gh}}{c_{gf}}\delta_{hf}\,\mathrm{spoly}_1^{T_{fg}}(f, g) = \mathrm{spoly}_1^{T_{gh}}(g, h)$$

which shows that $\mathrm{spoly}_1^{T_{gh}}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$. Clearly this also works for second type S-polynomials $\mathrm{spoly}_2^{w}(g, h)$ or $\mathrm{spoly}_2^{\tilde{w}}(h, g)$ if we choose w or $\tilde{w}$ such that $\mathrm{LM}(g)w\mathrm{LM}(h) = T_{gh}$ or $\mathrm{LM}(h)\tilde{w}\mathrm{LM}(g) = T_{hg}$.

Remark 7.18.
We have a similar criterion for G-polynomials. Let $\mathcal{G} \subseteq \mathcal{P}$ and f, g, $h \in \mathcal{G}$. We use the above notation and assumptions for T_{ab} and τ_{ab}. Let

1. $T_{hg} = T_{gh}$ overlap both T_{hf} and T_{gf} with $\delta_{gf} T_{hf} = T_{hg}$ and $\delta_{hf} T_{gf} = T_{gh}$ for some δ_{gf}, $\delta_{hf} \in \mathcal{P}^e$ and

2. $\mathrm{LC}(f) \mid \gcd(\mathrm{LC}(g), \mathrm{LC}(g))$ with $d := \dfrac{\gcd(\mathrm{LC}(g), \mathrm{LC}(g))}{\mathrm{LC}(f)}$.

We will show that $\mathrm{gpoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$. First of all note that

$$\begin{aligned}
\mathrm{gpoly}(g, h) &= b_g \tau_{gh} g + b_h \tau_{hg} h = \gcd(\mathrm{LC}(g), \mathrm{LC}(h)) T_{gh} + b_g \tau_{gh} \,\mathrm{tail}(g) + b_h \tau_{hg} \,\mathrm{tail}(h), \\
\mathrm{spoly}(f, g) &= \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \tau_{fg} f - \tau_{gf} g = \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \tau_{fg} \,\mathrm{tail}(f) - \tau_{gf} \,\mathrm{tail}(g) \quad \text{and} \\
\mathrm{spoly}(f, h) &= \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} \tau_{fh} f - \tau_{hf} h = \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} \tau_{fh} \,\mathrm{tail}(f) - \tau_{hf} \,\mathrm{tail}(h).
\end{aligned}$$

Since T_{fh} divides T_{gh} there exists $w \in \mathcal{P}^e$ with $w\mathrm{LM}(f) = T_{gh}$. Then

$$w\mathrm{LM}(f) = T_{gh} = \delta_{gf} T_{fh} = \delta_{gf} T_{fh} \mathrm{LM}(f).$$

Hence $w = \delta_{gf} \tau_{fh}$ and analogously $w = \delta_{hf} \tau_{fg}$.
Moreover, $dw\mathrm{LC}(f)\mathrm{LM}(f) = \gcd(\mathrm{LC}(g), \mathrm{LC}(h)) T_{gh}$ and finally we obtain

$$\begin{aligned}
&\mathrm{gpoly}(g, h) - dwf + b_g \delta_{hf} \,\mathrm{spoly}(f, g) + b_h \delta_{gf} \,\mathrm{spoly}(f, h) \\
&= \gcd(\mathrm{LC}(g), \mathrm{LC}(h)) T_{gh} + b_g \tau_{gh} \,\mathrm{tail}(g) + b_h \tau_{hg} \,\mathrm{tail}(h) \\
&\quad - (\gcd(\mathrm{LC}(g), \mathrm{LC}(h)) T_{gh} + dw \,\mathrm{tail}(f)) \\
&\quad + b_g \delta_{hf} \left(\frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \tau_{fg} \,\mathrm{tail}(f) - \tau_{gf} \,\mathrm{tail}(g) \right) \\
&\quad + b_h \delta_{gf} \left(\frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} \tau_{fh} \,\mathrm{tail}(f) - \tau_{hf} \,\mathrm{tail}(h) \right) \\
&= b_g \tau_{gh} \,\mathrm{tail}(g) + b_h \tau_{hg} \,\mathrm{tail}(h) - dw \,\mathrm{tail}(f) \\
&\quad + b_g \frac{\mathrm{LC}(g)}{\mathrm{LC}(f)} \delta_{hf} \tau_{fg} \,\mathrm{tail}(f) - b_g \underbrace{\delta_{hf} \tau_{gf}}_{=\tau_{gh}} \,\mathrm{tail}(g) \\
&\quad + b_h \frac{\mathrm{LC}(h)}{\mathrm{LC}(f)} \underbrace{\delta_{gf} \tau_{fh}}_{=\delta_{hf} \tau_{fg}} \,\mathrm{tail}(f) - b_h \underbrace{\delta_{gf} \tau_{hf}}_{=\tau_{hg}} \,\mathrm{tail}(h) \\
&= \left(\frac{b_g \mathrm{LC}(g) + \mathrm{LC}(h)}{\mathrm{LC}(f)} \delta_{hf} \tau_{fg} - dw \right) \mathrm{tail}(f) \\
&= d(\delta_{hf} \tau_{fg} - w) \,\mathrm{tail}(f) \\
&= 0.
\end{aligned}$$

Thus

$$\text{gpoly}(g,\, h) = dwf - b_g \delta_{hf}\, \text{spoly}(f,\, g) - b_h \delta_{gf}\, \text{spoly}(f,\, h)$$

is a strong Gröbner representation of $\text{gpoly}(g,\, h)$.

We conclude that the criteria for S- and G-polynomials from chapter 5 can also be applied in the non-commutative case with modifications, if we distinguish between first and second type S- and G-polynomials. The chain criteria require adjusted conditions to apply Remark 5.15. Computations will show how hard these requirements are to be fulfilled compared to the commutative case.
The following strong normal form algorithm uses LM-reductions similar to Algorithm 5.9 but now for non-commutative polynomials and can be compared to the algorithm "NF" in [4], pp. 4–5.

Algorithm 7.19. (**Normal form algorithm over** $\mathcal{R}\langle X\rangle$)
We redefine the normal form algorithm from chapter 5 to work over non-commutative polynomial rings.

NormalForm

---

input: $f \in \mathcal{P}$, $\mathcal{G} \subseteq \mathcal{G}$ finite and partially ordered
output: normal form of f w.r.t. $\mathcal{G}$
01: $h = f$
02: **while** $h \neq 0$ **and** $\mathcal{G}_h = \{g \in \mathcal{G} \mid g \text{ LM-reduces } h\} \neq \emptyset$ **do**
03: choose $g \in \mathcal{G}_h$
04: choose $a \in \mathcal{R} \setminus \{0\}$, $b \in \mathcal{R}$ with $\text{LC}(h) = a\text{LC}(g) + b$ and $|b| < |\text{LC}(h)|$
05: choose $\tau \in \mathcal{P}^e$ with $\text{LM}(h) = \tau\text{LM}(g)$
06: $h = h - a\tau g$ LM-reduction of h by g
07: **end while**
08: **return** h

Termination and Correctness is analogous to the commutative case of strong normal forms.

A finite set $\mathcal{G} \subseteq \mathcal{P}$ is called **degree-bounded strong Gröbner basis** for an ideal $\mathcal{I}$, if there is a Gröbner basis $\mathcal{G}'$ for $\mathcal{I}$ such that $\mathcal{G} \subseteq \mathcal{G}'$ contains precisely the elements of $\mathcal{G}'$ with degree smaller or equal to d for some $d \in \mathbb{N}$.

Algorithm 7.20. (**Buchberger's algorithm for degree-bounded strong Gröbner bases over $\mathcal{R}\langle X\rangle$**)
The following algorithm computes a degree-bounded strong Gröbner basis for an input ideal.

SBBA

---

input: $\mathcal{I} = \langle f_1, \ldots, f_k\rangle \subseteq \mathcal{R}\langle X\rangle$, $d \in \mathbb{N}$, NORMALFORM
output: bounded strong Gröbner basis $\mathcal{G}$ for $\mathcal{I}$
01: $\mathcal{G} = \{f_1, \ldots, f_k\}$
02: $\mathcal{L} = \emptyset$
03: **for** $1 \leq i \leq j \leq k$ **do**
04: compute lcm(LM(f_i), LM(f_j))
05: **for** $t \in$ lcm(LM(f_i), LM(f_j)) with $|t| \leq d$ **do**
06: $\mathcal{L} = \mathcal{L} \cup \{\text{spoly}_1^t(f_i, f_j), \text{gpoly}_1^t(f_i, f_j)\}$
$\cup \{\text{spoly}_1^t(f_j, f_i), \text{gpoly}_1^t(f_j, f_i)\}$
07: **end do**
08: **for** $w \in X$ with $\deg(f_i w f_j) \leq d$ **do**
09: $\mathcal{L} = \mathcal{L} \cup \{\text{spoly}_2^w(f_i, f_j), \text{gpoly}_2^w(f_i, f_j)\}$
$\cup \{\text{spoly}_2^w(f_j, f_i), \text{gpoly}_2^w(f_j, f_i)\}$
10: **end do**
11: **end do**
12: **while** $\mathcal{L} \neq \emptyset$ **do**
13: choose $h \in \mathcal{L}$
14: $\mathcal{L} = \mathcal{L} \setminus \{h\}$
15: $h =$ NORMALFORM(h, $\mathcal{G}$)
16: **if** $h \neq 0$ **then**
17: $\mathcal{G} = \mathcal{G} \cup \{h\}$
18: **for** $g \in \mathcal{G}$ **do**
19: compute lcm(LM(g), LM(h))
20: **for** $t \in$ lcm(LM(g), LM(h)) with $|t| \leq d$ **do**
21: $\mathcal{L} = \mathcal{L} \cup \{\text{spoly}_1^t(g, h), \text{gpoly}_1^t(g, h)\}$
$\cup \{\text{spoly}_1^t(h, g), \text{gpoly}_1^t(h, g)\}$
22: **end do**
23: **for** $w \in X$ with $\deg(gwh) \leq d$ **do**
24: $\mathcal{L} = \mathcal{L} \cup \{\text{spoly}_2^w(g, h), \text{gpoly}_2^w(g, h)\}$
$\cup \{\text{spoly}_2^w(h, g), \text{gpoly}_2^w(h, g)\}$
25: **end do**
26: **end do**
27: **end if**
28: **end while**
29: **return** $\mathcal{G}$

Compared to Algorithm 5.11 there are two significant changes. For each pair we must consider multiple S- and G-polynomials. We do this with for-loops in lines 05, 08, 20

and 23. Secondly we compute S-polynomials of polynomials with themselves. Therefore, we have $i \leq j$ in line 03 and we add h to $\mathcal{G}$ in line 17 before computing the S- and G-polynomials. Note that G-polynomials of elements with themselves are always redundant and, therefore, must not be added. We overlooked this in the above algorithm for readability. It should also be mentioned that the algorithm computes a Gröbner basis for $\mathcal{I}$ if the monomials w in lines 08 and 23 are chosen freely without an upper bound. Of course then the procedure does not terminate.
For the algorithm to terminate we need the set $\mathcal{L}$ to become empty eventually. This happens if and only if after finitely many steps every S- and G-polynomial based on any combination of leading terms has normal form zero w.r.t $\mathcal{G}$, i.e. there exists a chain of LM-reductions such that the current S- or G-polynomial reduces to zero. However, LM-reductions only take place when we have reducing polynomials of equal or smaller degree and all of these have already been computed at this point, due to our choice of a graded global monomial ordering. Thus it is not possible that we obtain elements which can not be reduced unless we remove the degree-bound. Therefore, the algorithm terminates.

For the correctness of the algorithm we still need a version of Buchberger's criterion as in Theorem 5.10. More precisely we want $\mathcal{G}$ to be a Gröbner basis for $\mathcal{I}$ if and only if for every pair f, $g \in \mathcal{G}$, where $f = g$ is allowed, their S- and G-polynomials reduce to zero. Moreover, we only want to consider first and second type S- and G-polynomials i.e. only use $t \in \mathrm{cm}(\mathrm{LM}(f), \mathrm{LM}(g))$ with

1. $t = \mathrm{LM}(f)t'_f = t_g\mathrm{LM}(g)$,
2. $t = \mathrm{LM}(f) = t_g\mathrm{LM}(g)t'_g$,
3. $t = t_f\mathrm{LM}(f) = \mathrm{LM}(g)t'_g$ or
4. $t = t_f\mathrm{LM}(f)t'_f = \mathrm{LM}(g)$

for t_f, t'_f, t_g, $t'_g \in X$. This excludes all cases where t is not minimal, i.e. $t = w_1t'w_2$ for w_1, $w_2 \in X$ and t' satisfying one of the above cases. Moreover, we noted in chapter 4, Remark 4.15, that for a basis of the left syzygy module (which is not finitely generated in general) we may use syzygies, that have exactly two non-zero entries.

Lemma 7.21.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$. Then $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I} := \langle \mathcal{G} \rangle$, if and only if for every pair f, $g \in \mathcal{G}$ their first and second type S- and G-polynomials reduce to zero w.r.t. $\mathcal{G}$.

Proof.
The proof is similar to the commutative case. The "only if" part follows immediately from Theorem 7.5.
For "if" let $0 \neq f \in \langle \mathcal{G} \rangle = \mathcal{I}$ with $f = \sum_i h_i g_i$ for some $h_i \in \mathcal{P}^e$. We set $t := \max(\mathrm{LM}(h_i g_i)$ and $M := \{i \in \mathbb{N} \mid \mathrm{LM}(h_i g_i) = t\}$. Clearly $\mathrm{LM}(f) \preceq t$ and we may assume that there is no other representation of f where t is smaller. Without loss of generality let $M = \{1, \ldots, m\}$. Moreover, since the Euclidean norm induces a well ordering, we can choose a representation where $\sum_{i=1}^{m} |\mathrm{LC}(h_i)\mathrm{LC}(g_i)|$ is minimal w.r.t. t. If M contains

exactly one element, then $t = \mathrm{LM}(f)$ and we have a strong standard representation of f w.r.t. $\mathcal{G}$. Suppose otherwise that $\mathrm{card}(M) > 1$. Then $t \geq \mathrm{LM}(f)$. Note that $t = \mathrm{LM}(h_i g_i) = \mathrm{LM}(h_i)\mathrm{LM}(g_i)$ for $i \leq m$. Then there exist monomials t_1, t_1', t_2, $t_2' \in X$, such that $t = t_1\mathrm{LM}(g_1)t_1' = t_2\mathrm{LM}(g_2)t_2'$. This induces an overlap relation of the leading monomials, because then there exist s_1, s_1', s_2, $s_2' \in X$ such that

- $T := \mathrm{LM}(g_1)s_1' = s_2\mathrm{LM}(g_2)$,
- $T := \mathrm{LM}(g_1) = s_2\mathrm{LM}(g_2)s_2'$,
- $T := s_1\mathrm{LM}(g_1) = \mathrm{LM}(g_2)s_2'$ or
- $T := s_1\mathrm{LM}(g_1)s_1' = \mathrm{LM}(g_2)$

and $t = \tau T$ for some monomial $\tau \in \mathcal{P}^e$. Moreover, let τ_1, τ_2 result from s_1, s_1', s_2, s_2', such that $\tau_1 T = \mathrm{LM}(g_1)$, $\tau_2 T = \mathrm{LM}(g_2)$. Furthermore, let

$$a_1 := \frac{\mathrm{lcm}(\mathrm{LC}(g_1), \mathrm{LC}(g_2))}{\mathrm{LC}(g_1)},\ a_2 := \frac{\mathrm{lcm}(\mathrm{LC}(g_1), \mathrm{LC}(g_2))}{\mathrm{LC}(g_2)}$$

$d := \gcd(\mathrm{LC}(g_1), \mathrm{LC}(g_2)) = b_1\mathrm{LC}(g_1) + b_2\mathrm{LC}(g_2) \in \mathcal{R}$, the Bézout identity for the leading coefficients. Now if T corresponds to a non-trivial overlap, then we can compute $\mathrm{spoly}_1^T(g_1, g_2)$, $\mathrm{gpoly}_1^T(g_1, g_2)$ or $\mathrm{spoly}_1^T(g_2, g_1)$, $\mathrm{spoly}_1^T(g_2, g_1)$, respectively. Otherwise there exists $w \in \mathcal{X}$, such that $T = \mathrm{LM}(g_1)w\mathrm{LM}(g_2)$ or $T = \mathrm{LM}(g_2)w\mathrm{LM}(g_1)$. In this case we are interested in $\mathrm{spoly}_2^w(g_1, g_2)$, $\mathrm{gpoly}_2^w(g_1, g_2)$ or $\mathrm{spoly}_2^w(g_2, g_1)$, $\mathrm{spoly}_2^w(g_2, g_1)$, respectively. Anyway this shows that

$$\mathrm{spoly}(g_1, g_2) := a_1\tau_1 g_1 - a_2\tau_2 g_2$$

and

$$\mathrm{gpoly}(g_1, g_2) := b_1\tau_1 g_1 + b_2\tau_2 g_2$$

are first or second type S- and G-polynomials and $\mathrm{LM}(h_1) = \tau\tau_1$, $\mathrm{LM}(h_2) = \tau\tau_2$. Analogous to the proof of Theorem 5.10 there exists a, $b \in \mathcal{R} \setminus \{0\}$ such that $\mathrm{LC}(h_1)\mathrm{LC}(g_1) + \mathrm{LC}(h_2)\mathrm{LC}(g_2) = ad$ and $\mathrm{LC}(h_1) = ab_1 + ba_1$, $\mathrm{LC}(h_2) = ab_2 - ba_2$. Then since $|a_1\mathrm{LC}(g_1) + a_2\mathrm{LC}(g_2)| > 0$ and by the triangle inequality we have

$$\begin{aligned}
&|\mathrm{LC}(h_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(h_2)\mathrm{LC}(g_2)|\\
=&|(ab_1 + ba_1)\mathrm{LC}(g_1)| + |(ab_2 - ba_2)\mathrm{LC}(g_2)|\\
\geq&|ab_1\mathrm{LC}(g_1)| + |ba_1\mathrm{LC}(g_1)| + |ab_2\mathrm{LC}(g_2)| + |ba_2\mathrm{LC}(g_2)|\\
>&|ab_1\mathrm{LC}(g_1)| + |ab_2\mathrm{LC}(g_2)|\\
\geq&|ab_1\mathrm{LC}(g_1) + ab_2\mathrm{LC}(g_2)|\\
=&|ad|,
\end{aligned}$$

thus $|ad| < |\mathrm{LC}(h_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(h_2)\mathrm{LC}(g_2)|$. Furthermore, we have

$$\begin{aligned}
h_1 g_1 + h_2 g_2 =&(\mathrm{LC}(h_1)\mathrm{LM}(h_1)\,\mathrm{tail}(h_1))g_1 + (\mathrm{LC}(h_2)\mathrm{LM}(h_2)\,\mathrm{tail}(h_2))g_2\\
=&(ab_1 + ba_1)\tau\tau_1 g_1 + \mathrm{tail}(h_1)g_1 + (ab_2 - ba_2)\tau\tau_2 g_2 + \mathrm{tail}(h_2)g_1\\
=&a\tau(b_1\tau_1 g_1 + b_2\tau_2 g_2) + b\tau(a_1\tau_1 g_1 - a_2\tau_2 g_2) + \mathrm{tail}(h_1)g_1 + \mathrm{tail}(h_2)g_1\\
=&a\tau\,\mathrm{gpoly}(g_1, g_2) + b\tau\mathrm{spoly}(g_1, g_2) + \mathrm{tail}(h_1)g_1 + \mathrm{tail}(h_2)g_1.
\end{aligned}$$

Since the S- and the G-polynomial are of first or second type they reduce to zero w.r.t. $\mathcal{G}$. Hence we can write $h_1g_1 + h_2g_2 = \sum_j h'_j g_j$ for $h'_j \in \mathcal{P}^e$ and define $M' := \{j \in \mathbb{N} \mid \mathrm{LM}(h'_j g_j) = t\}$. Since $\mathrm{LM}(\tau\mathrm{spoly}(g_1, g_2)) \prec t$, $\mathrm{LM}(\mathrm{tail}(h_1)g_1) \prec t$ and $\mathrm{LM}(\mathrm{tail}(h_2)g_1) \prec t$ we have

$$\begin{aligned}
&\sum_{j\in M'} |\mathrm{LC}(h'_j)\mathrm{LC}(g_j)| \\
=&\sum_{j\in M'} |\mathrm{LC}(h'_j g_j)| \\
=&|\mathrm{LC}(d\tau\,\mathrm{gpoly}(g_1, g_2))| \\
=&|ad| \\
<&|\mathrm{LC}(h_1)\mathrm{LC}(g_1)| + |\mathrm{LC}(h_2)\mathrm{LC}(g_2)|,
\end{aligned}$$

which contradicts our assumption that the leading coefficient of our original representation are minimal. Therefore, M contains exactly one element and thus we have a strong Gröbner representation of f w.r.t. $\mathcal{G}$, i.e. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$. □

This is similar to a statement over fields which can be found in [12] (chapter 1.3.1, Lemma 1.45). The point is that these overlap relations or "obstructions" $t_f\mathrm{LM}(f)t'_f = t_g\mathrm{LM}(g)t'_g$ correspond to S- and G-polynomials up to coefficients. But since the coefficients are uniquely determined by f and g and we compute S- and G-polynomials for all pairs, we do not loose any information. Now let $\tau_f = t_f \otimes t'_f$, $\tau_g = t_g \otimes t'_g \in \mathcal{P}^e$, $t \in \mathrm{cm}(\mathrm{LM}(f), \mathrm{LM}(g))$ with $t = \tau_f\mathrm{LM}(f) = \tau_g\mathrm{LM}(g)$. Then there exists a $t' \in \mathrm{cm}(\mathrm{LM}(f), \mathrm{LM}(g))$ that satisfies one of the above four cases 1. – 4. and τ, τ'_f, $\tau'_g \in \mathcal{P}^e$ such that $t = \tau t' = \tau'_f\mathrm{LM}(f) = \tau'_g\mathrm{LM}(g)$ and $\tau_f = \tau\tau'_f$, $\tau_g = \tau\tau'_g$. Let

$$\begin{aligned}
\mathrm{spoly}(f, g) &= a_f\tau_f f - a_g\tau_g g & \mathrm{gpoly}(f, g) &= b_f\tau_f f + b_g\tau_g g \\
\mathrm{spoly}'(f, g) &= a_f\tau'_f f - a_g\tau'_g g & \mathrm{gpoly}'(f, g) &= b_f\tau'_f f + b_g\tau'_g g
\end{aligned}$$

be the corresponding S- and G-polynomials. Clearly $\mathrm{spoly}'(f, g)$, $\mathrm{gpoly}'(f, g)$ are first or second type S- and G-polynomials and we have $\mathrm{spoly}(f, g) = \tau\,\mathrm{spoly}'(f, g)$ and $\mathrm{gpoly}(f, g) = \tau\,\mathrm{gpoly}'(f, g)$. Therefore, if $\mathrm{spoly}'(f, g)$, $\mathrm{gpoly}'(f, g)$ reduce to zero w.r.t. $\mathcal{G}$, then so do $\mathrm{spoly}(f, g)$ and $\mathrm{gpoly}(f, g)$.

Before we describe a method to implement this algorithm in the computer algebra system Singular [24] we should address the necessity of second type S- and G-polynomials. A question that arises is if $\mathrm{gpoly}_2^w(f, g)$ may be redundant for $|w|$ high enough, i.e. if there is w' with $|w'| < |w|$ such that $\mathrm{LM}(\mathrm{gpoly}_2^{w'}(f, g))$ divides $\mathrm{LM}(\mathrm{gpoly}_2^w(f, g))$. We consider an example to visualize this.

Example 7.22.
For $n \in \mathbb{N}_0$ let $X_n \subseteq X$ be the set of monomials in X of length n. If X is finite, then clearly $\mathrm{card}(X_n) = (\mathrm{card}(X))^n$ is the cardinality of X_n.

- Let $f = 4x$, $g = 6y \in \mathbb{Z}\langle x, y\rangle$. Then $2xy$ is a G-polynomial of f and g and divides every other G-polynomial $2xwy$ for a monomial $w \in \langle x, y\rangle$, because either w starts

with y or ends with x or otherwise w must contain (i.e. is divisible by) xy. Similarly $2yx$ is a G-polynomial of g and f and divides every other G-polynomial $2ywx$. So in this particular case $\{4x,\, 6y,\, 2xy,\, 2yx\}$ is a finite strong Gröbner basis for the ideal $\langle f,\, g\rangle$.
Observation: Note that $\langle 4x,\, 6y\rangle = \langle 2\rangle \cdot \langle 2x,\, 3y\rangle$ and a strong Gröbner basis for $\langle 2x,\, 3y\rangle$ is given by $\{2x,\, 3y,\, xy,\, yx\}$ with $\{4x,\, 6y,\, 2xy,\, 2yx\} = 2 \cdot \{2x,\, 3y,\, xy,\, yx\}$. This tells us that our problem with Gröbner basis over rings results from the coefficients in $\langle 2x,\, 3y\rangle$ and not from the greatest common divisor of the leading coefficients. We, therefore, proceed with polynomials that have coprime leading coefficients.

- Now let $f = 2x,\, g = 3y \in \mathbb{Z}\langle x,\, y,\, z\rangle$. Then xy is a G-polynomial of f and g and according to the algorithm we compute every other second type G-polynomial $\operatorname{gpoly}_2^w(f,\, g) = xwy$ for $w \in \langle x,\, y,\, z\rangle$. But both xxy and xyy are divided by xy and, therefore, the only necessary second type G-polynomial with $|w| = 1$ is xzy. In a different notation this means that the monomial set xX_1y contains all three second type G-polynomials of f and g but only one that is not reducible. In fact, it is easy to see that all G-polynomials in $xX_{|w|}y$ are redundant except

$$xwy = x \underbrace{z \cdots z}_{|w| \text{ times}} y$$

  for every $w \in X$. In numbers this means that X_2 contains nine elements but eight are redundant, X_3 contains 27 elements but 26 of them are redundant, etc. We have the analogous statement for the G-polynomials ywx for $w \in X$.

- A less trivial example can be found when looking at $f = 2xy,\, g = 3xz \in \mathbb{Z}\langle x,\, y,\, z\rangle$. Then $\operatorname{gpoly}_2^w(f,\, g) = xywxz$ for $w \in \langle x,\, y,\, z\rangle$ and

$$xyX_0xz = \{xyxz\}$$

  contains one element and it is not any further reducible. Next

$$xyX_1xz = \{xyxxz,\, xyyxz,\, xyzxz\}$$

  contains three elements of which none are further reducible. For $|w| = 2$ the set

$$xyX_2xz = \{xyxxxz,\, xyxyxz,\, xyxzxz,\, xyyxxz,\, \ldots\}$$

  contains nine elements of which two are reducible namely $xyxyxz$ and $xyxzxz$. Note that the elements of xyX_jxz can if possible only be reduced by elements of xyX_ixz with $i \leq j - 2$. One can check that xyX_3xz contains 27 elements of which 12 are reducible, xyX_4xz contains 81 elements of which 50 are reducible and xyX_5xz contains 243 elements of which 105 are reducible.

One might conclude that the more elements X contains and the larger the degree of f and g, the less elements are contained in $xyX_{|w|}xz$ which are reducible. Thus we have more necessary second type G-polynomials, which has to be checked with further computations.

The number of reducible elements is not trivial to compute and depends on $|w|$, the degree of the input polynomials and their leading monomials and the monoid X itself. Therefore, to predict whether gpoly_2^w is necessary is expected to be just as hard as letting the normal form handle the reductions automatically as it is done in Algorithm 7.20.

In A.2 we give an example for a computation of a Gröbner basis for an ideal in the field case, the commutative case and our current case, non-commutative with coefficients in $\mathcal{R}$.

We give some more examples for Gröbner basis that have been computed up to a certain degree.

Example 7.23. (cf. [23], Examples 1–4)
Let $\mathcal{P} = \mathcal{Z}\langle x, y, z\rangle$ with the graded left lexicographical ordering and $x \succ y \succ z$.

- We consider the ideal $\mathcal{I} = \langle f_1 = yx - 3xy - 3z,\ f_2 = zx - 2xz + y,\ f_3 = zy - yz - x\rangle$. Then $\mathcal{I}$ has an infinite Gröbner basis and the elements, which can be subsequently constructed, are

$$\begin{aligned}\mathcal{G} = \{&f_1,\ f_2,\ f_3,\\ &6yz + 3x,\ 9xz - 3y,\ 12xy + 9z,\ 12y^2 - 27z^2,\ x^2 + 2y^2 - 6z^2,\\ &9z^3 - 30xy - 21z,\ 4y^3 + 9yz^2 + 3y,\ 4xy^2 + 3yz + 3x,\ 3xyz - 3y^2 + 9z^2,\\ &3yz^3 - 90xy^2 3xz^2 - 3yz - 36x,\ 2y^3z - 3xy^2 + 3yz,\ xy^2z - 3y^3 - 3xz,\\ &y^3z^3 - 2xy^4 - 3y^3z - 3yz^3 + xy^2 - 3yz,\ xy^3z + 3y^4 - 6y^2z^2,\\ &xy^4z + y^5 + y^3z^2 + y^3z^2 + 2y^3 - 3yz^2,\ xy^5z - y^6 + 3y^4z^2,\ \ldots\}.\end{aligned}$$

  However, one can show that $\mathcal{I}$ contains an element $xy^iz + \text{l.o.t.}$ for every $2 \leq i \in \mathbb{N}$ and these are the only polynomials that have to be added to $\mathcal{G}$ in order to obtain a Gröbner basis for $\mathcal{I}$.

- Let $\mathcal{I} = \langle f_1 = yx - 3xy - z,\ f_2 = zx - xz + y,\ f_3 = zy - yz - x\rangle$. Then $\mathcal{I}$ has a finite strong Gröbner basis, namely

$$\mathcal{G} = \{f_1,\ f_2,\ f_3,\ 8xy + 2z,\ 4xz,\ -2y,\ 4yz + 2x,\ 2x^2 - 2y^2,\ 4y^2 - 2z^2,\ 2z^3 - 2xy\}.$$

- Another ideal that has a finite Gröbner basis is $\mathcal{I} = \langle f_1 = yx - 3xy,\ zx + y^2,\ zy - yz + z^2\rangle$. A Gröbner basis for $\mathcal{I}$ is given by

$$\begin{aligned}\mathcal{G} = \{&f_1,\ f_2,\ f_3,\ 2y^3 + y^2z - 2yz^2 + 2z^3,\ 14yz^3 - 28z^4,\\ &y^2z^2 - 4yz^3 + 6z^4,\ 27xy^2z - 54xyz^2 + 54xz^3 + y^4,\ 14z^5,\\ &2yz^4 - 6z^5,\ y^4z,\ y^5,\ 2xyz^3 - 4xz^4,\ 27xy^3z,\ 2z^6,\ 2xz^5\}.\end{aligned}$$

There are two problems with our above considerations. First of all we can only compute up to a certain upper bound for the length of leading monomials, because Gröbner bases over $\mathcal{P}$ are usually infinite. Secondly most implementations in SINGULAR [24] and other computer algebra systems are for commutative polynomials only. However, in 2009

Levandovskyy and La Scala developed a subsystem SINGULAR:LETTERPLACE [25] in [5], that uses commutative data structures and parts of Gröbner bases over the free algebra $\mathbb{Q}\langle X\rangle$. Every element up to a degree d of the polynomial ring $\mathcal{P} = \mathcal{R}\langle x_1, \ldots, x_n\rangle$ corresponds to an element of $\mathcal{LP} := \mathcal{R}[(x_1 \mid 1), \ldots, (x_1 \mid d), (x_2 \mid 1), \ldots, (x_2 \mid d), \ldots, (x_n \mid 1), \ldots, (x_n \mid d)]$ where for a monomial $(x_i \mid p) \in \mathcal{LP}$ the **letter** i refers to the element $x_i \in \mathcal{P}$ and the **place** p stands for its position in a monomial.

Example 7.24.
The monomial $x_1x_4x_3x_1 \in \mathcal{P}$ corresponds to $(x_1 \mid 1)(x_4 \mid 2)(x_3 \mid 3)(x_1 \mid 4) \in \mathcal{LP}$ which is the same as $(x_1 \mid 1)(x_1 \mid 4)(x_3 \mid 3)(x_4 \mid 2)$, because $\mathcal{LP}$ is commutative. On the other hand there are no elements in $\mathcal{P}$ which correspond to $(x_1 \mid 1)(x_2 \mid 1)$ (because the position $p = 1$ is overdetermined) or to $(x_1 \mid 1)(x_2 \mid 3)$ (because the position $p = 2$ is empty). By convention the unitary element $1 \in X$ corresponds to the 1-monomial in $\mathcal{LP}$.

The following definitions and considerations are analogous to [5] and [11].
We define a map $\phi : \mathcal{P} \to \mathcal{LP}$ with $x_{i_1} \cdots x_{i_k} \mapsto (x_{i_1} \mid 1) \cdots (x_{i_k} \mid k)$ for $k \leq d$. Clearly this map is injective and in every element of the image of a monomial the positions $1 \leq p \leq k$ occur exactly once.

Definition 7.25.
The commutative polynomial ring $\mathcal{LP}$ is called **Letterplace ring**. The monomials contained in $\mathrm{im}(\phi)$, including the 1-monomial, are called **Letterplace monomials**. A finite $\mathcal{R}$-linear combination of Letterplace monomials is called a **Letterplace polynomial**.

Since the Letterplace ring requires an upper bound for the length of monomials just as we need an upper bound for computations in Buchberger's algorithm 7.20, we will attempt to apply the idea of SINGULAR:LETTERPLACE [25] to $\mathcal{R}\langle X\rangle$.
The product of two monomials in $\mathcal{P}$ is also a monomial. This is trivial but on the other hand ϕ is not a homomorphism, i.e. the product of two Letterplace polynomials is not a Letterplace monomial in general. Also we have to transfer the concept of overlaps to $\mathcal{LP}$ and, most importantly, we need a way to construct a monomial ordering on $\mathcal{LP}$ based on a given monomial ordering on $\mathcal{P}$.
For a Letterplace monomial $x = (x_{i_1} \mid 1) \cdots (x_{i_k} \mid k)$ and $\ell \in \mathbb{N}_0$ such that $k + \ell \leq d$ we define

$$\mathrm{shift}(x, \ell) = (x_{i_1} \mid 1 + \ell) \cdots (x_{i_k} \mid k + \ell),$$

the **shift** of x by ℓ and

$$x \times_{\ell p} y := x\,\mathrm{shift}(y, |x|),$$

the **$\mathcal{LP}$-product** of two Letterplace monomials x and y with $|x| + |y| \leq d$. Moreover, we say that x **$\mathcal{LP}$-divides** y if there exists $\ell \in \mathbb{N}_0$ with $\ell + |x| \leq d$ and $\mathrm{shift}(x, \ell)$ divides y in $\mathcal{LP}$. We denote this by $x|_{\ell p}y$. Finally for two Letterplace monomials x, y and $\ell \in \mathbb{N}$ with $\ell > |x|$ and $\ell + |y| \leq d$ we set

$$\mathrm{split}(w) := (x, y),$$

if $w = x\,\mathrm{shift}(y, \ell)$. Clearly w is not a Letterplace monomial. This would only be the case for $\ell = |x|$.

Example 7.26.
The Letterplace monomial $x := (x_2 \mid 1)$ $\mathcal{LP}$-divides $y := (x_1 \mid 1)(x_2 \mid 2)$, because $\mathrm{shift}(x, 1) = (x_2 \mid 2)$ divides y in $\mathcal{LP}$. This corresponds to the fact that x_1x_2 is divisible by x_2 in $\mathcal{P}$.

Remark 7.27.
Let $v, w \in \mathcal{P}$ be monomials. Then the Letterplace monomial corresponding to vw is the $\mathcal{LP}$-product of their Letterplace monomials, i.e. $\phi(vw) = \phi(v)\,\mathrm{shift}(w, |v|)$. $\mathcal{LP}$-multiplication is associative but not commutative. Furthermore, v divides w, if and only if $\phi(v)$ $\mathcal{LP}$-divides $\phi(w)$.
Let $\preceq$ be the graded left lexicographical ordering with $x_1 \succ x_2 \succ \ldots \succ x_n$ on X. Then there is a monomial ordering $\preceq_{\ell p}$ on the monomials of $\mathcal{LP}$ such that for $v, w \in X$ we have $v \prec w$, if and only if $\phi(v) \prec_{\ell p} \phi(w)$. We can take the graded lexicographical ordering with $(x_1 \mid 1) \succ (x_2 \mid 1) \succ \ldots \succ (x_n \mid 1) \succ (x_1 \mid 2) \succ (x_2 \mid 2) \succ \ldots \succ (x_n \mid 2) \succ \ldots$ and this chain stops at the smallest monomial of length 1 namely x_n^d, again indicating that we need an upper bound d.
Now the principal idea is to compute an element of $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ using commutative polynomials. Let $f, g \in \mathcal{LP} \setminus \{0\}$, such that $\mathrm{LM}(f)$ is a Letterplace monomial and $\mathrm{LM}(g)$ is the shift of a Letterplace monomial. Then there exists uniquely determined Letterplace monomials a, b such that $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f) \times_{\mathcal{LP}} b = a\,\mathrm{LM}(g)$ or $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f) = (a\,\mathrm{LM}(g)) \times_{\mathcal{LP}} b$. It is essential to point out that the least common multiple is uniquely determined in this commutative setting. Take for example $v = x_1x_2x_3x_2x_3$, $w = x_2x_3x_2x_3x_4 \in \mathcal{P}$ with two non-trivial overlaps $x_2x_3x_2x_3$ (blue) and x_2x_3 (red). The corresponding Letterplace monomials are $\phi(v) = (x_1 \mid 1)(x_2 \mid 2)(x_3 \mid 3)(x_2 \mid 4)(x_3 \mid 5)$ and $\phi(w) = (x_2 \mid 1)(x_3 \mid 2)(x_2 \mid 3)(x_3 \mid 4)(x_4 \mid 5)$. Then the corresponding least common multiples in $\mathcal{LP}$ that we are interested in are given by

$$\mathrm{lcm}(\phi(v), \mathrm{shift}(\phi(w), 1)) = (x_1 \mid 1)(x_2 \mid 2)(x_3 \mid 3)(x_2 \mid 4)(x_3 \mid 5)(x_4 \mid 6)$$

for

x_1	x_2	x_3	x_2	x_3		
	x_2	x_3	x_2	x_3	x_4	

and

$$\mathrm{lcm}(\phi(v), \mathrm{shift}(\phi(w), 3)) = (x_1 \mid 1)(x_2 \mid 2)(x_3 \mid 3)(x_2 \mid 4)(x_3 \mid 5)(x_2 \mid 6)(x_3 \mid 7)(x_4 \mid 8)$$

for

x_1	x_2	x_3	x_2	x_3			
			x_2	x_3	x_2	x_3	x_4

but we also have to consider trivial overlaps. In the field case it suffices to take

$$\begin{aligned}
&\phi(v) \times_{\mathcal{LP}} \phi(w)\\
=&\phi(v)\,\mathrm{shift}(\phi(w),\,5)\\
=&(x_1 \mid 1)(x_2 \mid 2)(x_3 \mid 3)(x_2 \mid 4)(x_3 \mid 5)(x_2 \mid 6)(x_3 \mid 7)(x_2 \mid 8)(x_3 \mid 9)(x_4 \mid 10),
\end{aligned}$$

because $\phi(v)$ has length 5. When computing over $\mathcal{R}$, we also need the infinitely many

$$\begin{aligned}
&\phi(v) \times_{\mathcal{LP}} \tilde{w} \times_{\mathcal{LP}} \phi(w)\\
=&\phi(v)\,\mathrm{shift}(\tilde{w},\,5)\,\mathrm{shift}(\phi(w),\,5+|\tilde{w}|)\\
=&(x_1 \mid 1)(x_2 \mid 2)(x_3 \mid 3)(x_2 \mid 4)(x_3 \mid 5)\,\hat{w}\,\cdots\\
&\cdots(x_2 \mid 6+|\tilde{w}|)(x_3 \mid 7+|\tilde{w}|)(x_2 \mid 8+|\tilde{w}|)(x_3 \mid 9+|\tilde{w}|)(x_4 \mid 10+|\tilde{w}|)
\end{aligned}$$

for every Letterplace monomial $\tilde{w}$ and $\hat{w} = \mathrm{shift}(\tilde{w},\,5)$. The procedure stops when $|\phi(v)|+|\tilde{w}|+|\phi(w)| \geq d$.

Algorithm 7.28. (**Buchberger's algorithm for degree-bounded strong Gröbner bases over $\mathcal{R}\langle X\rangle$ with Letterplace**)
The following algorithm computes a set $\mathcal{G}$ of Letterplace polynomials such that the preimage $\phi^{-1}(\mathcal{G})$ is a degree-bounded strong Gröbner basis for the ideal generated by the preimage of the input Letterplace polynomials.

SbbaLP

---

input: $\{f_1, \ldots, f_k\} \subseteq \mathcal{LP}$, $d \in \mathbb{N}$, Reduce, LmShift, InsertPair, Spoly, Gpoly
output: degree-bounded set $\mathcal{G}$ of Letterplace polynomials
01: $\mathcal{G} = \emptyset$
02: $T = \emptyset$
03: $L = \{(0,\, 0,\, f_i) \mid 1 \leq i \leq k\}$
04: **while** $L \neq \emptyset$ **do**
05: choose $(a,\, b,\, h) \in L$
06: $L = L \setminus \{(a,\, b,\, h)\}$
07: **if** $h = 0$ **then**
08: $h_1 = \mathrm{Spoly}(a,\, b)$
09: $h_2 = \mathrm{Gpoly}(a,\, b)$
10: **end if**
11: **for** $j \in \{1,\, 2\}$ **do**
12: $h = \mathrm{Reduce}(h_j,\, T)$
13: **if** $h \neq 0$ **then**
14: **for** $0 \leq l \leq d - \deg(h)$ **do**
15: $T = T \cup \{\mathrm{LmShift}(h,\, l)\}$
16: **end do**
17: $\mathcal{G} = \mathcal{G} \cup \{h\}$
18: **for** $g \in \mathcal{G}$ **do**

```
            for 0 ≤ l ≤ d − deg(h) do
               h′ = LmShift(h, l)
               if l ≥ deg(g) then
                  for w a Letterplace monomial with |w| = l − deg(g) do
                     w′ = shift(w, deg(g))
                     L = InsertPair(g, w′h′, L)
                  end do
               else
                  L = InsertPair(g, h′, L)
               end if
            end do
            for 1 ≤ l ≤ d − deg(h) do
               g′ = LmShift(g, l)
               if l ≥ deg(h) then
                  for w a Letterplace monomial with |w| = l − deg(h) do
                     w′ = shift(w, deg(h))
                     L = InsertPair(h, w′g′, L)
                  end do
               else
                  L = InsertPair(h, g′, L)
               end if
            end do
         end do
      end if
   end do
end while
return G
```

This algorithm is, similar to the field case, merely a translation of non-commutative polynomials to Letterplace polynomials and has the theoretical background conditions and special features as Algorithm 7.20. We should still comment the procedure, since it is rather lengthy. The set $\mathcal{G}$ was originally denoted by S for "standard basis" in 5 and contains the Letterplace polynomials that we are interested in, namely those, whose preimage is a bounded strong Gröbner basis. $\mathcal{G}$, or S respectively, is kept small in order to correspond to a reduced Gröbner basis. The set T on the other hand is used to reduce elements. The "lazy" set L consists of triplets which are either of shape $(0,\ 0,\ f_i)$, for the initial polynomials f_i, or $(a,\ b,\ 0)$, which are used to form S- and G-polynomials up to a certain degree. Whenever the leading monomials of a and b have a least common multiple, which is a Letterplace monomial, we add the pair in form of a triplet to the set L and thus, iteratively, obtain all possible combinations of S- and G-polynomials, both first and second type. These S- and G-polynomials are then reduced by, as we mentioned under Algorithm 7.20, polynomials of smaller or equal degree. After finitely many steps every S- and G-polynomial reduces to zero and the set L will be empty. Thus the algorithm terminates.

We use the following procedures.

Algorithm 7.29. (**Supporting Procedures**)
First type S- and G-polynomials are computed with the following two procedures. It is important to point out that in the following $\mathrm{LM}(f)$ is a Letterplace monomial, whereas $\mathrm{LM}(g)$ may be shifted.

SPOLY

---

input: $f, g \in \mathcal{LP}$
output: $\mathrm{spoly}(f, g)$
01: $t = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$
02: $a = \mathrm{lcm}(\mathrm{LC}(f), \mathrm{LC}(g))$
03: $t_f = \dfrac{t}{\mathrm{LM}(f)}$
04: $t_g = \dfrac{t}{\mathrm{LM}(g)}$
05: $a_f = \dfrac{a}{\mathrm{LC}(f)}$
06: $a_g = \dfrac{a}{\mathrm{LC}(g)}$
07: $(t_f, t'_f) = \mathrm{split}(t_f)$
08: $(t_g, t'_g) = \mathrm{split}(t_g)$
09: **return** $a_f t_f \times_{\mathcal{LP}} \mathrm{tail}(f) \times_{\mathcal{LP}} t'_f - a_g t_g \times_{\mathcal{LP}} \mathrm{tail}(g) \times_{\mathcal{LP}} t'_g$

It is important to note that the element t_f is a shift of a Letterplace monomial, because $\mathrm{LM}(f)$ is a Letterplace monomial. Therefore, we have $\mathrm{split}(t_f) = (1, t'_f)$ for some Letterplace monomial such that $\mathrm{LM}(f)t_f = \mathrm{LM}(f) \times_{\mathcal{LP}} t'_f$. This is an aspect of implementation as it is done in the field case.

GPOLY

---

input: $f, g \in \mathcal{LP}$
output: $\mathrm{spoly}(f, g)$
01: $t = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$
02: $(b, b_f, b_g) = \mathrm{ExtGcd}(\mathrm{LC}(f), \mathrm{LC}(g))$
03: $t_f = \dfrac{t}{\mathrm{LM}(f)}$
04: $t_g = \dfrac{t}{\mathrm{LM}(g)}$
05: $(t_f, t'_f) = \mathrm{split}(t_f)$
06: $(t_g, t'_g) = \mathrm{split}(t_g)$
07: **return** $b\, t_f \times_{\mathcal{LP}} \mathrm{LM}(f) \times_{\mathcal{LP}} t'_f + b_f t_f \times_{\mathcal{LP}} \mathrm{tail}(f) \times_{\mathcal{LP}} t'_f + b_g t_g \times_{\mathcal{LP}} \mathrm{tail}(g) \times_{\mathcal{LP}} t'_g$

Reduction of h happens whenever an element of $\mathcal{G}$ LM-reduces h. This is essentially our normal form Algorithm 5.9 from chapter 5.

REDUCE

input: $f \in \mathcal{LP}$, $T \subseteq \mathcal{LP}$
output: normal form of f w.r.t. T
01: $h = f$
02: **while** $h \neq 0$ and $T_h = \{g \in T \mid g \text{ LM-reduces } h\} \neq \emptyset$ **do**
03: choose $g \in T_h$
04: choose $a \in \mathcal{R} \setminus \{0\}$, $b \in \mathcal{R}$ with $\mathrm{LC}(h) = a\mathrm{LC}(g) + b$ and $|b| < |\mathrm{LC}(g)|$
05: $t = \dfrac{\mathrm{LM}(h)}{\mathrm{LM}(g)}$
06: $(t_1, t_2) = \mathrm{split}(t)$
07: $h = b\mathrm{LM}(h) + \mathrm{tail}(h) - at_1 \times_{\mathcal{LP}} \mathrm{tail}(g) \times_{\mathcal{LP}} t_2$
08: **end while**
09: **return** h

One problem that arises is that after shifting the leading monomial of a Letterplace polynomial it may have a different leading term. In other words $\mathrm{shift}(\mathrm{LM}(h), l)$ and $\mathrm{LM}(\mathrm{shift}(\mathrm{LM}(h), l) + \mathrm{tail}(h))$ may be distinct due to the construction of the Letterplace ring depending on the monomial ordering. However, the tail of h will be considered in the later steps of the algorithm allowing us to only focus on the shift of the leading monomial instead of shifting every monomial in h.

LMSHIFT

input: $h \in \mathcal{LP}$, $l \in \mathbb{N}_0$
output: h with shifted leading term
01: **return** $\mathrm{LC}(h)\mathrm{shift}(\mathrm{LM}(h), l) + \mathrm{tail}(h)$

A pair is inserted whenever the least common multiple of the leading monomials has the right structure, i.e. is a Letterplace monomial. This takes place after h is added to $\mathcal{G}$, because we need S-polynomials of elements with themselves.

INSERTPAIR

input: $f, g \in \mathcal{LP}$, $L \subseteq \mathcal{LP}^{1\times 3}$
output: L or $L \cup \{(f, g, 0)\}$
01: $t = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$
02: **if** t is a Letterplace monomial **then**
03: $L = L \cup \{(f, g, 0)\}$
04: **end if**
05: **return** L

To apply our criteria for critical pairs we will translate the conditions to $\mathcal{LP}$-polynomials.

Lemma 7.30.
Commutative version: If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$, then $\mathrm{gpoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$.
Non-commutative version: If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$, then every first and second type G-polynomial reduces to zero w.r.t. $\{f, g\}$.
$\mathcal{LP}$-version: Let $w \in X$ and $g' := \textsc{LmShift}(g, \deg(f))$, $w' := \textsc{LmShift}(w, \deg(f))$, $g'' := \textsc{LmShift}(g, |w|+\deg(f))$. If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$, then $\textsc{Gpoly}(f, g')$ and $\textsc{Gpoly}(f, w'g'')$ are redundant for Algorithm 7.28.

To apply this to the algorithm, we check in line 09, whether
$\gcd(\mathrm{LC}(a), \mathrm{LC}(b)) \in \{\mathrm{LC}(a), \mathrm{LC}(b)\}$. If this is true then we set $h_2 = h_1$ and hence only consider one element in line 11. Otherwise we continue with $h_2 = \textsc{Spoly}(a, b)$. For further improvements we can apply the Lemma in lines 23, 26, 34, 37 respectively, where a new pair is added to L. Whenever $\textsc{InsertPair}(g, h', L)$ (or any other of the four insertions) is called up, we check if $\gcd(\mathrm{LC}(g), \mathrm{LC}(h)) \in \{\mathrm{LC}(g), \mathrm{LC}(h)\}$ and skip the insertion if this is true (note that g', h' are just shifts of g, h respectively, and thus have the same leading coefficient).

Lemma 7.31.
Commutative version: If $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ are coprime and $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ are coprime, then $\mathrm{spoly}(f, g)$ reduces to zero w.r.t. $\{f, g\}$.
Non-commutative version: Let $\ell_f := |\mathrm{LM}(f)|-|\mathrm{LM}(\mathrm{tail}(f))|$, $\ell_g := |\mathrm{LM}(g)|-|\mathrm{LM}(\mathrm{tail}(g))|$ and $w \in X$. If $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ are coprime and either

- $\ell_f \neq \ell_g$ or
- $\ell_f = \ell_q > |w|$ and $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ have only trivial overlaps or
- $\ell_f = \ell_g < |w|$ and there do not exist monomials x, $y \in X$ with $\mathrm{LM}(f) = \mathrm{LM}(\mathrm{tail}(f))x$ and $\mathrm{LM}(g) = y\mathrm{LM}(\mathrm{tail}(g))$ or
- $\ell_f = \ell_g < |w|$, there exist monomials x, $y \in X$ with $\mathrm{LM}(f) = \mathrm{LM}(\mathrm{tail}(f))x$ and $\mathrm{LM}(g) = y\mathrm{LM}(\mathrm{tail}(g))$ and $\mathrm{LC}(f)\mathrm{LC}(\mathrm{tail}(g)) \neq \mathrm{LC}(g)\mathrm{LC}(\mathrm{tail}(f))$,

then $\mathrm{spoly}_2^w(f, g)$ reduces to zero. Shortly written, the above conditions imply that $\mathrm{LT}(\mathrm{tail}(f)wg) \neq \mathrm{LT}(fw\,\mathrm{tail}(g))$. However, note that the condition $\ell_f \neq \ell_g$ is easy to check and weak compared to conditions of coprimeness.
$\mathcal{LP}$-version: Let $g' := \textsc{LmShift}(g, \deg(f))$, $w' := \textsc{LmShift}(w, \deg(f))$ and $g'' := \textsc{LmShift}(g, |w| + \deg(f))$. If $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ are coprime then the corresponding $\mathcal{LP}$-polynomial to the second type S-polynomials is

$$\textsc{Spoly}(f, w'g'') = \mathrm{tail}(f) \times_{\mathcal{LP}} w \times_{\mathcal{LP}} g - f \times_{\mathcal{LP}} w \times_{\mathcal{LP}} \mathrm{tail}(g)$$

which is redundant for Algorithm 7.28, if

- $\ell_f := \deg(f) - \deg(\mathrm{tail}(f)) \neq \deg(g) - \deg(\mathrm{tail}(g)) =: \ell_g$ or

- $\mathrm{LC}(f) \nmid \mathrm{LC}(\mathrm{tail}(f))$ or
- $\mathrm{LC}(g) \nmid \mathrm{LC}(\mathrm{tail}(g))$ or
- $\mathrm{LC}(f)\mathrm{LC}(\mathrm{tail}(g)) \neq \mathrm{LC}(g)\mathrm{LC}(\mathrm{tail}(f))$ or
- $|w| < \ell_f$ and $\mathrm{LM}(f)$, $\mathrm{shift}(\mathrm{LM}(g), \deg(\mathrm{tail}(f)) + |w|)$ are coprime or
- $\mathrm{LM}(f)$, $\mathrm{LM}(\mathrm{tail}(f))$ are coprime or
- $\mathrm{LM}(g)$, $\mathrm{shift}(\mathrm{LM}(\mathrm{tail}(g)), \ell_g)$ are coprime or
- $\mathrm{LM}(f)$, $\mathrm{shift}(w, \deg(\mathrm{tail}(f)))$ are coprime or
- $|w| \geq \ell_g$ and w, $\mathrm{shift}(\mathrm{LM}(g), |w| - \ell_g)$ are coprime or
- $|w| < \ell_f$ and $\mathrm{LM}(g)$, $\mathrm{shift}(w, \ell_f - |w|)$ are coprime.

This criterion finds application in lines 23 and 34 where the second type polynomials are added to L via InsertPair. If $h = h_1$ and $l \geq \deg(g)$ in line 20 or $l \geq \deg(g)$ in line 31 then we check if $\mathrm{LC}(g)$, $\mathrm{LC}(h)$ are coprime and again skip the insertion if this is true and one of the above four conditions holds. Furthermore, over fields this criterion can be easily implemented in the InsertPair-procedure by checking if $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g'))$ is a Letterplace polynomial with $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g')) = \mathrm{LM}(f) \times_{\mathcal{LP}} \mathrm{LM}(g)$.

Lemma 7.32.
Commutative version: Let $f, g, h \in \mathcal{G} \subseteq \mathcal{P}$, such that

1. $\mathrm{LM}(f) \mid \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h))$,
2. $\mathrm{LC}(f) \mid \mathrm{lcm}(\mathrm{LC}(g), \mathrm{LC}(h))$ and
3. $\mathrm{spoly}(f, g)$ and $\mathrm{spoly}(f, h)$ have strong Gröbner representations.

Then $\mathrm{spoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.
Moreover, if

1. $\mathrm{LM}(f) \mid \mathrm{lcm}(\mathrm{LM}(g), \mathrm{LM}(h))$ and
2. $\mathrm{LC}(f) \mid \mathrm{gcd}(\mathrm{LC}(g), \mathrm{LC}(h))$,

then $\mathrm{gpoly}(g, h)$ has a strong Gröbner representation w.r.t. $\mathcal{G}$.
Non-commutative version: Let $f_1, f_2, f_3 \in \mathcal{G} \subseteq \mathcal{P}$ with

1. $\mathrm{LM}(f_1)r_1 = r_3\mathrm{LM}(f_3)$,
2. $\mathrm{LM}(f_1)s_1 = s_2\mathrm{LM}(f_2)$,
3. $\mathrm{LM}(f_2)t_2 = t_3\mathrm{LM}(f_3)$,
4. $\mathrm{LM}(f_2)$ divides $\mathrm{LM}(f_1)r_1 = r_3\mathrm{LM}(f_3)$ and

5. $\mathrm{LC}(f_2) \mid \mathrm{lcm}(\mathrm{LC}(f_1), \mathrm{LC}(f_3))$.

for $r_1, r_3, s_1, s_2, t_2, t_3 \in X$. We consider the to these overlap relations corresponding S-polynomials. If $\mathrm{spoly}(f_1, f_2)$ and $\mathrm{spoly}(f_2, f_3)$ reduce to zero, then so does $\mathrm{spoly}(f_1, f_3)$.

Proof.
Let

$$c_{ij} := \frac{\mathrm{lcm}(\mathrm{LC}(f_i), \mathrm{LC}(f_j)}{\mathrm{LC}(f_i)}$$

for $i, j \in \{1, 2, 3\}$. Then

$$\frac{c_{ij}c_{ki}}{c_{ik}} = \frac{c_{ji}c_{kj}}{c_{jk}}$$

for $\{i, j, k\} = \{1, 2, 3\}$. By the above relations 1. - 4. there are $r, s, t, u, v \in X$ with $\mathrm{LM}(f_1) = rst$, $\mathrm{LM}(f_2) = stu$, $\mathrm{LM}(f_3) = tuv$. Hence we have $r_1 = uv$, $r_3 = rs$, $s_1 = u$, $s_2 = r$, $t_2 = v$, $t_3 = s$ and thus $\mathrm{LM}(f_1)u = r\mathrm{LM}(f_2)$, $\mathrm{LM}(f_2)v = s\mathrm{LM}(f_3)$. Now

$$\begin{aligned}
\mathrm{spoly}(f_1, f_3) =& c_{13}f_1r_1 - c_{31}r_3f_3 \\
=& c_{13}f_1uv - c_{31}rsf_3 + \frac{c_{31}c_{23}}{c_{32}}rf_2v - \frac{c_{31}c_{23}}{c_{32}}rf_2v \\
=& c_{13}f_1uv - c_{31}rsf_3 + \frac{c_{31}c_{23}}{c_{32}}rf_2t_2 - \frac{c_{13}c_{21}}{c_{12}}s_2f_2v \\
=& \frac{c_{31}}{c_{32}}r(c_{23}f_2t_2 - c_{32}t_3f_3) + \frac{c_{13}}{c_{12}}(c_{12}f_1s_1 - c_{21}s_2f_2)v \\
=& \frac{c_{31}}{c_{32}}r\mathrm{spoly}(f_2, f_3) + \frac{c_{13}}{c_{12}}\mathrm{spoly}(f_1, f_2)v
\end{aligned}$$

reduces to zero. □

Moreover, if

1. $\mathrm{LM}(f_1)r_1 = r_3\mathrm{LM}(f_3)$,
2. $\mathrm{LM}(f_1)s_1 = s_2\mathrm{LM}(f_2)$,
3. $\mathrm{LM}(f_2)t_2 = t_3\mathrm{LM}(f_3)$,
4. $\mathrm{LM}(f_2)$ divides $\mathrm{LM}(f_1)r_1 = r_3\mathrm{LM}(f_3)$ and
5. $\mathrm{LC}(f_2) \mid \gcd(\mathrm{LC}(f_1), \mathrm{LC}(f_3))$,

then the corresponding G-polynomial $\mathrm{gpoly}(f_1, f_3)$ reduces to zero.

Proof.
With the above notations from the proof of the chain criterion for S-polynomials let $w := r \otimes v \in \mathcal{P}^e$, $\gcd(\mathrm{LC}(f_1), \mathrm{LC}(f_3)) = b_1\mathrm{LC}(f_1) + b_3\mathrm{LC}(f_3)$ and

$$d := \frac{\gcd(\mathrm{LC}(f_1), \mathrm{LC}(f_3))}{\mathrm{LC}(f_2)} \in \mathcal{R}.$$

Then $dw\mathrm{LT}(f_2) = \gcd(\mathrm{LC}(f_1), \mathrm{LC}(f_3))\mathrm{LM}(f_1)r_1$ and

$$\begin{aligned}
&\mathrm{gpoly}(f_1, f_3) - dwf_2 - b_1\,\mathrm{spoly}(f_1, f_2)v + b_3 r\,\mathrm{spoly}(f_2, f_3)\\
=&b_1 f_1 r_1 + b_3 r_3 f_3 - dr f_2 v - b_1 f_1 s_1 v + b_1 c_{21} s_2 f_2 v - b_3 c_{23} r f_2 t_2 + b_3 r t_3 f_3\\
=&b_1\,\mathrm{tail}(f_1)uv + b_3 rs\,\mathrm{tail}(f_3) - dr\,\mathrm{tail}(f_2)v\\
&- b_1\,\mathrm{tail}(f_1)uv + b_1 c_{21} r\,\mathrm{tail}(f_2)v + b_3 c_{23} r\,\mathrm{tail}(f_2)v - b_3 rs\,\mathrm{tail}(f_3)\\
=&-dr\,\mathrm{tail}(f_2))v + b_1 c_{21} r\,\mathrm{tail}(f_2)v + b_3 c_{23} r\,\mathrm{tail}(f_2)v\\
=&\underbrace{(b_1 c_{21} + b_3 c_{23} - d)}_{=0} r\,\mathrm{tail}(f_2)v,
\end{aligned}$$

because $\mathrm{LC}(f_2)c_{21} = \mathrm{LC}(f_1)$, $\mathrm{LC}(f_2)c_{23} = \mathrm{LC}(f_3)$. Hence $\mathrm{gpoly}(f_1, f_3)$ has a strong Gröbner representation. □

We have seen the basic idea of these two proofs several times but under the given hypothesis it becomes much clearer. Obviously this works for any permutation of 1, 2, 3 and these are all cases we need to consider to have an analogues statement to the chain criterion in the commutative situation.
$\mathcal{LP}$-version: Let $f_1, f_2, f_3 \in \mathcal{LP}$ with

1. $\mathrm{LM}(f_1) \times_{\mathcal{LP}} r_1 = r_3 \times_{\mathcal{LP}} \mathrm{LM}(f_3)$,
2. $\mathrm{LM}(f_1) \times_{\mathcal{LP}} s_1 = s_2 \times_{\mathcal{LP}} \mathrm{LM}(f_2)$,
3. $\mathrm{LM}(f_2) \times_{\mathcal{LP}} t_2 = t_3 \times_{\mathcal{LP}} \mathrm{LM}(f_3)$,
4. $\mathrm{LM}(f_2) \mid_{\mathcal{LP}} \mathrm{LM}(f_1) \times_{\mathcal{LP}} r_1 = r_3\mathrm{LM}(f_3)$ and
5. $\mathrm{LC}(f_2) \mid \mathrm{lcm}(\mathrm{LC}(f_1), \mathrm{LC}(f_3))$

for Letterplace monomials $r_1, r_3, s_1, s_2, t_2, t_3$. Let $f_2' = \textsc{LmShift}(f_2, |s_2|)$, $f_3' = \textsc{LmShift}(f_3, |t_3|)$ and $f_3'' = \textsc{LmShift}(f_3, |r_3|)$. If $\textsc{Spoly}(f_1, f_2')$ and $\textsc{Spoly}(f_2, f_3')$ have been declared as useless for the procedure, then so is $\textsc{Spoly}(f_1, f_3'')$.
Moreover, if

1. $\mathrm{LM}(f_1) \times_{\mathcal{LP}} r_1 = r_3 \times_{\mathcal{LP}} \mathrm{LM}(f_3)$,
2. $\mathrm{LM}(f_1) \times_{\mathcal{LP}} s_1 = s_2 \times_{\mathcal{LP}} \mathrm{LM}(f_2)$,
3. $\mathrm{LM}(f_2) \times_{\mathcal{LP}} t_2 = t_3 \times_{\mathcal{LP}} \mathrm{LM}(f_3)$,
4. $\mathrm{LM}(f_2) \mid_{\mathcal{LP}} \mathrm{LM}(f_1) \times_{\mathcal{LP}} r_1 = r_3\mathrm{LM}(f_3)$ and
5. $\mathrm{LC}(f_2) \mid \gcd(\mathrm{LC}(f_1), \mathrm{LC}(f_3))$

for Letterplace monomials $r_1, r_3, s_1, s_2, t_2, t_3$, then $\textsc{Gpoly}(f_1, f_3'')$ is redundant to Algorithm 7.28 with $f_3'' = \textsc{LmShift}(f_3, |r_3|)$.

Lemma 7.33.
If $t = \mathrm{LM}(f)$ is divisible by $\mathrm{LM}(g)$ then the only first type S- and G-polynomials w.r.t. t are $\mathrm{spoly}_1^t(f, g)$ and $\mathrm{gpoly}_1^t(f, g)$. However, these two are not uniquely determined. Moreover, if $t = \mathrm{LM}(f) = \mathrm{LM}(g)$, then $\langle f, g\rangle = \langle \mathrm{spoly}_1^t(f, g), \mathrm{gpoly}_1^t(f, g)\rangle$. In this case $\mathrm{spoly}_1^t(f, g)$ and $\mathrm{gpoly}_1^t(f, g)$ are unique. This does not include the case where t has non-trivial self overlap.

For the criteria to be applied in the algorithm explicitly, we will modify the InsertPair-procedure and change the sets of triples L to a set of quintuples, such that the fourth and fifth entries are boolean values which indicate, whether a pair is redundant by one of the criteria ("done") or not ("to do"). The problem is that a pair might have an S-polynomial that reduces to zero, i.e. is redundant, but on the other hand have a G-polynomial that is required, which is why we need two boolean values instead of one, as in the field case. We, therefore, replace the following lines in Algorithm 7.28.

03′: $L = \{(0, 0, f_i \mid \text{"to do"}, \text{"to do"}) \mid 1 \leq i \leq k\}$
04′: **while** $\{(a, b, h \mid B_1, B_2) \in L \mid B_1 = \text{"to do" or } B_2 = \text{"to do"}\} \neq \emptyset$ **do**
05′: choose $(a, b, h \mid B_1, B_2) \in L$
06′: $L = L \setminus \{(a, b, h \mid B_1, B_2)\}$

11′a: **for** $j \in \{1, 2\}$ **do**
11′b: **if** $B_j =$ "to do" **then**

24′: $L = \mathrm{InsertPair}_j(g, w'h', B_1, B_2, L)$
27′: $L = \mathrm{InsertPair}_j(g, h', B_1, B_2, L)$
35′: $L = \mathrm{InsertPair}_j(h, w'g', B_1, B_2, L)$
38′: $L = \mathrm{InsertPair}_j(h, g', B_1, B_2, L)$

42′a: **else**
42′b: $B_j =$ "done"
42′c: **end if**

B_1 indicates if an S-polynomial (h_1) is "done", while B_2 stands for G-polynomials. The procedure InsertPair is also replaced.

$\mathrm{InsertPair}_1$

---

input: $f, g \in \mathcal{LP}$, B_1, B_2 boolean values, $L \subseteq \mathcal{LP}^{1\times 5}$
output: a superset of L
01: $t = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$
02: **if** t is a Letterplace monomial **then**
03: **if** $t = \mathrm{LM}(f)\mathrm{LM}(g)$, $\mathrm{LC}(f)$, $\mathrm{LC}(g)$ coprime and (
$\mathrm{LC}(f)\mathrm{LC}(\mathrm{tail}(g)) \neq \mathrm{LC}(g)\mathrm{LC}(\mathrm{tail}(f))$ or
$\deg(f) - \deg(\mathrm{tail}(f)) \neq \deg(g) - \deg(\mathrm{tail}(g))$)
then

04: $L = L \cup \{(f,\, g,\, 0 \mid \text{“done”},\, B_2)\}$
05: **else if** $\exists (f,\, p',\, 0, \mid \text{“done”},\, \tilde{B}_2),\, (p,\, g,\, 0, \mid \text{“done”},\, \hat{B}_2) \in L$ with
$p' = \text{LmShift}(p,\, \deg(f))$,
$\text{LC}(p) \mid \text{lcm}(\text{LC}(f),\, \text{LC}(g))$ and
$\text{LM}(p) \;\mid_{\mathcal{LP}} t$
then
06: $L = L \cup \{(f,\, g,\, 0 \mid \text{“done”},\, B_2)\}$
07: **else**
08: $L = L \cup \{(f,\, g,\, 0 \mid \text{“to do”},\, B_2)\}$
09: **end if**
10: **end if**
11: **return** L

In InsertPair$_1$ we check in line 03 for the product criterion and in line 05 for the chain criterion. The product criterion has different possibilities to be checked as we see in Lemma 7.31. The easiest ones in terms of computational effort are to use ℓ_f and ℓ_g or to look at the coefficients.

InsertPair$_2$

---

input: $f,\, g \in \mathcal{LP}$, B_1, B_2 boolean values, $L \subseteq \mathcal{LP}^{1\times 5}$
output: a superset of L
01: $t = \text{lcm}(\text{LM}(f),\, \text{LM}(g))$
02: **if** t is a Letterplace monomial **then**
03: **if** $\text{LC}(f) \mid \text{LC}(g)$ or $\text{LC}(g) \mid \text{LC}(f)$ **then**
04: $L = L \cup \{(f,\, g,\, 0 \mid B_1,\, \text{“done”})\}$
05: **else if** $\exists (f,\, p',\, 0, \mid \tilde{B}_1,\, \tilde{B}_2),\, (p,\, g,\, 0, \mid \hat{B}_1,\, \hat{B}_2) \in L$ with
$p' = \text{LmShift}(p,\, \deg(f))$,
$\text{LC}(p) \mid \gcd(\text{LC}(f),\, \text{LC}(g))$ and
$\text{LM}(p) \;\mid_{\mathcal{LP}} t$
then
06: $L = L \cup \{(f,\, g,\, 0 \mid B_1,\, \text{“done”})\}$
07: **else**
08: $L = L \cup \{(f,\, g,\, 0 \mid B_1,\, \text{“to do”})\}$
09: **end if**
10: **end if**
11: **return** L

Again we check in line 05 of InsertPair for the chain criterion for G-polynomials. In line 03 we apply the fact, that a G-polynomial reduces to zero, if one of the leading coefficients divides the other.
Another improvement can be made by relaxing the ending criterion of the while loop. We had a similar statement in chapter 5.

Lemma 7.34.
Let $\mathcal{G} \subseteq \mathcal{P} \setminus \{0\}$ and $\mathcal{I} \subseteq \mathcal{P}$ be an ideal. The following are equivalent.

1. $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$.
2. Let $f, g \in \mathcal{I} \setminus \{0\}$. If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$ or $\mathrm{LC}(g) \mid \mathrm{LC}(f)$, then every first and second type S-polynomial reduces to zero. If on the other hand $\mathrm{LC}(f) \nmid \mathrm{LC}(g)$ and $\mathrm{LC}(g) \nmid \mathrm{LC}(f)$, then every first and second type G-polynomial reduces to zero.

Proof.
If $\mathcal{G}$ is a strong Gröbner basis for $\mathcal{I}$, then every first and second type S- and G-polynomial reduces to zero by 7.21.
Now let $f, g \in \mathcal{G}$ with $\mathrm{LM}(f)t_f = t_g\mathrm{LM}(g)$. Then the corresponding S- and G-polynomial are

$$\begin{aligned}\mathrm{spoly}(f, g) &= a_f \,\mathrm{tail}t_f - a_g t_g \,\mathrm{tail}(g)\\ \mathrm{gpoly}(f, g) &= dt + b_f \,\mathrm{tail}t_f + b_g t_g \,\mathrm{tail}(g)\end{aligned}$$

and are of first or second type with $d = \gcd(\mathrm{LC}(f), \mathrm{LC}(g))$. If $\mathrm{LC}(f) \mid \mathrm{LC}(g)$ or $\mathrm{LC}(g) \mid \mathrm{LC}(f)$, then the G-polynomial reduces to zero and so does the S-polynomial by 2. If on the other hand $\mathrm{LC}(f) \nmid \mathrm{LC}(g)$ and $\mathrm{LC}(g) \nmid \mathrm{LC}(f)$ then according to 2. the G-polynomial reduces to zero and we have $a_f b_g + a_g b_f = 1$, as well as

$$\mathrm{spoly}(f, \mathrm{gpoly}(f, g)) := ft_f - a_g\mathrm{gpoly}(f, g) = b_g\mathrm{spoly}(f, g)$$

and

$$\mathrm{spoly}(\mathrm{gpoly}(f, g), g) := a_f\mathrm{gpoly}(f, g) - t_g g = b_f\mathrm{spoly}(f, g)$$

are S-polynomials of first or second type and we can construct a first or second type G-polynomial

$$\begin{aligned}&\mathrm{gpoly}(\mathrm{spoly}(f, \mathrm{gpoly}(f, g)), \mathrm{spoly}(\mathrm{gpoly}(f, g), g))\\ :=& a_f b_g\mathrm{spoly}(f, g) + a_g b_f\mathrm{spoly}(f, g)\\ =& \mathrm{spoly}(f, g)\end{aligned}$$

which reduces to zero. We have the analogous statement for $\mathrm{LM}(f) = t_g\mathrm{LM}(g)t'_g$ or for f, g interchanged. □

Thus the boolean value B_1 only needs to be "done", when $\mathrm{LC}(f) \mid \mathrm{LC}(g)$ or $\mathrm{LC}(g) \mid \mathrm{LC}(f)$. Simultaneously B_2 only needs to be "done", when $\mathrm{LC}(f) \nmid \mathrm{LC}(g)$ and $\mathrm{LC}(g) \nmid \mathrm{LC}(f)$.
When $\mathcal{R}$ is not a Euclidean domain, but we want to consider $(\mathbb{Z}/m\mathbb{Z})$ for some non-zero $m \in \mathbb{Z}$, not a unit and not prime, then we can use factorizations of m as we have seen in chapter 6. Recall that a factorization of m, say $m = ab$, implies that $xy \neq m$ for $a \nmid x \mid a$, $b \nmid y \mid b$. Suppose that $cx = a$, $dy = b$ and for a contradiction $xy = m$. Then $m = ab = cdxy = cdm$ and thus $m(1 - cd) = 0$ which implies $1 = cd$, because $\mathcal{R}$ is a commutative domain. But then c is a unit contradicting $a \nmid x$. This was easy to see but means that we have to choose our coefficients wisely when using lifting methods.

Lemma 7.35.
Let $\mathcal{R}$ be a Euclidean domain and $m = ab \in \mathcal{R}$ with a, b coprime such that $ar + bs = 1$ for some r, $s \in \mathcal{R}$. Then there are canonical projections $\pi : \mathcal{R}[X] \to (\mathcal{R}/m\mathcal{R})[X]$, as well as

$$\pi_a : (\mathcal{R}/m\mathcal{R})\langle X\rangle \cong (a\mathcal{R} + b\mathcal{R})/m\mathcal{R}\langle X\rangle \to (\mathcal{R}/a\mathcal{R})\langle X\rangle$$

and

$$\pi_b : (\mathcal{R}/m\mathcal{R})\langle X\rangle \cong (a\mathcal{R} + b\mathcal{R})/m\mathcal{R}\langle X\rangle \to (\mathcal{R}/b\mathcal{R})\langle X\rangle.$$

For an ideal $\mathcal{I}$ of $(\mathcal{R}/m\mathcal{R})\langle X\rangle =: \overline{\mathcal{P}}$, we assume that there exist countable sets $\mathcal{G}_a = \{g_{a,i}\}_i$, $\mathcal{G}_b = \{g_{b,j}\}_j \subseteq \overline{\mathcal{P}}$, such that $\pi_a(\mathcal{G}_a)$ is a strong Gröbner basis for $\pi_a(\mathcal{I})$ and $\pi_b(\mathcal{G}_b)$ is a strong Gröbner basis for $\pi_b(\mathcal{I})$. Additionally let $\pi(a) \in \mathcal{G}_a$, $\pi(b) \in \mathcal{G}_b$, $\pi(a) \nmid \mathrm{LC}(g_{a,i}) \mid \pi(a)$ for $g_{a,i} \neq \pi(a)$ and $\pi(b) \nmid \mathrm{LC}(g_{b,j}) \mid \pi(b)$ for $g_{b,j} \neq \pi(b)$. Recall that this implies that the leading coefficients are non-trivial zero divisors in the respective quotient rings. For every pair i, j there exist monomials $\tau_{i,j}$, $\tau_{j,i} \in \mathcal{P}^e$ such that $\tau_{i,j}\mathrm{LM}(g_{a,i}) = \tau_{j,i}\mathrm{LM}(g_{b,j})$ and

1. $\tau_{i,j} = 1 \otimes x'$, $\tau_{j,i} = y \otimes 1$ or
2. $\tau_{i,j} = x \otimes 1$, $\tau_{j,i} = 1 \otimes y'$ or
3. $\tau_{i,j} = 1 \otimes 1$, $\tau_{j,i} = y \otimes y'$ or
4. $\tau_{i,j} = x \otimes x'$, $\tau_{j,i} = 1 \otimes 1$

for monomials x, x', y, y'. These are precisely the overlap relations corresponding to first and second type S- and G-polynomials. We define

$$f_{i,j} := \pi(ar)\mathrm{LC}(g_{a,i})\tau_{j,i}g_{b,j} + \pi(bs)\mathrm{LC}(g_{b,j})\tau_{i,j}g_{a,i}.$$

Then $\mathcal{G} := \{f_{i,j} \mid \tau_{i,j}\mathrm{LM}(g_{a,i}) = \tau_{j,i}\mathrm{LM}(g_{b,j})\}$ is a strong Gröbner basis for $\mathcal{I}$.

Proof.
The proof is similarly to Corollary 6.8 a direct consequence of Theorem 6.4 and Theorem 6.6 which are proven in the non-commutative case analogously to the commutative one. □

Note that the $\tau_{i,j}$, $\tau_{j,i}$ are not uniquely determined since all overlap relations of the leading monomials have to be considered. The above lemma leads to similar algorithms as in chapter 6.

Conclusion and future work

Non-commutative Gröbner bases over rings lead to so far unknown phenomena and unsolved problems. It is possible to transfer ideas, statements and criteria from commutative Gröbner bases and the field case to this new situation under certain adjustments. Coefficients require the definition of G-polynomials and, in principal ideal rings, also A-polynomials. The lack of a general product criterion leads to infinitely many overlap relations of leading monomials, since we cannot simply ignore non-trivial overlap relations as in the field case. It is also possible in the field case to have an infinite Gröbner bases, but this is due to a boundless growing number of overlap relations where the product criterion excludes the trivial ones. Also, chain criteria are harder to apply, since they require a certain shape of leading monomials. On the other hand, we obtain much more pairs to be able to reduce newly constructed polynomials during Buchberger's algorithm. Example A.2 shows that we are computing much more S- and G-polynomials than in the commutative case or in the field case. There are many zero-reductions that are not predictable by the product or chain criterion. It is, therefore, necessary to find more criteria and also to choose pairs of which we compute S- and G-polynomials in order to be able to reduce further. A consequence of Example 7.22 and Example A.2 is the "blowing up"-effect of second type S- and G-polynomials spoly_2^w and gpoly_2^w, where $w \in X$ is the power product of a single letter, for example $w = x^\ell = x \cdots x$. We can see that these elements are not reducible. For every other shape of $w \in X$, we need, due to the lack of criteria, an option to choose pairs efficiently in order to minimize computational effort. The implementations of Buchberger's algorithm using Singular:Letterplace [25] are expected to give fruitful results and new insights on this behaviour.

It is useful from an implementational point of view not to exclude too many pairs, so that we have more possibilities of reduction. The implementation of Algorithm 7.28 without criteria needs to be tested, before we can engage the search for new criteria and strategies. Moreover, it is desirable to find a closed expression for an infinite Gröbner basis, for example $\mathcal{G} = \{2x,\, 3y\} \cup \{xz^iy,\, yz^ix \mid i \in \mathbb{N}\}$. As we have seen in Example 7.22, it is not easy to find such a pattern in more general cases.

Subject of future research will be Gröbner bases for bilateral modules, especially for submodules of $(\mathcal{P}^e)^n = (\mathcal{P} \otimes \mathcal{P}^{\mathrm{opp}})^n$ with $n \in \mathbb{N}_{>1}$ and finitely presented modules over $\mathbb{Z}$. For the commutative field case $(\mathbb{K}[X])^n$ this was done in [8], chapter 2, with Schreyer orderings. A great interest lies in finding criteria for algorithms to compute such bases in order to gain new insights on bilateral syzygy modules.

References

[1] Christian Eder, Gerhard Pfister, Adrian Popescu: *Standard Bases over Euclidean Domains*
arXiv.org, 2018
https://arxiv.org/abs/1811.05736

[2] Christian Eder, Gerhard Pfister, Adrian Popescu: *New strategies for Standard Bases over Z*
arXiv.org, 2016
https://arxiv.org/abs/1609.04257

[3] Christian Eder, Tommy Hofmann: *Efficient Gröbner Basis Computation over Principal Ideal Rings*
arXiv.org, 2019
https://arxiv.org/abs/1906.08543

[4] Viktor Levandovskyy: *Non-Commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementations*
Doctoral Thesis at TU Kaiserslautern, 2005
https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/1670

[5] Roberto La Scala, Viktor Levandovskyy: *Letterplace ideals and non-commutative Gröbner bases*
Journal of Symbolic Computation Vol. 44, pp. 1374–1393, sciencedirect.com, 2009
https://www.sciencedirect.com/science/article/pii/S0747717109000637

[6] Daniel Lichtblau: *Effective computation of strong Gröbner bases over Euclidean domains*
Illinois Journal of Mathematics Vol. 56, pp. 177–194, projecteuclid.org, 2012
https://projecteuclid.org/euclid.ijm/1380287466

[7] F. Leon Pritchard: *The Ideal Membership Problem in Non-Commutative Polynomial Rings*
Journal of Symbolic Computation Vol. 22, pp. 27–48, sciencedirect.com, 1996
https://www.sciencedirect.com/science/article/pii/S0747717196900401

[8] Gert-Martin Greuel, Gerhard Pfister: *A Singular Introduction to Commutative Algebra*
Springer, 2007

[9] Dave Bayer, André Galligo, Mike Stillman: *Gröbner Bases and Extension of Scalars*
Symposia Mathematica Vol. 34, pp. 198–215, arXiv.org, 1993
https://arxiv.org/pdf/alg-geom/9202021.pdf

[10] Hideyuki Matsumura: *Commutative Ring Theory*
Cambridge studies in advanced mathematics, 1989

[11] Karim Abou Zeid: *Letterplace Gröbner Bases, their Implementation and Applications*
Bachelor thesis at RWTH Aachen University, 2019

[12] Grischa Studzinski: *Implementation and Applications of Fundamental Algorithms relying on Gröbner Bases in Free Associative Algebras*
Doctoral thesis at RWTH Aachen University, 2013
http://publications.rwth-aachen.de/record/228489

[13] E. S. Golod: *On Non-Commutative Gröbner Bases over Rings*
Journal of Mathematical Sciences Vol. 140, No. 2, pp. 239–242, researchgate.net, 2007
https://www.researchgate.net/publication/225545350

[14] Teo Mora: *Solving Polynomial Equation Systems IV - Buchberger's Theory and Beyond*
Cambridge University Press, 2015

[15] Teo Mora: *Gröbner bases for non-commutative rings*
L. N. Comp. Sci. Vol. 229, pp. 353–362, 1985

[16] Franz Pauer: *Gröbner Bases with Coefficients in Rings*
Journal of Symbolic Computation, Vol. 42, pp. 1003–1011, sciencedirect.com, 2007
https://www.sciencedirect.com/science/article/pii/S0747717107001022

[17] Äbdelilah Kandri-Rody, Deepak Kapur: *Computing a Gröbner basis of a polynomial ideal over a Euclidean domain*
Journal of Symbolic Computation Vol. 6, pp. 37–57, sciencedirect.com, 1988
https://www.sciencedirect.com/science/article/pii/S0747717188800208

[18] Äbdelilah Kandri-Rody, Deepak Kapur: *Algorithms for Computing Gröbner bases of polynomial ideals over various Euclidean rings*
Springer, pp. 195–206, 1984

[19] Bruno Buchberger: *Gröbner-bases: An algorithmic method in polynomial ideal theory*
Reidel Publishing Company, pp. 1084–2322, 1985

[20] Eva Zerz: *Computeralgebra*
Lecture script at RWTH Aachen, 2012

[21] Eva Zerz: *Commutative Algebra*
Lecture script at RWTH Aachen, 2013

[22] Eva Zerz: *Algebraic Systems Theory*
Lecture script at RWTH Aachen, 2015

[23] Joachim Apel: *Computational ideal theory in finitely generated extension rings*
Theoretical Computer Science Vol. 244, pp. 1–33, sciencedirect.com, 2000
https://www.sciencedirect.com/science/article/pii/S0304397500001729

[24] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, Hans Schönemann: SINGULAR 4-1-2 – *A computer algebra system for polynomial computations*
TU Kaiserslautern, 2019
http://www.singular.uni-kl.de

[25] Viktor Levandovskyy, Karim Abou Zeid, Hans Schönemann: SINGULAR:LETTERPLACE – *A* SINGULAR 4-1-2 *Subsystem for Non-commutative Finitely Presented Algebras*
TU Kaiserslautern & RWTH Aachen, 2019
http://www.singular.uni-kl.de

A Appendix

Example A.1. (ad Example 7.22)
Recall Example 7.22, where we considered $\langle 2x,\, 3y\rangle \subseteq \mathbb{Z}\langle x,\, y,\, z\rangle$ with the graded left lexicographical ordering. Then every S-polynomial of the generators is zero and every G-polynomial of $2x$, $3y$ is of second type and contained in one of the sets xX_ny given as follows.

$$xX_0y = \{xy\}$$

$$xX_1y = \{xxy,\, xyy,\, xzy\}$$

$$xX_2y = \{xxxy,\, xxyy,\, xxzy,\, xyxy,\, xyyy,\, xyzy,\, xzxy,\, xzyy,\, xzzy\}$$

$$\begin{aligned} xX_3y = \{&xxxxy,\, xxxyy,\, xxxzy,\, xxyxy,\, xxyyy,\, xxyzy,\, xxzxy,\, xxzyy,\, xxzzy,\\ &xyxxy,\, xyxyy,\, xyxzy,\, xyyxy,\, xyyyy,\, xyyzy,\, xyzxy,\, xyzyy,\, xyzzy,\\ &xzxxy,\, xzxyy,\, xzxzy,\, xzyxy,\, xzyyy,\, xzyzy,\, xzzxy,\, xzzyy,\, xzzzy\} \end{aligned}$$

$$\begin{aligned} xX_4y = \{&xxxxxy,\, xxxxyy,\, xxxxzy,\, xxxyxy,\, xxxyyy,\, xxxyzy,\, xxxzxy,\, xxxzyy,\, xxxzzy,\\ &xxyxxy,\, xxyxyy,\, xxyxzy,\, xxyyxy,\, xxyyyy,\, xxyyzy,\, xxyzxy,\, xxyzyy,\, xxyzzy,\\ &xxzxxy,\, xxzxyy,\, xxzxzy,\, xxzyxy,\, xxzyyy,\, xxzyzy,\, xxzzxy,\, xxzzyy,\, xxzzzy,\\ &xyxxxy,\, xyxxyy,\, xyxxzy,\, xyxyxy,\, xyxyyy,\, xyxyzy,\, xyxzxy,\, xyxzyy,\, xyxzzy,\\ &xyyxxy,\, xyyxyy,\, xyyxzy,\, xyyyxy,\, xyyyyy,\, xyyyzy,\, xyyzxy,\, xyyzyy,\, xyyzzy,\\ &xyzxxy,\, xyzxyy,\, xyzxzy,\, xyzyxy,\, xyzyyy,\, xyzyzy,\, xyzzxy,\, xyzzyy,\, xyzzzy,\\ &xzxxxy,\, xzxxyy,\, xzxxzy,\, xzxyxy,\, xzxyyy,\, xzxyzy,\, xzxzxy,\, xzxzyy,\, xzxzzy,\\ &xzyxxy,\, xzyxyy,\, xzyxzy,\, xzyyxy,\, xzyyyy,\, xzyyzy,\, xzyzxy,\, xzyzyy,\, xzyzzy,\\ &xzzxxy,\, xzzxyy,\, xzzxzy,\, xzzyxy,\, xzzyyy,\, xzzyzy,\, xzzzxy,\, xzzzyy,\, xzzzzy\} \end{aligned}$$

The set X_n contains all monomials in X of length n and has cardinality 3^n. But if we compute a strong Gröbner basis with Algorithm 7.20, then every element of xX_ny reduces to zero w.r.t. elements of $xX_0y \cup \ldots \cup xX_{n-1}y$, except $xz\cdots zy$. Equivalently every element of yX_nx reduces to zero, except $yz\cdots zx$.

Example A.2. (Exemplary Calculation of a strong Gröbner basis with Buchbergers Algorithm up to a degree-bound)
Let $f_1 = 6xy + 2$, $f_2 = 4yz$ and $\mathcal{I} = \langle f_1,\, f_2\rangle$.

First case: $\mathcal{I} \subseteq \mathbb{Z}[x,\, y,\, z]$
// We follow the steps of Buchberger's algorithm 5.11.
$\mathcal{G} = \{f_1,\, f_2\}$
$f_3 = \text{spoly}(f_1,\, f_2) = 2zf_1 - 3xf_2 = 4z$

// We already see that f_3 reduces f_2 to zero, thus f_2 is redundant.
$f_4 = \text{gpoly}(f_1,\, f_2) = zf_1 - xf_2 = 2xyz + 2z$
$\mathcal{L} = \{f_3,\, f_4\}$ is not empty.
Choose $f_3 \in \mathcal{L}$. // completely reduced and non-zero
// We do not compute any S- or G-polynomials involving f_2.
$f_5 = \text{spoly}(f_1,\, f_3) = 2zf_1 - 3xyf_3 = 4z = f_3$
$f_6 = \text{gpoly}(f_1,\, f_3) = zf_1 - xyf_3 = 2xyz + 2z = f_4$
$\mathcal{L} = \{f_3,\, f_4\}$
$\mathcal{G} = \{f_1,\, f_3\}$
// f_3 reduces to zero w.r.t. $\mathcal{G}$.
Choose $f_4 \in \mathcal{L}$. // completely reduced and non-zero
// $\text{LC}(f_4) = 2$ divides every leading coefficient of $\mathcal{G}$.
// Thus we do not need G-polynomials.
$f_7 = \text{spoly}(f_1,\, f_4) = zf_1 - 3f_4 = -4z = -f_3$
$f_8 = \text{spoly}(f_3,\, f_4) = xyf_3 - 2f_4 = -4z = -f_3$
$\mathcal{L} = \{f_3,\, f_4\}$
$\mathcal{G} = \{f_1,\, f_3,\, f_4\}$
// Every element of $\mathcal{L}$ reduces to zero w.r.t. $\mathcal{G}$.
// $\mathcal{G} = \{6xy + 2,\, 4z,\, 2xyz + 2z\}$ is a strong Gröbner basis for $\mathcal{I}$.

Second case: $\mathcal{I} \subseteq \mathbb{Q}\langle x,\, y,\, z\rangle$
// Extract contents.
$f_1 = 3xy + 1$
$f_2 = yz$
// We only need first type S-polynomials due to the product criterion over fields.
$f_3 = \text{spoly}_1^{xyz}(f_1,\, f_2) = f_1z - 3xf_2 = z$
// As above, f_2 is redundant.
// There is no first type S-polynomial $\text{spoly}_1^t(f_2,\, f_1)$.
$\mathcal{L} = \{f_3\}$
Choose $f_3 \in \mathcal{L}$ // completely reduced and non-zero
// $\text{LM}(f_1)$, $\text{LM}(f_3)$ have no overlap, the S-polynomial will reduce to zero.
$\mathcal{G} = \{f_1,\, f_3\}$
// $\mathcal{G} = \{3xy + 1,\, z\}$ is a Gröbner basis for $\mathcal{I}$ and finite, as expected.

Third case: $\mathcal{I} \subseteq \mathbb{Z}\langle x,\, y,\, z\rangle$
As a degree bound we choose $d := 5$ and our global monomial ordering shall be the graded lexicographical one with $x \succ y \succ z$.
$\mathcal{G} = \{f_1,\, f_2\}$
$\mathcal{L} = \emptyset$
// We only compute the S-polynomials which are non-zero.
$f_3 = \text{gpoly}_1^{xyz}(f_1,\, f_2) = f_1z - xf_2 = 2xyz + 2z$
$f_4 = \text{gpoly}_2^{1}(f_1,\, f_2) = f_1yz - xyf_2 = 2xyyz + 2yz$
$f_5 = \text{gpoly}_2^{x}(f_1,\, f_2) = f_1xyz - xyxf_2 = 2xyxyz + 2xyz = xyf_3$
$f_6 = \text{gpoly}_2^{y}(f_1,\, f_2) = f_1yyz - xyyf_2 = 2xyyyz + 2yyz$
$f_7 = \text{gpoly}_2^{z}(f_1,\, f_2) = f_1zyz - xyzf_2 = 2xyzyz + 2zyz = f_3yz$

$f_8 = \mathrm{gpoly}_2^1(f_2,\, f_1) = -f_2xy + yzf_1 = 2yzxy + 2yz$
$f_9 = \mathrm{gpoly}_2^x(f_2,\, f_1) = -f_2xxy + yzxf_1 = 2yzxxy + 2yzx$
$f_{10} = \mathrm{gpoly}_2^y(f_2,\, f_1) = -f_2yxy + yzyf_1 = 2yzyxy + 2yzy$
$f_{11} = \mathrm{gpoly}_2^z(f_2,\, f_1) = -f_2zxy + yzzf_1 = 2yzzxy + 2yzz$
$f_{12} = \mathrm{spoly}_1^{xyz}(f_1,\, f_2) = 2f_1z - 3xf_2 = 4z$
$f_{13} = \mathrm{spoly}_2^1(f_1,\, f_2) = 2f_1yz - 3xyf_2 = 4yz = yf_{12}$
$f_{14} = \mathrm{spoly}_2^x(f_1,\, f_2) = 2f_1xyz - 3xyxf_2 = 4xyz = xyf_{12}$
$f_{15} = \mathrm{spoly}_2^y(f_1,\, f_2) = 2f_1yyz - 3xyyf_2 = 4yyz = yyf_{12}$
$f_{16} = \mathrm{spoly}_2^z(f_1,\, f_2) = 2f_1zyz - 3xyzf_2 = 4zyz = zyf_{12}$
$f_{17} = \mathrm{spoly}_2^1(f_2,\, f_1) = -3f_2xy + 2yzf_1 = 4yz = yf_{12}$
$f_{18} = \mathrm{spoly}_2^x(f_2,\, f_1) = -3f_2xxy + 2yzxf_1 = 4yzx = yf_{12}x$
$f_{19} = \mathrm{spoly}_2^y(f_2,\, f_1) = -3f_2yxy + 2yzyf_1 = 4yzy = yf_{12}y$
$f_{20} = \mathrm{spoly}_2^z(f_2,\, f_1) = -3f_2zxy + 2yzzf_1 = 4yzz = yf_{12}y$
$\mathcal{L} = \{f_3,\, \ldots,\, f_{20}\}$
// We add all elements to $\mathcal{G}$, that do not reduce to zero.
// Moreover, we can remove f_2 from $\mathcal{G}$, because $f_2 = yf_{12}$.
$\mathcal{G} = \{f_1,\, f_3,\, f_4,\, f_6,\, f_8,\, f_9,\, f_{10},\, f_{11},\, f_{12}\}$.
// This was the first iteration of Algortihm 7.20
// Furthermore, we compute the S- and G-polynomials of all these elements with each other.
$f_{21} = \mathrm{gpoly}_2^1(f_1,\, f_{12}) = f_1z - xyf_{12} = 2xyz + 2z = f_3$
$f_{22} = \mathrm{gpoly}_2^1(f_{12},\, f_1) = -f_{12}xy + zf_1 = 2zxy + 2z$
$f_{23} = \mathrm{gpoly}_2^x(f_{12},\, f_1) = -f_{12}xxy + zxf_1 = 2zxxy + 2zx$
$f_{24} = \mathrm{gpoly}_2^y(f_{12},\, f_1) = -f_{12}yxy + zyf_1 = 2zyxy + 2zy = f_{22}y$
$f_{25} = \mathrm{gpoly}_2^z(f_{12},\, f_1) = -f_{12}zxy + zzf_1 = 2zzxy + 2zz = zf_{22}$
// etc.
// All other new G-polynomials will reduce to zero by Remark 7.10, except
$f_{26} = \mathrm{spoly}_1^{xyz}(f_1,\, f_3) = -f_1z + 3f_3 = 4z = f_{12}$
$f_{27} = \mathrm{spoly}_2^1(f_1,\, f_3) = -f_1xyz + 3xyf_3 = 4xyz = xyf_{12}$
$f''_{28} = \mathrm{spoly}_2^1(f_3,\, f_1) = 3f_3xy - xyzf_1 = 6zxy - 2xyz$ // which is reducible to
$f'_{28} = -f''_{28} + f_{12}xy = 2xyz - 2zxy$.
// Note at this point, that in the field case f'_{28} would reduce to zero w.r.t. f_{12},
// because then $\mathrm{LC}(f_{12}) = 4 \sim 1$ is a unit.
// In the commutative case on the other hand we would clearly have $f'_{28} = 0$.
// However, we can reduce further on.
$f_{28} = -f'_{28} + f_3 = 2zxy + 2z = f_{22}$
$f_{29} = \ldots$
// We continue with computing all possible combinations of S- and G-polynomials for the elements of $\mathcal{L}$ up to degree 5.
// No reduction can be expected in the case of a leading monomial of shape $\bullet x \cdots x\bullet$, $\bullet y \cdots y\bullet$ or $\bullet z \cdots z\bullet$ which will be infinitely many.