Syzygienberechnung über nicht-kommutativen Polynomringen

Diplomarbeit

im Studiengang Mathematik
angefertigt am Fachbereich Mathematik
der Universität Dortmund

von

Holger Bluhm

Dortmund, Mai 2005

Betreuer: Prof. Dr. Martin Kreuzer

Inhaltsverzeichnis

Kapitel 1

Einleitung

Die Theorie der *Syzygien* stellt einen zentralen Bereich der Computeralgebra dar. In der kommutativen Computeralgebra ist dabei die folgende Situation gegeben. Sei $\{x_1, \ldots, x_n\}$ eine Menge von Unbestimmten, sei $P = K[x_1, \ldots, x_n]$ der Polynomring über einem Körper K und P^r ein endlich erzeugter freier P-Modul. Für Elemente $g_1, \ldots, g_s \in P^r$ ist eine Syzygie des Tupels $\mathcal{G} = (g_1, \ldots, g_s)$ nun definiert als ein Tupel $(f_1, \ldots, f_s) \in P^s$, das die Relation $f_1 g_1 + \ldots + f_s g_s = 0$ erfüllt. Die Menge dieser Elemente besitzt zudem eine P-Modulstruktur und wird deshalb der Syzygienmodul von $\mathcal{G}$ genannt. Das Thema der Syzygienberechnung ist für den kommutativen Fall bereits ausführlich behandelt worden. So finden sich die theoretischen Grundlagen und Algorithmen zur Berechnung von Syzygien z.B. bei Kreuzer und Robbiano ([5]). Hier wird in diesem Zusammenhang auch die Theorie der *Gröbnerbasen* für P-Untermoduln von P^r detailliert beschrieben. Diese ermöglicht es, für P-Moduln Erzeugendensysteme mit besonderen Eigenschaften anzugeben. So lässt sich z.B. jeder Leitterm eines Elements in P^r durch die Leitterme der Gröbnerbasiselemente darstellen.

Diese Arbeit soll sich nun zentral mit der Frage beschäftigen, in wie weit sich die Erkenntnisse zu den Themen Gröbnerbasen und Syzygienberechnung auf den nicht-kommutativen Fall übertragen lassen. Hierbei stellt sich zunächst die Frage, welche algebraische Struktur den Untersuchungen zu Grunde liegen soll. Aufgrund der fehlenden Kommutativität ist in unserer Situation zwischen der Multiplikation von rechts und von links mit nichtkommutativen Polynomen zu unterscheiden, d.h. zwischen freien rechtsseitigen, linksseitigen und zweiseitigen Moduln. Für die Gröbnerbasistheorie von Rechtsmoduln verweisen wir auf Green ([3]) bzw. auf Ackermann und Kreuzer ([1]). Wir wollen uns in dieser Arbeit aber mit freien zweiseitigen Moduln beschäftigen. Diese wurden in bisherigen Betrachtungen noch nicht berücksichtigt. D.h. die im Folgenden erarbeiteten Aussagen bilden die Grundlage

für weitere Untersuchungen zu diesem Thema. Die Konstruktion des freien zweiseitigen Moduls basiert dabei auf dem Tensorprodukt. Ist $K[\Sigma^*]$ der nicht-kommutative Polynomring über einem von $\Sigma = \{x_1, \ldots, x_n\}$ erzeugten nicht-kommutativen Monoid Σ^*, so besitzt $K[\Sigma^*] \otimes_K K[\Sigma^*]$ zusammen mit einer zweiseitigen skalaren Multiplikation eine zweiseitige $K[\Sigma^*]$-Modulstruktur. Wir bezeichnen diesen Modul als den freien zweiseitigen $K[\Sigma^*]$-Modul F_1 vom Rang 1. Der freie zweiseitige $K[\Sigma^*]$-Modul F_r vom Rang r ist dann definiert als die direkte Summe $F_r = \bigoplus_{i=1}^{r} K[\Sigma^*] \otimes K[\Sigma^*]$. Für F_r schreiben wir zur besseren Verständlichkeit auch $\bigoplus_{i=1}^{r} K[\Sigma^*]e_iK[\Sigma^*]$. Der Modul F_r heißt dann der freie von $\{e_1, \ldots, e_r\}$ zweiseitig erzeugte $K[\Sigma^*]$-Modul.

Eine analoge Differenzierung muss bei dem Begriff der Syzygie erfolgen. Auch hier ist zu unterscheiden, ob die Elemente $g_1, \ldots, g_s$ von rechts, von links oder zweiseitig mit Polynomen multipliziert werden sollen, um die obige Relation zu erfüllen. Wir werden uns ausschließlich den zweiseitigen Syzygien widmen. Nun gestaltet sich die Definition einer solchen Syzygie im Vergleich zum kommutativen Fall etwas komplizierter. Wir betrachten dazu die Elemente $g_1 = x_1e_1$ und $g_2 = x_2x_1e_1 + x_1e_1x_2$. Durch die Gleichung $x_2g_1 + g_1x_2 - g_2 = 0$ ist dann eine Syzygie gegeben. An diesem Beispiel wird deutlich, dass ein Element g_i mehrfach in der obigen Relation enthalten sein kann. Eine zweiseitige Syzygie von $(g_1, \ldots, g_s)$ ist nun definiert als ein Element des freien von $\{\varepsilon_1, \ldots, \varepsilon_s\}$ zweiseitig erzeugten $K[\Sigma^*]$-Moduls E, welches mit dem Homomorphismus $\lambda : E \longrightarrow F_r$, $\varepsilon_i \mapsto g_i$ auf Null abgebildet wird. Der Syzygienmodul $\mathrm{Syz}(g_1, \ldots, g_s)$, ein zweiseitiger $K[\Sigma^*]$-Untermodul von E, ist demnach der Kern von λ.

Eine Motivation für die Untersuchung zweiseitiger Syzygien liefert eine praktische Anwendung aus dem Gebiet der Kryptographie. Wir betrachten dazu einen Monoidring $K[\mathcal{M}]$ und ein Public-Key-Kryptosystem mit öffentlichem Schlüssel $g_1 \in K[\mathcal{M}]$. Eine Person A möchte nun einer Person B eine Nachricht übermitteln. Person B wählt dazu einen geheimen Schlüssel $f \in K[\mathcal{M}]$ und sendet $g_2 = fg_1f^{-1}$ an Person A. Diese wiederum verschlüsselt ihre Nachricht mit g_2 und übermittelt sie an Person B, die sie durch ihre Kenntnis von f dechiffrieren kann. Das beschriebene Kryptosystem ist sicher, solange keine dritte Person aus g_2 und dem öffentlichen Schlüssel g_1 den geheimen Schlüssel f ermitteln kann. D.h. die Sicherheit des Systems hängt von der Schwierigkeit der Aufgabe ab, aus einem Element des Monoidrings $K[\mathcal{M}]$ und einem Konjugat den zugehörigen Konjugator zu bestimmen. Das beschriebene mathematische Problem wird auch das *Konjugationssuchproblem* in Monoidringen genannt.

Dieses Problem lässt sich auch mit der folgenden Sichtweise betrachten. Die Relation $g_2 = fg_1f^{-1}$ kann auch formuliert werden als die Gleichung

$fg_1 - g_2 f = 0$. Damit erfüllt das Element $f\varepsilon_1 - \varepsilon_2 f \in E$ die definierende Eigenschaft einer zweiseitigen Syzygie des Tupels (g_1, g_2). Das Lösen des Konjugationssuchproblems ist also äquivalent zu dem Problem, die zweiseitige Syzygie des Tupel (g_1, g_2) von obiger Gestalt zu berechnen.

Wir wollen nun zunächst eine kurze Übersicht darüber geben, wie wir bei der Erarbeitung der Gröbnerbasistheorie für Untermoduln freier zweiseitiger Moduln und der Syzygienberechnung vorgehen werden. Dabei sei an dieser Stelle angemerkt, dass wir uns beim Aufbau in Kapitel 2 und 3 an [5] orientieren.

In Kapitel 2 wird als Grundlage dieser Arbeit die Theorie der Gröbnerbasen für Untermoduln freier zweiseitiger Moduln eingeführt. Dazu befassen wir uns zuerst mit Termordnungen für freie zweiseitige Moduln. In diesem Kontext gelangen wir zu dem Begriff des Leitterms, der eine zentrale Rolle in der Definition einer Gröbnerbasis einnimmt. Die besonderen Eigenschaften einer solchen Gröbnerbasis verdeutlichen wir, indem wir die Zusammenhänge mit dem Divisionsalgorithmus und den Termersetzungssystemen studieren. Das zentrale Ergebnis stellt schließlich der Buchberger-Algorithmus dar, der das Aufzählen einer Gröbnerbasis ermöglicht.

In Kapitel 3 beschäftigen wir uns dann mit der Syzygienberechnung. Hierbei betrachten wir zunächst Syzygien von Tupeln aus Monomen, bevor wir das „Liften“ solcher Syzygien erklären. Anschließend gehen wir auf eine allgemeine Methode der Syzygienberechnung ein. Dabei ist ein Studium der Eliminationstheorie nötig, wobei insbesondere die Theorie der Komponenten-Elimination zur Anwendung kommt.

Kapitel 4 ist der Berechnung von zweiseitigen Syzygien über Restklassenringen von $K[\Sigma^*]$ gewidmet. Dazu werden wir eine Gröbnerbasistheorie für Restklassenmoduln erarbeiten. Die daraufhin getroffenen Aussagen zur Syzygienberechnung über Restklassenringen übertragen wir dann auf den Fall der Monoidringe, um letztlich alle Syzygien des Tupels $(g_1, g_2) \in K[\mathcal{M}]$ bestimmen zu können.

In Kapitel 5 geben wir abschließend einige interessante Fragestellungen an, die in dieser Arbeit nicht berücksichtigt werden konnten. So z.B. die Frage, wie unter allen Syzygien von (g_1, g_2) genau diejenige der Gestalt $f\varepsilon_1 - \varepsilon_2 f$ gefunden werden kann.

Nach dieser kurzen Übersicht über den Verlauf dieser Arbeit befassen wir uns nun etwas detaillierter mit den oben vorgestellten Themen der Kapitel 2 bis 4. Der erste Abschnitt des 2. Kapitels befasst sich mit Termordnungen auf dem Monoid der Terme Σ^* und dem dadurch induzierten Begriff des Leitterms. Dabei verstehen wir wie in der kommutativen Theorie unter einer Termordnung eine totale Ordnung, die zum einen ordnungstreu unter der zweiseitigen Multiplikation mit Termen ist und zum anderen eine Wohlord-

nung ist, d.h. dass jede absteigende Kette von Termen stationär wird. Es ist hierbei zu bemerken, dass nicht jede Termordnung auf dem kommutativen Monoid zugleich eine auf dem nicht-kommutativen darstellt. Ein Beispiel hierfür erhalten wir mit der lexikographischen Termordnung. Ist eine Termordnung σ gewählt, lässt sich nun jedes Element in $K[\Sigma^*]$ ordnen und der größte Term bzgl. σ, der sogenannte Leitterm, identifizieren.

Diese Begriffe lassen sich wie im kommutativen Fall auch auf Moduln übertragen. Die bereits beschriebene Konstruktion des freien zweiseitigen $K[\Sigma^*]$-Moduls F_r stellt dabei die Grundlage weiterer Betrachtungen dar. Im Folgenden befassen wir uns mit zweiseitigen Untermoduln M von F_r, wobei τ stets eine Termordnung auf der Menge der Terme $\mathbb{T}(F_r)$ von F_r ist. Die Leitterme aller Elemente in M bilden wieder einen zweiseitigen $K[\Sigma^*]$-Untermodul von F_r. Für diesen Leittermmodul $\mathrm{LT}_\sigma(M)$ lässt sich nun die Gültigkeit eines zentralen Ergebnisses aus der kommutativen Computeralgebra nachweisen. Die Aussage von Macaulays Basis-Theorem, dass die Restklassen der Terme in $\mathbb{T}(F_r)\backslash\mathrm{LT}_\tau(M)$ eine K-Basis von F_r/M bilden, gilt auch in unserer Situation. Im Gegensatz dazu fehlen in der nicht-kommutativen Theorie wichtige Resultate wie Dickson's Lemma und damit auch der Hilbert-Basis-Satz. Diese Tatsache zerstört nun jede Hoffnung auf die gesicherte Existenz endlicher Gröbnerbasen G von Moduln M. Diese sind im Übrigen analog zum kommutativen Fall definiert, d.h. die Leitterme der Elemente in G erzeugen den Leittermmodul von M. Das bedeutet aber nicht, dass Gröbnerbasen ihre besonderen Eigenschaften verlieren:

- Jedes Element $m \in M$ lässt sich in den Elementen von G darstellen, so dass jeder Summand einen durch $\mathrm{LT}_\tau(m)$ beschränkten Leitterm hat.
- Das von G induzierte Termersetzungssystem ist konvergent.
- Jedes Element in F_r besitzt eine eindeutige Normalform.
- Ein Element $m \in F_r$ reduziert genau dann zu Null, wenn $m \in M$ ist.
- Ist G endlich, so entsprichte der normale Rest im Divisionsalgorithmus der Normalform eines Elements.

Des Weiteren funktioniert der Buchberger-Algorithmus analog zur kommutativen Theorie. Der einzige Unterschied besteht darin, dass dieser nicht enden muss. Um auch Gröbnerbasen für zweiseitige Ideale I von $K[\Sigma^*]$ mit Erzeugendensystem $\{f_1, \ldots, f_s\}$ berechnen zu können, identifizieren wir ein Ideal eineindeutig mit einem Restklassenmodul eines Untermoduls von F_1. Der Hintergrund dieser komplizierteren Sichtweise ist der folgende. Es lässt sich einem Polynom in $K[\Sigma^*]$ nicht eineindeutig ein Element des Moduls F_1 zuordnen. Entspricht z.B. das Polynom x_1 dem Element x_1e_1 oder e_1x_1. Wir bilden deshalb Restklassenmoduln M_I/N mit dem zweiseitigen Untermodul $N = \langle x_ie_1 - e_1x_i \,|\, i = 1, \ldots, n\rangle$ von F_1. Nun haben die Elemente x_1e_1 und e_1x_1

dieselbe Restklasse. Dabei ist M_I der von $\{e_1 f_1, \ldots, e_1 f_s\}$ zweiseitig erzeugte Untermodul von F_1. Ist nun G eine Gröbnerbasis des Moduls $M_I + N$, so erhalten wir nach Anwendung des Homomorphismus $F_1 \longrightarrow K[\Sigma^*]$, $e_1 \mapsto 1$ auf die Elemente in G eine Gröbnerbasis von I.

In Kapitel 3 befassen wir uns mit dem Thema der Syzygienberechnung. Hier lassen sich zunächst die gleichen Ergebnisse wie in der kommutativen Theorie erzielen. Für Monome $m_1, \ldots, m_s \in F_r$ erhalten wir mit der Menge der Fundamentalsyzygien $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(m_i)} w_i \varepsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(m_j)} w_j \varepsilon_j w_j'$ ein endliches Erzeugendensystem des Syzygienmoduls von $(m_1, \ldots, m_s)$. Ist $\{g_1, \ldots, g_s\}$ eine Gröbnerbasis, so funktioniert auch in unserer Situation das sogenannte „Liften“ der Syzygien von $(\mathrm{LM}_\tau(g_1), \ldots, \mathrm{LM}_\tau(g_s))$. D.h. es lässt sich aus einem endlichen Erzeugendensytem von $\mathrm{Syz}(\mathrm{LM}_\tau(g_1), \ldots, \mathrm{LM}_\tau(g_s))$ ein solches für $\mathrm{Syz}(g_1, \ldots, g_s)$ konstruieren. Bildet hingegen $\{g_1, \ldots, g_s\}$ keine Gröbnerbasis, so stellt sich nun das folgende Problem. In der kommutativen Computeralgebra wird in diesem Fall zunächst eine endliche Gröbnerbasis G von $M = \langle g_1, \ldots, g_s \rangle$ zusammen mit einer Transformationsmatrix bestimmt. Den Elementen des Syzygienmoduls von G werden dann mittels der Matrix Syzygien von $(g_1, \ldots, g_s)$ zugeordnet. Diese Methode kann im nicht-kommutativen Fall so nicht umgesetzt werden. Dies scheitert an der Tatsache, dass der Modul M keine endliche Gröbnerbasis besitzen muss. Deshalb wählen wir eine andere Strategie, die wirklich übertragbar ist. Dabei betrachten wir sogenannte *Komponenten-Eliminationsordnungen*. Das sind Termordnungen mit der Eigenschaft, dass für ein Element in F_r, dessen Leitterm keinen der Erzeuger in $L \subseteq \{e_1, \ldots, e_r\}$ enthält, auch jeder andere Term diese nicht umfasst. Unter dem Komponenten-Eliminationsmodul von M bzgl. L verstehen wir dabei den zweiseitigen Untermodul von M, dessen Elemente keinen der Erzeuger in L enthalten. In diesem Kontext ergibt sich das zentrale Ergebnis, dass der Syzygienmodul $\mathrm{Syz}(g_1, \ldots, g_s)$ dem Modul all derjenigen Elemente in $U = \langle g_1 - e_{r+1}, \ldots, g_s - e_{r+s} \rangle$ entspricht, die im freien von $\{e_{r+1}, \ldots, e_{r+s}\}$ zweiseitig erzeugten Modul $\widehat{F}$ enthalten sind. Dieser kann auch als der Komponenten-Eliminationsmodul von U bzgl. $L = \{e_1, \ldots, e_r\}$ identifiziert werden. Eine Gröbnerbasis von $U \cap \widehat{F}$ erhalten wir nun aus einem Resultat der Eliminationstheorie: Ist G eine Gröbnerbasis von U, so ist $G \cap \widehat{F}$ eine Gröbnerbasis von $U \cap \widehat{F}$.

In Kapitel 4 studieren wir zunächst Gröbnerbasen für zweiseitige Moduln über einem Restklassenring $R = K[\Sigma^*]/I$, wobei I durch eine endliche Gröbnerbasis gegeben ist. Das Ziel dabei ist die Berechnung einer Gröbnerbasis von $\mathrm{Syz}(g_1, \ldots, g_s)$ für $g_1, \ldots, g_s \in R$. Das Ergebnis ist eine Isomorphie zwischen $\mathrm{Syz}(g_1, \ldots, g_s)$ und dem Komponenten-Eliminationsmodul von $\langle e_1 g_1 - e_2, \ldots, e_1 g_s - e_{s+1} \rangle + M_I + N$ bzgl. $L = \{1\}$. Dieses Resultat lässt sich

nun auch auf Monoidringe übertragen. Das abschließende Beispiel zeigt die Anwendung der Prozedur auf ein Tupel von Elementen der symmetrischen Gruppe S_3.

Kapitel 2

Gröbnerbasen für zweiseitige Moduln

In diesem Kapitel befassen wir uns mit den Grundlagen für die Berechnung von Syzygien. Der Schwerpunkt liegt dabei auf dem Begriff der *Gröbnerbasis* eines Moduls. Darunter verstehen wir ein Erzeugendensystem eines Moduls, welches, wie in der kommutativen Theorie, auch hier besondere Eigenschaften besitzt, die für weitere Berechnungen interessant sind. Wir betrachten dabei zweiseitige Moduln über nicht-kommutativen Polynomringen, die Thema des ersten Abschnitts sind. Es folgen Termordnungen für Moduln und in diesem Kontext die Einführung von Gröbnerbasen. Im dritten Abschnitt beschäftigen wir uns mit dem Divisionsalgorithmus, bevor wir anschließend Termersetzungssysteme und deren Zusammenhang mit Gröbnerbasen ansprechen. Der Buchberger-Algorithmus steht im Mittelpunkt des fünften Abschnitts. Er ermöglicht eine Berechnung von Gröbnerbasen. Im letzten Abschnitt behandeln wir einen wichtigen Spezialfall der zweiseitigen Moduln, den der zweiseitigen Ideale von nicht-kommutativen Polynomringen. Dabei werden die in den ersten Abschnitten gewonnenen Erkenntnisse auf zweiseitige Ideale angewendet.

2.1 Der nicht-kommutative Polynomring

Im Folgenden sei $\Sigma = \{x_1, \ldots, x_n\}$ eine Menge von Unbestimmten und Σ^* bezeichne das von Σ erzeugte nicht-kommutative Monoid der Terme. In anderen Zusammenhängen (siehe Kapitel 4) heißt Σ auch ein Alphabet und Σ^* entspricht der Menge der Wörter. Die Elemente von Σ^* haben die Form $w = x_{i_1} \cdots x_{i_k}$ mit $i_1, \ldots, i_k \in \{1, \ldots, n\}$ für ein $k \in \mathbb{N}_0$. Als Verknüpfung dient die Konkatenation. Das neutrale Element ist das leere Wort $1 = 1_{\Sigma^*}$.

D.h. für $w, w' \in \Sigma^*$ mit $w = x_{i_1} \cdots x_{i_k}$ und $w' = x_{j_1} \cdots x_{j_l}$ ist dann $ww' = x_{i_1} \cdots x_{i_k} x_{j_1} \cdots x_{j_l}$, wobei $i_1, \ldots, i_k, j_1, \ldots, j_l \in \{1, \ldots, n\}$ und $k, l \in \mathbb{N}_0$.

Definition 2.1.1 Sei $w = x_{i_1} \cdots x_{i_k} \in \Sigma^*$ mit $i_1, \ldots, i_k \in \{1, \ldots, n\}$ und $k \in \mathbb{N}$.

1) Die Zahl $\deg(w) = k \in \mathbb{N}_0$ heißt der **Grad** von w.
2) Für jedes $\mu \in \{1, \ldots, k\}$ heißt $x_{i_1} \cdots x_{i_\mu}$ **Präfix** von w und $x_{i_\mu} \cdots x_{i_k}$ **Suffix** von w.

Definition 2.1.2 Sei K ein Körper. Unter dem **nicht-kommutativen Polynomring** (oder der **freien assoziativen Algebra**) von Σ^* über K verstehen wir die Menge aller endlichen Linearkombinationen von Termen, d.h.

$$K[\Sigma^*] := \{\sum_{i=1}^{k} c_i w_i \,|\, c_i \in K\backslash\{0\}, w_i \in \Sigma^*, k \in \mathbb{N}\},$$

mit der üblichen Addition und der linearen Fortsetzung der Multiplikation in Σ^* als Multiplikation.

Wir wollen nun zunächst die Elemente des Monoids Σ^* ordnen. Dazu betrachten wir totale Ordnungen auf Σ^* mit zusätzlichen Eigenschaften, sogenannte *Termordnungen*. Diese geben uns dann die Möglichkeit, die Elemente von $K[\Sigma^*]$ auf eindeutige Art und Weise darzustellen.

Definition 2.1.3 Eine vollständige Relation σ auf Σ^* heißt **Monoidordnung** auf Σ^*, falls für alle Terme $w_1, w_2, w_3, w_4 \in \Sigma^*$ gilt:

1) $w_1 \geq_\sigma w_1$,
2) $w_1 \geq_\sigma w_2, w_2 \geq_\sigma w_1 \;\Rightarrow\; w_1 = w_2$,
3) $w_1 \geq_\sigma w_2, w_2 \geq_\sigma w_3 \;\Rightarrow\; w_1 \geq_\sigma w_3$,
4) $w_1 \geq_\sigma w_2 \;\Rightarrow\; w_3 w_1 w_4 \geq_\sigma w_3 w_2 w_4$.

Eine Monoidordnung σ heißt **Termordnung**, falls zusätzlich gilt, dass

5) σ eine Wohlordnung ist, d.h. dass jede absteigende Kette von Termen $w_1 \geq_\sigma w_2 \geq_\sigma \cdots$ in Σ^* stationär wird.

Für $w_1 \geq_\sigma w_2$ mit $w_1, w_2 \in \Sigma^*$ schreiben wir auch $w_2 \leq_\sigma w_1$. Ist zudem $w_1 \neq w_2$, so notieren wir dies mit $w_1 >_\sigma w_2$ bzw. mit $w_2 <_\sigma w_1$.

Die Terme eines Elements $f \in K[\Sigma^*]$ lassen sich nun bzgl. einer Termordnung σ anordnen und f erhält eine eindeutige Darstellung $f = \sum_{i=1}^{k} c_i w_i$ mit $c_i \in K\backslash\{0\}$ und $w_1 >_\sigma \cdots >_\sigma w_k$ für ein $k \in \mathbb{N}$.

Die Notwendigkeit einer Termordnung, d.h. die Gültigkeit von 5), wird hier zunächst nicht deutlich. Sie liefert jedoch das wesentliche Argument in späteren Betrachtungen.

Beispiel 2.1.4

a) Für zwei Terme ist die lexikographische Ordnung `Lex` wie folgt definiert:

$$x_{i_1} \cdots x_{i_r} >_{\texttt{Lex}} x_{j_1} \cdots x_{j_s} \iff \begin{array}{l} \text{es existiert ein } 1 \leq k \leq r \text{ mit} \\ i_1 = j_1, \ldots, i_{k-1} = j_{k-1} \text{ und } i_k < j_k, \end{array}$$

wobei $i_1, \ldots, i_r, j_1, \ldots, j_s \in \{1, \ldots, n\}$. Die Ordnung `Lex` ist eine Monoidordnung. Sie bildet jedoch für $n \geq 2$ keine Termordnung auf Σ^*, denn es lässt sich eine unendliche, echt absteigende Kette von Termen konstruieren:

$$x_1 >_{\texttt{Lex}} x_2x_1 >_{\texttt{Lex}} x_2^2x_1 >_{\texttt{Lex}} x_2^3x_1 >_{\texttt{Lex}} \ldots$$

b) Ein Beispiel für eine Termordnung auf Σ^* liefert die länge-lexikographische Ordnung `LLex`. Für zwei Terme $w_1, w_2 \in \Sigma^*$ gilt $w_1 \geq_{\texttt{LLex}} w_2$ genau dann, wenn $\deg(w_1) > \deg(w_2)$ oder $\deg(w_1) = \deg(w_2)$ und $w_1 \geq_{\texttt{Lex}} w_2$.

Abschließend wollen wir noch den Begriff des *Leitterms* eines Elements von $K[\Sigma^*]$ einführen, der eine Bezeichnung für den jeweils größten Term darstellt. Dieser wird in den folgenden Abschnitten von besonderer Bedeutung sein.

Definition 2.1.5 Sei σ eine Termordnung auf Σ^*. Ist $f = \sum_{i=1}^{k} c_i w_i$ ein Element von $K[\Sigma^*]$ mit $c_1, \ldots, c_k \in K\backslash\{0\}$, $w_1, \ldots, w_k \in \Sigma^*$, $k \geq 1$ und $w_1 >_\tau \cdots >_\tau w_k$, so heißt $\mathrm{LT}_\tau(f) = w_1$ der **Leitterm**, $\mathrm{LC}_\tau(f) = c_1$ der **Leitkoeffizient** und $\mathrm{LM}_\tau(f) = c_1w_1$ das **Leitmonom** von f.

Es ist hier zu beachten, dass für $f = 0$ die obigen Begriffe nicht definiert sind.

2.2 Modultermordnungen

Nachdem wir den nicht-kommutativen Polynomring $K[\Sigma^*]$ eingeführt haben, wollen wir uns nun mit der algebraischen Struktur der freien zweiseitigen Moduln über $K[\Sigma^*]$ befassen. Für diese definieren wir wieder Termordnungen, sogenannte Modultermordnungen, bevor wir uns mit dem Begriff der Gröbnerbasis für zweiseitige Moduln beschäftigen.

Wir betrachten zunächst das Tensorprodukt $K[\Sigma^*] \otimes_K K[\Sigma^*]$, welches mit $K \times (K[\Sigma^*] \otimes_K K[\Sigma^*]) \longrightarrow K[\Sigma^*] \otimes_K K[\Sigma^*]$, $c(g \otimes_K g') = cg \otimes_k g'$ eine K-Modulstruktur besitzt. Für nähere Details verweisen wir auf [2], Kapitel 2 § 3. Eine der definierenden Eigenschaften des Tensorproduktes besteht in der Gültigkeit der Relation $cg \otimes_K g' = g \otimes_K cg'$ für alle $c \in K\backslash\{0\}$

und $g, g' \in K[\Sigma^*]$. Ein Element von $K[\Sigma^*] \otimes_K K[\Sigma^*]$ hat also die Form $\sum_{i\in\mathbb{N}} c_i w_i \otimes_K w_i'$, wobei $c_i \in K$, $w_i, w_i' \in \Sigma^*$ und nur endlich viele der c_i von Null verschieden sind. Wir können $K[\Sigma^*] \otimes_K K[\Sigma^*]$ auch als zweiseitigen $K[\Sigma^*]$-Modul interpretieren. Sei dazu die skalare Multiplikation definiert durch $\cdot : (K[\Sigma^*] \times K[\Sigma^*]) \times (K[\Sigma^*] \otimes_K K[\Sigma^*]) \longrightarrow K[\Sigma^*] \otimes_K K[\Sigma^*]$ mit $(f_1, f_2) \cdot (g \otimes_K g') \mapsto f_1 g \otimes g' f_2$.

Definition 2.2.1 Sei $r \in \mathbb{N}$. Unter dem **freien zweiseitigen Modul** F_r **über** $K[\Sigma^*]$ **vom Rang** r verstehen wir die Menge $(K[\Sigma^*] \otimes_K K[\Sigma^*])^r$ versehen mit der komponentenweisen Addition und der skalaren Multiplikation $(f_1, f_2) \cdot (g_1 \otimes_K g_1', \ldots, g_r \otimes_K g_r') = (f_1 g_1 \otimes_K g_1' f_2, \ldots, f_1 g_r \otimes g_r' f_2)$.

Zur besseren Verständlichkeit schreiben wir im Folgenden den soeben definierten Modul $(K[\Sigma^*] \otimes_K K[\Sigma^*])^r$ als $F_r = \bigoplus_{i=1}^r K[\Sigma^*] e_i K[\Sigma^*]$. D.h. die Elemente von F_r sind nun von der Form $\sum_{i=1}^r \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_i w_{ij}'$ mit $c_{ij} \in K$, $w_{ij}, w_{ij}' \in \Sigma^*$ für $i = 1, \ldots, r$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_i von Null verschieden sind. Wir nennen diesen Modul auch den freien zweiseitigen Modul über $K[\Sigma^*]$ erzeugt von $\{e_1, \ldots, e_r\}$. Wird aus dem jeweiligen Kontext ersichtlich, dass es sich bei F_r um den genannten Modul handelt, so schreiben wir auch F statt F_r.

Soweit nicht anders erwähnt verstehen wir von nun an unter einem Modul stets einen zweiseitigen $K[\Sigma^*]$-Modul. Ist $G = \{g_i \mid i \in I\}$ für eine Indexmenge I, so schreiben wir für den von G erzeugten zweiseitigen Modul kurz $\langle g_i \mid i \in I\rangle$. Ein Homomorphismus $\varphi : F \longrightarrow F'$ von freien zweiseitigen Moduln F und F' sei im Folgenden eine Abbildung, so dass für $m_1, m_2 \in F$ und $f_1, f_2 \in K[\Sigma^*]$ die Bedingung $\varphi(f_1(m_1 + m_2)f_2) = f_1\varphi(m_1)f_2 + f_1\varphi(m_2)f_2$ erfüllt ist.

Wir wollen zunächst, bevor wir wie im vorherigen Abschnitt Termordnungen für freie zweiseitige Moduln einführen, die im weiteren Verlauf der Arbeit häufig verwendete *universelle Eigenschaft* freier zweiseitiger Moduln diskutieren.

Satz 2.2.2 (Universelle Eigenschaft freier zweiseitiger Moduln)
Sei F_r der freie von $\{e_1, \ldots, e_r\}$ zweiseitig erzeugte $K[\Sigma^*]$-Modul, seien F' ein weiterer freier zweiseitiger $K[\Sigma^*]$-Modul und $m_1, \ldots, m_r$ Elemente in F'. Dann existiert genau ein Homomorphismus $\varphi : F_r \longrightarrow F'$, so dass $\varphi(e_i) = m_i$ für $i = 1, \ldots, r$.

Beweis. Der freie zweiseitige Modul F_r vom Rang r ist die direkte Summe aus dem freien zweiseitigen Modul F_1 vom Rang 1 als r-facher Summand. Der Modul F_1 wiederum ist als das Tensorprodukt $K[\Sigma^*] \otimes_K K[\Sigma^*]$ definiert. Aus der universellen Eigenschaft des Tensorproduktes (siehe dazu [2], Kapitel 2 § 3.1 Prop. 1b)) und der direkten Summe folgt nun die Behauptung. □

Definition 2.2.3

1) Ein Element in F der Form we_iw' mit $i \in \{1, \ldots, r\}$ und $w, w' \in \Sigma^*$ heißt **Term** in F. Mit $\mathbb{T}(F)$ sei die Menge aller Terme in F bezeichnet.
2) Eine **Modultermordnung** auf $\mathbb{T}(F)$ ist eine totale Ordnung τ, so dass gilt:
   i) Aus $t_1 \leq_\tau t_2$ folgt $w_1t_1w_2 \leq_\tau w_1t_2w_2$ für alle Terme $t_1, t_2 \in \mathbb{T}(F)$ und $w_1, w_2 \in \Sigma^*$.
   ii) Jede absteigende Kette $t_1 \geq_\tau t_2 \geq_\tau \cdots$ von Termen in $\mathbb{T}(F)$ wird stationär, d.h. τ ist eine Wohlordnung.
3) Sei σ eine Monoidordnung auf Σ^*. Eine Modultermordnung τ auf $\mathbb{T}(F)$ heißt **verträglich** mit σ, falls aus $w_1w_1' \leq_\sigma w_2w_2'$ stets $w_1tw_1' \leq_\tau w_2tw_2'$ folgt für alle $w_1, w_1', w_2, w_2' \in \Sigma^*$ und $t \in \mathbb{T}(F)$.

Die Terme wtw' mit $w, w' \in \Sigma^*$ und $t \in \mathbb{T}(F)$ nennen wir im Folgenden auch Vielfache des Terms t.

Mit Hilfe einer Modultermordnung τ lässt sich nun ein Element $f \in F$ analog zu den nicht-kommutativen Polynomen eindeutig darstellen. Wir können f schreiben als $f = \sum_{i=1}^{k} c_it_i$ mit $c_1, \ldots, c_k \in K\backslash\{0\}$, $t_1, \ldots, t_k \in \mathbb{T}(F)$ und $t_1 >_\tau t_2 >_\tau \ldots >_\tau t_k$ für ein $k \in \mathbb{N}$.

Ab jetzt sei, soweit nicht anders erwähnt, τ stets eine Modultermordnung auf $\mathbb{T}(F)$. Die wichtigsten und damit für uns relevanten Modultermordnungen sind wie folgt aufgebaut.

Beispiel 2.2.4 Sei `To` eine Termordnung auf Σ^* und $w_1, w_1', w_2, w_2' \in \Sigma^*$.

a) Für Terme $w_1e_iw_1', w_2e_jw_2' \in \mathbb{T}(F)$ mit $i, j \in \{1, \ldots, r\}$ ist die Ordnung `ToPos` definiert durch

$$\begin{aligned} & w_1e_iw_1' >_{\texttt{ToPos}} w_2e_jw_2' \\ \iff\ & w_1w_1' >_{\texttt{To}} w_2w_2' \text{ oder } (w_1w_1' = w_2w_2' \text{ und } w_1 >_{\texttt{To}} w_2) \\ & \text{oder } (w_1 = w_2 \text{ und } w_1' = w_2' \text{ und } i < j). \end{aligned}$$

   Wir erhalten mit `ToPos` eine Modultermordnung auf der Menge der Terme $\mathbb{T}(F)$. Vereinfacht gesagt werden zunächst die beteiligten Terme bzgl. `To` verglichen und bei Gleichheit entscheidet deren jeweilige Position.

b) Ähnlich lässt sich nun auch die Modultermordnung `PosTo` für Terme $w_1e_iw_1', w_2e_jw_2' \in \mathbb{T}(F)$ mit $i, j \in \{1, \ldots, r\}$ definieren:

$$\begin{aligned} & w_1e_iw_1' >_{\texttt{PosTo}} w_2e_jw_2' \\ \iff\ & i < j \text{ oder } (i = j \text{ und } w_1w_1' >_{\texttt{To}} w_2w_2') \\ & \text{oder } (i = j \text{ und } w_1w_1' = w_2w_2' \text{ und } w_1 >_{\texttt{To}} w_2). \end{aligned}$$

Auch der Begriff des Leitterms lässt sich auf Elemente eines Moduls übertragen. In diesem Zusammenhang wollen wir des Weiteren den *Leittermmodul* ansprechen, den wir am Ende dieses Abschnitts für die Definition der Gröbnerbasis benötigen.

Definition 2.2.5 Sei M ein zweiseitiger Untermodul von F.

1) Ist $m = \sum_{i=1}^{k} c_i t_i \in F$ mit $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}(F)$ und $k \geq 1$, wobei $t_1 >_\tau \cdots >_\tau t_k$, so heißt $\mathrm{LT}_\tau(m) = t_1$ der **Leitterm**, $\mathrm{LC}_\tau(m) = c_1$ der **Leitkoeffizient** und $\mathrm{LM}_\tau(m) = c_1 t_1$ das **Leitmonom** von m.
2) Der zweiseitige Untermodul $\mathrm{LT}_\tau(M) = \langle \mathrm{LT}_\tau(m) \,|\, m \in M\backslash\{0\}\rangle$ von F heißt der **(zweiseitige) Leittermmodul** von M und $\mathrm{LT}_\tau\{M\} = \{\mathrm{LT}_\tau(m) \,|\, m \in M\backslash\{0\}\}$ die **Menge der Leitterme** von M.

Wie bei den nicht-kommutativen Polynomen ist auch hier der Leitterm für $m = 0$ nicht definiert. Um die Modulstruktur des in 2) definierten Leittermmoduls zu sichern, führen wir noch folgendes Lemma an.

Lemma 2.2.6 *Sei σ eine Monoidordnung auf Σ^* und τ verträglich mit σ. Dann gilt für $m, m_1, m_2 \in F\backslash\{0\}$, $w, w' \in \Sigma^*$ und $f, f' \in K[\Sigma^*]\backslash\{0\}$:*

a) Ist $m_1 + m_2 \neq 0$ und $\mathrm{LT}_\tau(m_1) \neq \mathrm{LT}_\tau(m_2)$ bzw. $\mathrm{LT}_\tau(m_1) = \mathrm{LT}_\tau(m_2)$ und $\mathrm{LC}_\tau(m_1) \neq -\mathrm{LC}_\tau(m_2)$, so ist

$$\mathrm{LT}_\tau(m_1 + m_2) = \max_\tau\{\mathrm{LT}_\tau(m_1), \mathrm{LT}_\tau(m_2)\}.$$

b) $\mathrm{LT}_\tau(wmw') = w \cdot \mathrm{LT}_\tau(m) \cdot w'$.
c) $\mathrm{LT}_\tau(fmf') = \mathrm{LT}_\sigma(f) \cdot \mathrm{LT}_\tau(m) \cdot \mathrm{LT}_\sigma(f')$.

Beweis. Für den Beweis von a) schreiben wir m_1 und m_2 als $m_1 = \sum_{i=1}^{k} c_i t_i$ bzw. $m_2 = \sum_{i=1}^{k'} c_i' t_i'$ anhand von 2.2.5 1). Sind die Leitterme von m_1 und m_2 verschieden, so folgt die Behauptung direkt. Bei gleichen Leittermen erhält dieser nach der Addition den Koeffizienten $c_1 + c_2$, der nach Voraussetzung ungleich Null ist. Damit ist der Leitterm von m_1 und m_2 auch der von $m_1 + m_2$.

Um b) zu zeigen, schreiben wir wieder $m = \sum_{i=1}^{k} c_i t_i$ mit $t_i \in \mathbb{T}(F)$ und $c_i \in K\backslash\{0\}$ für $i = 1, \ldots, k$. Dann ist $wmw' = \sum_{i=1}^{k} c_i w t_i w'$. Da τ eine Modultermordnung ist, folgt aus $t_i <_\tau t_j$ nun $wt_iw' <_\tau wt_jw'$. Damit ergibt sich $\mathrm{LT}_\tau(wmw') = w\mathrm{LT}_\tau(m)w'$.

Für den Beweis von c) seien $f = \sum_{j=1}^{l} d_j w_j$ und $f' = \sum_{j'=1}^{l'} d_{j'}' w_{j'}'$ mit $d_j, d_{j'}' \in K\backslash\{0\}$, $w_j, w_{j'}' \in \Sigma^*$ für $j = 1, \ldots, l$ bzw. $j' = 1, \ldots, l'$. Dann ergibt sich $fmf' = \sum_{i=1}^{k} \sum_{j=1}^{l} \sum_{j'=1}^{l'} c_i d_j d_{j'} w_j t_i w_{j'}$ mit von Null verschiedenen Koeffizienten. Aufgrund der Verträglichkeit von τ mit σ folgt nun die Behauptung. □

Mit Hilfe der Menge der Leitterme lässt sich nun explizit eine Basis des K-Vektorraums F/M angeben. Dazu betrachten wir den folgenden wichtigen Satz.

Satz 2.2.7 (Macaulays Basis-Theorem)
Sei M ein zweiseitiger Untermodul von F. Dann bilden die Restklassen der Terme in $\mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}$ eine K-Basis von F/M.

Beweis. Für $v \in F$ sei $\overline{v}$ die zugehörige Restklasse in F/M. Angenommen, die Restklassen von $\mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}$ bilden kein Erzeugendensystem von F/M. Dann sei $v \in F$ so gewählt, dass v einen minimalen Leitterm bzgl. τ hat mit der Eigenschaft, dass $\overline{v} \notin \langle \overline{t} \,|\, t \in \mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}\rangle_K =: B$. Gilt $\mathrm{LT}_\tau(v) \in \mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}$, so ist auch die Restklasse von $v' = v - \mathrm{LM}_\tau(v)$ nicht in B enthalten. Nun hat v' aber einen kleineren Leitterm als v im Widerspruch zur Wahl von v. Ist $\mathrm{LT}_\tau(v) \in \mathrm{LT}_\tau\{M\}$, so existiert ein $m \in M$ mit $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(v)$. Wieder ist die Restklasse von $v' = v - \frac{\mathrm{LC}_\tau(v)}{\mathrm{LC}_\tau(m)} m$ nicht in B enthalten und $\mathrm{LT}_\tau(v') <_\tau \mathrm{LT}_\tau(v)$, ein Widerspruch. Damit wird F/M durch die Restklassen von $\mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}$ erzeugt.

Zum Beweis der linearen Unabhängigkeit nehmen wir an, dass für ein $k \geq 1$ gilt $\sum_{i=1}^k c_i \overline{t}_i = \overline{0}$ mit $c_i \in K\backslash\{0\}$ und Termen $t_i \in \mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}$. Es folgt $\sum_{i=1}^k c_i t_i \in M$ und damit $\mathrm{LT}_\tau(\sum_{i=1}^k c_i t_i) \in \mathrm{LT}_\tau\{M\} \cap (\mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\})$, ein Widerspruch. □

Im restlichen Teil dieses Abschnitts wollen wir uns nun mit Gröbnerbasen für zweiseitige Moduln auseinandersetzen. Dazu geben wir zunächst deren Definition an, bevor die ersten besonderen Eigenschaften von Gröbnerbasen erfasst werden.

Definition 2.2.8 Sei M ein zweiseitiger Untermodul von F. Eine Teilmenge $G \subseteq M\backslash\{0\}$ heißt **(zweiseitige) τ-Gröbnerbasis** von M, falls gilt

$$\mathrm{LT}_\tau\{M\} = \{w_1 \mathrm{LT}_\tau(m) w_2 \,|\, m \in G, w_1, w_2 \in \Sigma^*\}.$$

Die Definition einer τ-Gröbnerbasis von M ist natürlich gleichbedeutend damit, dass der Leittermmodul $\mathrm{LT}_\tau(M)$ von den Leittermen der Elemente in G erzeugt wird. Weiter sei Folgendes bemerkt.

Bemerkung 2.2.9 Sei $G \subseteq M\backslash\{0\}$ eine τ-Gröbnerbasis von M.

a) Der Modul M besitzt i. Allg. keine eindeutige τ-Gröbnerbasis, denn für $m \in M\backslash G$ ist auch $G \cup \{m\}$ eine τ-Gröbnerbasis von M.
b) Die Existenz einer τ-Gröbnerbasis ist gesichert, denn $G = M\backslash\{0\}$ stellt stets eine τ-Gröbnerbasis von M dar.

c) Eine τ-Gröbnerbasis von M hängt immer von der gewählten Modultermordnung τ ab. Ist $\tilde{\tau}$ eine andere Modultermordnung auf $\mathbb{T}(F)$, so muss also G keine $\tilde{\tau}$-Gröbnerbasis von M sein. Dies wird aus der Tatsache ersichtlich, dass bereits die Leitterme und damit der Leittermmodul von M von der Modultermordnung abhängen.

Beispiel 2.2.10 Sei $K = \mathbb{Q}$ und $\Sigma = \{x_1, x_2\}$. Sei F der freie zweiseitige Modul erzeugt von $\{e_1, e_2\}$ und $\tau =$ `PosLLex` die gewählte Modultermordnung auf $\mathbb{T}(F)$.

a) Sei $M = \langle g_1, g_2\rangle$ ein zweiseitiger Untermodul von F mit $g_1 = x_1^2e_1 + e_2$ und $g_2 = 2x_2^3e_1 - e_2x_2$. Dann ist $G = \{g_1, g_2\}$ eine τ-Gröbnerbasis von M, denn jedes von Null verschiedene Element von M lässt sich schreiben als $m = \sum_{i=1}^{k}(c_iw_ix_1^2e_1w_i' + c_iw_ie_2w_i') + \sum_{j=1}^{l}(2d_jv_jx_2^3e_1v_j' - d_jv_je_2x_2v_j')$ mit $k, l \in \mathbb{N}_0$, $c_i, d_j \in \mathbb{Q}\backslash\{0\}$, $w_i, w_i', v_j, v_j' \in \Sigma^*$ für $i = 1, \ldots, k$ und $j = 1, \ldots, l$. Dabei können sich nun zwei Monome $c_iw_ix_1^2e_1w_i'$ und $2d_jv_jx_2^3e_1v_j'$ nicht gegenseitig wegheben. Deshalb ist der Leitterm von m entweder ein Vielfaches von $x_1^2e_1 = \mathrm{LT}_\tau(g_1)$ oder $x_2^3e_1 = \mathrm{LT}_\tau(g_2)$.

b) Sei nun $M = \langle g_1, g_2\rangle$ mit $g_1 = x_1^2e_1x_2 + x_1e_1$ und $g_2 = e_1x_2^2 + e_2$. Dann ist $\{g_1, g_2\}$ keine τ-Gröbnerbasis von M, denn es gilt $x_1e_1x_2 - x_1^2e_2 = g_1x_2 - x_1^2g_2$ und damit $x_1e_1x_2 = \mathrm{LT}_\tau(x_1e_1x_2 - x_1^2e_2) \in \mathrm{LT}_\tau(M)$, aber $x_1e_1x_2 \notin \langle \mathrm{LT}_\tau(g_1), \mathrm{LT}_\tau(g_2)\rangle$.

Es stellt sich schnell heraus, dass der Nachweis, dass eine Teilmenge G von $M\backslash\{0\}$ eine τ-Gröbnerbasis von M ist, nur selten so einfach gelingt wie in den obigen Beispielen. Wie der komplizierte Nachweis der definierenden Bedingung umgangen werden kann, werden wir anhand des *Buchberger-Algorithmus* im vorletzten Abschnitt dieses Kapitels erklären.

Eine erste wichtige Eigenschaft von Gröbnerbasen soll der nächste Satz vermitteln. Demnach besitzt jedes Element in $M\backslash\{0\}$ eine besondere Darstellung in den Elementen einer Gröbnerbasis.

Satz 2.2.11 *Sei M ein zweiseitiger Untermodul von F und $G \subseteq M\backslash\{0\}$. Dann sind folgende Aussagen äquivalent:*

a) G ist eine τ-Gröbnerbasis von M.

b) Für jedes Element $m \in M\backslash\{0\}$ existieren $g_1, \ldots, g_s \in G$, $w_1, \ldots, w_s$, $w_1', \ldots, w_s' \in \Sigma^*$ und $c_1, \ldots, c_s \in K\backslash\{0\}$ für ein $s \in \mathbb{N}$, so dass gilt $m = \sum_{i=1}^{s} c_iw_ig_iw_i'$ und $\mathrm{LT}_\tau(m) \geq_\tau \mathrm{LT}_\tau(w_ig_iw_i')$ für $i = 1, \ldots, s$.

Beweis. Sei zunächst G eine τ-Gröbnerbasis von M und $m_1 \in M\backslash\{0\}$. Dann ist $\mathrm{LT}_\tau(m_1) \in \mathrm{LT}_\tau\{M\}$ und es existieren ein $g_1 \in G$, $w_1, w_1' \in \Sigma^*$ mit $\mathrm{LT}_\tau(m_1) = w_1\mathrm{LT}_\tau(g_1)w_1' = \mathrm{LT}_\tau(w_1g_1w_1')$. Wir betrachten nun das Element

$m_2 = m_1 - \frac{\mathrm{LC}_\tau(m_1)}{\mathrm{LC}_\tau(g_1)} w_1 g_1 w_1'$. Es gilt $\mathrm{LT}_\tau(m_2) <_\tau \mathrm{LT}_\tau(m_1)$ und $\mathrm{LT}_\tau(m_2) \in \mathrm{LT}_\tau\{M\}$. Da G eine τ-Gröbnerbasis von M ist, finden wir wieder ein $g_2 \in G$ und $w_2, w_2' \in \Sigma^*$ mit $\mathrm{LT}_\tau(m_2) = \mathrm{LT}_\tau(w_2 g_2 w_2')$. Damit erhalten wir ein Element $m_3 = m_2 - \frac{\mathrm{LC}_\tau(m_2)}{\mathrm{LC}_\tau(g_2)} w_2 g_2 w_2'$ mit $\mathrm{LT}_\tau(m_3) <_\tau \mathrm{LT}_\tau(m_2)$. Da τ eine Wohlordnung ist, endet dieses Verfahren nach endlich vielen Schritten. Ist s die Anzahl dieser Schritte, so gilt $m_1 = \sum_{i=1}^{s} \frac{\mathrm{LC}_\tau(m_i)}{\mathrm{LC}_\tau(g_i)} w_i g_i w_i'$.

Umgekehrt gelte nun die Aussage in b). Zu zeigen ist, dass G eine τ-Gröbnerbasis von M ist. Sei dazu $t \in \mathrm{LT}_\tau\{M\}$, d.h. es gibt ein $f \in M\backslash\{0\}$ mit $\mathrm{LT}_\tau(f) = t$. Nach Vor. besitzt f eine Darstellung $f = \sum_{i=1}^{s} c_i w_i g_i w_i'$ mit $g_1, \ldots, g_s \in G$, $w_1, \ldots, w_s, w_1', \ldots, w_s' \in \Sigma^*$, $c_1, \ldots, c_s \in K\backslash\{0\}$ und $\mathrm{LT}_\tau(f) \geq_\tau \mathrm{LT}_\tau(w_i g_i w_i')$ für $i = 1, \ldots, s$. Es existiert also ein $j \in \{1, \ldots, s\}$ mit $t = \mathrm{LT}_\tau(f) = \mathrm{LT}_\tau(w_j g_j w_j') = w_j \mathrm{LT}_\tau(g_j) w_j'$. G erfüllt demnach die Bedingung aus der Definition einer τ-Gröbnerbasis von M. □

Korollar 2.2.12 *Sei M ein zweiseitiger Untermodul von F und $G \subseteq M\backslash\{0\}$ eine τ-Gröbnerbasis von M. Dann ist G auch ein Erzeugendensystem des Moduls M.*

Beweis. Die Behauptung folgt sofort aus der Implikation a) ⇒ b) des vorangehenden Satzes. □

Wir haben gesehen, dass der Begriff der Gröbnerbasis ein spezielles Erzeugendensystem beschreibt. Weitere äquivalente Aussagen werden in den Abschnitten 4 und 5 folgen.

2.3 Der Divisionsalgorithmus

Im vorangehenden Abschnitt haben wir τ-Gröbnerbasen für zweiseitige Moduln M kennen gelernt und gesehen, dass sich jedes $m \in M$ mit Elementen aus G auf eine bestimmte Art und Weise darstellen lässt. Nun stellt sich zwangsläufig die Frage, wie wir zu einer solchen Darstellung gelangen können. Die Antwort wird in diesem Abschnitt mit dem Divisionsalgorithmus gegeben. Er ermöglicht es uns, ein Element $m \in F$ durch ein Tupel $(g_1, \ldots, g_s) \in F^s$ zu „dividieren“, d.h. er liefert Elemente $q_{ij}, q_{ij}' \in K[\Sigma^*]$ und $p \in F$, so dass

$$m = q_{11} g_1 q_{11}' + \cdots + q_{1n_1} g_1 q_{1n_1}' + \cdots + q_{s1} g_s q_{s1}' + \cdots + q_{sn_s} g_s q_{sn_s}' + p.$$

Bevor wir den Algorithmus und seine Eigenschaften formal vorstellen, wollen wir zunächst intuitiv an einem Beispiel vorgehen.

Beispiel 2.3.1 Sei F der freie von $\{e_1, e_2\}$ zweiseitig erzeugte Modul über $\mathbb{Q}[x_1, x_2]$ und $\tau = \texttt{PosLLex}$ die gewählte Modultermordnung auf $\mathbb{T}(F)$. Wir betrachten Elemente $m, g_1, g_2 \in F$ mit $m = x_2^2x_1e_1x_2^2+x_1e_1x_2x_1^2+x_1^2x_2e_2+e_2$, $g_1 = e_1x_2x_1^2 + x_1x_2e_2 + e_2$ und $g_2 = x_2x_1e_1x_2 - e_2$. Wir wollen nun m durch das Tupel (g_1, g_2) darstellen. Dazu reduzieren wir schrittweise den Leitterm von m und erhalten:

$$\begin{array}{rcl}
x_2^2x_1e_1x_2^2 + x_1e_1x_2x_1^2 + x_1^2x_2e_2 + e_2 & = & x_2g_2x_2 + x_1g_1 + p \\
\underline{x_2^2x_1e_1x_2^2 - x_2e_2x_2} & & \\
x_1e_1x_2x_1^2 + x_1^2x_2e_2 + x_2e_2x_2 + e_2 & & \\
\underline{x_1e_1x_2x_1^2 + x_1^2x_2e_2 + x_1e_2} & & \\
x_2e_2x_2 - x_1e_2 + e_2 & = & p
\end{array}$$

Damit ergibt sich die Darstellung $m = q_1g_1q_1' + q_2g_2q_2' + p$ mit $q_1 = x_1$, $q_1' = 1$, $q_2 = q_2' = x_2$ und Rest $p = x_2e_2x_2 - x_1e_2 + e_2$. Dabei erfüllt p die zusätzliche Eigenschaft, dass $\mathrm{LT}_\tau(p) <_\tau \mathrm{LT}_\tau(g_1)$ und $\mathrm{LT}_\tau(p) <_\tau \mathrm{LT}_\tau(g_2)$. Wir erhalten also $\mathrm{LT}_\tau(p) \notin \langle \mathrm{LT}_\tau(g_1), \mathrm{LT}_\tau(g_2)\rangle$. Außerdem gilt $\mathrm{LT}_\tau(m) \geq_\tau \mathrm{LT}_\tau(q_1g_1q_1')$ und $\mathrm{LT}_\tau(m) \geq_\tau \mathrm{LT}_\tau(q_2g_2q_2')$.

Wir kommen nun zur eigentlichen Formulierung des Algorithmus und werden sehen, dass die im obigen Beispiel aufgetretenen zusätzlichen Eigenschaften stets erfüllt sind.

Satz 2.3.2 (Der Divisionsalgorithmus)
Seien $s \geq 1$ und $m, g_1, \ldots, g_s \in F\backslash\{0\}$. Wir betrachten die folgenden Instruktionen:

1) *Für $i = 1, \ldots, s$ seien $n_i = 1$, $q_{i1}, q_{i1}' \in K[\Sigma^*]$ mit $q_{i1} = q_{i1}' = 0$, sowie $0 = p \in F$ und $f = m$.*
2) *Bestimme das kleinste $i \in \{1, \ldots, s\}$, so dass $w, w' \in \Sigma^*$ existieren mit $\mathrm{LT}_\tau(f) = w\mathrm{LT}_\tau(g_i)w'$. Existiert solch ein i,*
   - *erhöhe n_i um 1,*
   - *setze $q_{in_i} = \frac{\mathrm{LC}_\tau(f)}{\mathrm{LC}_\tau(g_i)}w$ und $q_{in_i}' = w'$,*
   - *ersetze f durch $f - \frac{\mathrm{LC}_\tau(f)}{\mathrm{LC}_\tau(g_i)}wg_iw'$,*
   - *falls $f \neq 0$, fahre mit 2) fort,*
   - *falls $f = 0$, fahre mit 4) fort.*
3) *Ersetze p durch $p + \mathrm{LM}_\tau(f)$ und f durch $f - \mathrm{LM}_\tau(f)$. Ist nun $f \neq 0$, so fahre mit 2) fort.*
4) *Gib $([(q_{11}, q_{11}'), \ldots, (q_{1n_1}, q_{1n_1}')], \ldots, [(q_{s1}, q_{s1}'), \ldots, (q_{sn_s}, q_{sn_s}')])$ und p aus.*

Die Ausgabe des Algorithmus erfüllt folgende Bedingungen:

a) $m = q_{11}g_1q'_{11} + \cdots + q_{1n_1}g_1q'_{1n_1} + \cdots + q_{s1}g_sq'_{s1} + \cdots + q_{sn_s}g_sq'_{sn_s} + p$.

b) Kein Term $t \in \mathrm{Supp}(p)$ *ist in* $\langle \mathrm{LT}_\tau(g_1), \ldots, \mathrm{LT}_\tau(g_s)\rangle$ *enthalten.*

c) Gilt $q_{ij} \neq 0 \neq q'_{ij}$ *für ein* $i \in \{1, \ldots, s\}$ *und* $j \in \{1, \ldots, n_i\}$*, so ist* $\mathrm{LT}_\tau(q_{ij}g_iq'_{ij}) \leq_\tau \mathrm{LT}_\tau(m)$.

d) Für alle $i \in \{1, \ldots, s\}$ *und* $j \in \{1, \ldots, n_i\}$ *gilt*

$$\tfrac{1}{\mathrm{LC}_\tau(q_{ij})\mathrm{LC}_\tau(q'_{ij})} q_{ij}\mathrm{LT}_\tau(g_i)q'_{ij} \notin \langle \mathrm{LT}_\tau(g_1), \ldots, \mathrm{LT}_\tau(g_{i-1})\rangle.$$

e) Die Elemente $([(q_{11}, q'_{11}), \ldots, (q_{1n_1}, q'_{1n_1})], \ldots, [(q_{s1}, q'_{s1}), \ldots, (q_{sn_s}, q'_{sn_s})])$ *und* p *sind durch die Eigenschaften a)-d) eindeutig bestimmt.*

Beweis. Wir zeigen zunächst a), indem wir die Gültigkeit der Gleichung

$$m = q_{11}g_1q'_{11} + \cdots + q_{1n_1}g_1q'_{1n_1} + \cdots + q_{s1}g_sq'_{s1} + \cdots + q_{sn_s}g_sq'_{sn_s} + p + f$$

in jedem Schritt des Algorithmus nachprüfen. Da nur für $f = 0$ eine Ausgabe erfolgt, wären wir dann fertig. Im 1. Schritt ist die Gleichung mit Sicherheit erfüllt und der 2. Schritt ist nur zu beachten, falls ein $i \in \{1, \ldots, s\}$ mit den geforderten Bedingungen gefunden wird. Dann gilt aber wieder

$$q_{in_i}g_iq'_{in_i} + f = \tfrac{\mathrm{LC}_\tau(f)}{\mathrm{LC}_\tau(g_i)} wg_iw' + f - \tfrac{\mathrm{LC}_\tau(f)}{\mathrm{LC}_\tau(g_i)} wg_iw'.$$

Im 3. Schritt erhalten wir $p + f = p + \mathrm{LM}_\tau(f) + f - \mathrm{LM}_\tau(f)$. Eine etwaige Wiederholung der Schritte 2 und 3 ändert dabei nichts an der Gültigkeit der Gleichung. Diese Schritte werden im Übrigen nur endlich oft durchlaufen, da jedes Mal der Leitterm von f aufgrund der Wohlordnung von τ echt kleiner wird.

Ausschließlich in 3) erhält p einen neuen Term und nur dann, wenn dieser nicht Vielfaches einer der Leitterme von $g_1, \ldots, g_s$ ist. Damit ist auch b) erfüllt.

Für den Beweis von c) seien $i \in \{1, \ldots, s\}$ und $j \in \{1, \ldots, n_i\}$ mit $q_{ij} \neq 0 \neq q'_{ij}$. Wir betrachten nun den zugehörigen 2. Schritt im Algorithmus und erhalten $\mathrm{LT}_\tau(q_{ij}g_iq'_{ij}) = \mathrm{LT}_\tau(f) \leq_\tau \mathrm{LT}_\tau(m)$, da der Leitterm von f nach jedem Durchlauf echt kleiner wird.

Um d) zu zeigen, seien $i \in \{1, \ldots, s\}$ und $j \in \{1, \ldots, n_i\}$. Da im zugehörigen 2. Schritt das i minimal gewählt wurde, ist $\mathrm{LT}_\tau(f)$ kein Vielfaches eines der Terme $\mathrm{LT}_\tau(g_1), \ldots, \mathrm{LT}_\tau(g_{i-1})$. Hierbei ist aber

$$\mathrm{LT}_\tau(f) = \tfrac{1}{\mathrm{LC}_\tau(q_{ij})\mathrm{LC}_\tau(q'_{ij})} q_{ij}\mathrm{LT}_\tau(g_i)q'_{ij}.$$

Für den Beweis von e) seien $([(r_{11}, r'_{11}), \ldots, (r_{1m_1}, r'_{1m_1})], \ldots, [(r_{s1}, r'_{s1}), \ldots, (r_{sm_s}, r'_{sm_s})])$ und p' zwei weitere Elemente, die die Bedingungen a)-d) erfüllen. Damit ergibt sich

$$\begin{aligned} 0 \;=\; & q_{11}g_1q'_{11} + \ldots + q_{1n_1}g_1q_{1n_1} - r_{11}g_1r'_{11} - \ldots - r_{1m_1}g_1r'_{1m_1} \\ & \qquad\qquad \vdots \\ & + q_{s1}g_sq'_{s1} + \ldots + q_{sn_s}g_sq_{sn_s} - r_{s1}g_sr'_{s1} - \ldots - r_{sm_s}g_sr'_{sm_s} \\ & + p - p' \end{aligned}$$

mit $m_1, \ldots, m_s \in \mathbb{N}$. Wegen a) folgt nun $\mathrm{LT}_\tau(p-p') \notin \langle \mathrm{LT}_\tau(g_1), \ldots, \mathrm{LT}_\tau(g_s)\rangle$. Damit würde dieser Term tatsächlich in der Summe auftreten. Da diese aber Null ergibt, muss demnach $p = p'$ gelten. Aus der Bedingung d) lässt sich weiter folgern, dass die Leitterme von Summanden in verschiedenen Zeilen paarweise verschieden sind. Mit der obigen Argumentation bzw. mit 2.2.6 a) gilt somit, dass die Summe in jeder Zeile bereits Null ergeben muss. Für alle $i \in \{1, \ldots, s\}$ und $j, k \in \{1, \ldots, n_i\}$ mit $j > k$ haben wir dabei $\mathrm{LT}_\tau(q_{ij}g_iq'_{ij}) <_\tau \mathrm{LT}_\tau(q_{ik}g_iq'_{ik})$. Wir erhalten also $n_i = m_i$ und $q_{ij}g_iq'_{ij} = r_{ij}g_ir'_{ij}$. Demnach ist $q_{ij} = r_{ij}$ und $q'_{ij} = r'_{ij}$ für alle $i \in \{1, \ldots, s\}$ und $j \in \{1, \ldots, n_i\}$. □

Das Element $p \in F$ in der Ausgabe des Algorithmus wird auch der **normale Rest** $\mathrm{NR}_{\tau,\mathcal{G}}(m)$ von m bzgl. $\mathcal{G} = (g_1, \ldots, g_s)$ genannt. Er hängt i. Allg. von der Reihenfolge der Elemente $g_1, \ldots, g_s$ ab. Der nächste Abschnitt wird in diesem Zusammenhang zeigen, dass dies nicht der Fall ist, wenn $\{g_1, \ldots, g_s\}$ eine τ-Gröbnerbasis von $\langle g_1, \ldots, g_s\rangle$ ist.

2.4 Termersetzungssysteme

In diesem Abschnitt werden wir für eine Teilmenge $G \subseteq F$ eine Relation auf den Elementen von F einführen. Für zwei Elemente m_1 und m_2, die in Relation stehen, ist dann $m_1 - m_2$ in dem von G erzeugten zweiseitigen Untermodul von F enthalten. Hier lässt sich auch schon der enge Zusammenhang mit dem Divisionsalgorithmus erkennen. Denn für $m \in F$ wissen wir bereits, dass $m - \mathrm{NR}_{\tau,\mathcal{G}}(m) \in \langle G\rangle$ gilt. Dem normalen Rest $\mathrm{NR}_{\tau,\mathcal{G}}(m)$ wird dabei noch eine gesonderte Bedeutung zugewiesen.

Definition 2.4.1 Seien $g, m \in F$.

1) Existieren ein Term $w_1e_iw'_1 \in \mathrm{Supp}(m)$ und Elemente $w_2, w'_2 \in \Sigma^*$ mit $w_2\mathrm{LT}_\tau(g)w'_2 = w_1e_iw'_1$, dann sagen wir g **reduziert** m **in einem Schritt** zu $m' = m - \frac{c}{\mathrm{LC}(g)}w_2gw'_2$. Wir notieren dies mit $m \xrightarrow{g} m'$. Hierbei ist c der Koeffizient von $w_1e_iw'_1$ in m.
2) Für $G \subseteq F$ bezeichne $\xrightarrow{G}$ den reflexiven und transitiven bzw. $\xleftrightarrow{G}$ den reflexiven, symmetrischen und transitiven Abschluss von $\bigcup_{g\in G} \xrightarrow{g}$. Die Relation $\xrightarrow{G}$ heißt Reduktions- oder **Termersetzungssystem**.

3) Ein Element $f \in F$ heißt **irreduzibel** bzgl. $\xrightarrow{G}$, falls es kein $g \in G$ und kein $f' \in F\backslash\{f\}$ gibt mit $f \xrightarrow{G} f'$.
4) Ein Termersetzungssystem $\xrightarrow{G}$ heißt **noethersch**, falls es keine unendliche Reduktionskette gibt. Es heißt **konfluent**, falls für alle $f, f_1, f_2 \in F$ mit $f \xrightarrow{G} f_1$ und $f \xrightarrow{G} f_2$ ein Element $f_3 \in F$ existiert mit $f_1 \xrightarrow{G} f_3$ und $f_2 \xrightarrow{G} f_3$. Es heißt **lokal konfluent**, falls für alle $g_1, g_2 \in G$ und $f, f_1, f_2 \in F$ mit $f \xrightarrow{g_1} f_1$ und $f \xrightarrow{g_2} f_2$ ein Element $f_3 \in F$ existiert mit $f_1 \xrightarrow{G} f_3$ und $f_2 \xrightarrow{G} f_3$. Ein noethersches und konfluentes Termersetzungssystem heißt **konvergent**.

Bemerkung 2.4.2 Sei $G \subseteq F\backslash\{0\}$.

a) Das Termersetzungssystem $\xrightarrow{G}$ ist stets noethersch. Denn angenommen, es gibt eine unendliche absteigende Reduktionskette $f_1 \xrightarrow{g_1} f_2 \xrightarrow{g_2} \cdots$ mit $f_i \in F$ und $g_i \in G$ für alle $i \in \mathbb{N}$. Dann ergibt sich aber durch $\mathrm{LT}_\tau(f_1) \geq_\tau \mathrm{LT}_\tau(f_2) \geq_\tau \cdots$ eine unendliche absteigende Kette von Termen im Widerspruch dazu, dass τ eine Wohlordnung ist. Also ist $\xrightarrow{G}$ noethersch.
b) Es lässt sich zeigen, dass das Termersetzungssytem $\xrightarrow{G}$ genau dann konfluent ist, wenn es lokal konfluent ist. Ein Beweis hierfür findet sich z.B. in [4], Theorem 4.

Beispiel 2.4.3

a) Wir betrachten wieder Beispiel 2.3.1. Dabei ergibt sich $m \xrightarrow{g_2} x_1e_1x_2x_1^2 + x_1^2x_2e_2 + x_2e_2x_2 + e_2 \xrightarrow{g_1} x_2e_2x_2 - x_1e_2 + e_2 = \mathrm{NR}_{\tau,(g_1,g_2)}(m)$. Wir erhalten mit $\mathrm{NR}_{\tau,(g_1,g_2)}(m)$ ein irreduzibles Element.
b) In Beispiel 2.2.10 b) haben wir gesehen, dass für $g_1 = x_1^2e_1x_2 + x_1e_1$ und $g_2 = e_1x_2^2 + e_2$ die Menge $G = \{g_1, g_2\}$ keine τ- Gröbnerbasis des Moduls $M = \langle g_1, g_2\rangle$ ist. Wir wollen nun $m = x_1^2e_1x_2^2$ bzgl. G reduzieren. Nun ergeben sich zwei Möglichkeiten. Entweder reduzieren wir mit g_1 und erhalten $m \xrightarrow{G} -x_1e_1x_2$ oder mit g_2, was zu $m \xrightarrow{G} -x_1^2e_2$ führt. Beide Ergebnisse stellen bzgl. $\xrightarrow{G}$ irreduzible Elemente dar, sind aber verschieden. Also ist $\xrightarrow{G}$ nicht konfluent.

Das letzte Beispiel zeigt, dass auch die Eigenschaften eines Termersetzungssystems $\xrightarrow{G}$ davon abhängen, ob G eine τ-Gröbnerbasis ist oder nicht. Diese Aussage soll der nächste Satz konkretisieren.

Satz 2.4.4 *Sei M ein zweiseitiger Untermodul von F mit Erzeugendensystem $G \subseteq M\backslash\{0\}$. Dann sind folgende Aussagen äquivalent:*

a) G ist eine τ-Gröbnerbasis von M.
b) Das Termersetzungssystem $\xrightarrow{G}$ ist konvergent.
c) Zu jedem $m \in F$ existiert genau ein irreduzibles Element $\mathrm{NF}_{\tau,M}(m) \in F$ mit $m \xrightarrow{G} \mathrm{NF}_{\tau,M}(m)$.
d) Für ein Element $m \in F$ gilt $m \xrightarrow{G} 0$ genau dann, wenn $m \in M$.

Beweis. Um a) $\Rightarrow$ b) zu zeigen, sei G also eine τ-Gröbnerbasis von M. Nach Bemerkung 2.4.2 a) ist das Termersetzungssystem $\xrightarrow{G}$ noethersch.

Zum Beweis der Konfluenz seien $m, m_1, m_2 \in F$ mit $m \xrightarrow{G} m_1$ und $m \xrightarrow{G} m_2$. Wir erhalten nun durch endlich viele Reduktionen irreduzible Elemente $m_1', m_2' \in F$ mit $m_1 \xrightarrow{G} m_1'$ und $m_2 \xrightarrow{G} m_2'$. Dann ist $m_1' - m_2' \in M$ und wieder irreduzibel. Da G eine τ-Gröbnerbasis von M ist, gäbe es für $m_1' - m_2' \neq 0$ ein $g \in G$, so dass der Leitterm von $m_1' - m_2'$ ein Vielfaches von $\mathrm{LT}_\tau(g)$ ist. Dies steht im Widerspruch zur Irreduzibilität von $m_1' - m_2'$, womit $m_1' = m_2'$ folgt.

Wir wollen nun b) $\Rightarrow$ c) beweisen. Sei dazu $m \in F$. Da das Termersetzungssystem $\xrightarrow{G}$ stets noethersch ist, ist die Existenz eines irreduziblen Elements $\mathrm{NF}_{\tau,M}(m) \in F$ mit $m \xrightarrow{G} \mathrm{NF}_{\tau,M}(m)$ gegeben. Für den Beweis der Eindeutigkeit nehmen wir an, dass es ein zweites irreduzibles Element $m' \in F$ gibt mit $m \xrightarrow{G} m'$. Wegen der Konfluenz von $\xrightarrow{G}$ existiert nun ein Element $m'' \in F$ mit $\mathrm{NF}_{\tau,M}(m) \xrightarrow{G} m''$ und $m' \xrightarrow{G} m''$. Mit der Irreduzibilität von $\mathrm{NF}_{\tau,M}(m)$ und m' folgt dann aber $\mathrm{NF}_{\tau,M}(m) = m'' = m'$.

Für den Beweis von c) $\Rightarrow$ d) sei zunächst $m \in F$ mit $m \xrightarrow{G} 0$. D.h. es existieren Elemente $g_1, \ldots, g_k \in G$ und $m_1, \ldots, m_{k-1} \in F$ für ein $k \in \mathbb{N}$ mit $m \xrightarrow{g_1} m_1 \xrightarrow{g_2} \cdots \xrightarrow{g_{k-1}} m_{k-1} \xrightarrow{g_k} 0$. Also lässt sich m schreiben als $m = \sum_{i=1}^{k} c_i w_i g_i w_i'$, wobei $c_i \in K\backslash\{0\}$ und $w_i, w_i' \in \Sigma^*$ für $i = 1, \ldots, k$. Da nun G ein Erzeugendensystem von M ist, folgt $m \in M$.

Umgekehrt sei jetzt $m \in M$ gegeben. Dann lässt sich m mit Hilfe von Elementen $g_1, \ldots, g_k$ des Erzeugendensystems G darstellen. Dies induziert $m \xrightarrow{\{g_1,\ldots,g_k\}} 0$. Da 0 nun ein irreduzibles Element und nach c) die Normalform von m eindeutig bestimmt ist, erhalten wir auch $m \xrightarrow{G} 0$.

Um die Implikation d) $\Rightarrow$ a) zu zeigen, sei $m \in M$ beliebig. Mit d) gilt nun $m \xrightarrow{G} 0$, d.h. es existieren Elemente $g_1, \ldots, g_k \in G$, $m_2, \ldots, m_k \in F$ für ein $k \in \mathbb{N}$, so dass $m = m_1 \xrightarrow{g_1} m_2 \xrightarrow{g_2} \cdots \xrightarrow{g_{k-1}} m_k \xrightarrow{g_k} 0$. Es lässt sich m also darstellen als $m = \sum_{i=1}^{k} c_i w_i g_i w_i'$ mit $c_i \in K\backslash\{0\}$ und $w_i, w_i' \in \Sigma^*$ für $i = 1, \ldots, k$. Im i-ten Schritt der Reduktion wird dabei immer ein Term von m_i durch kleinere bzgl. der Modultermordnung τ ersetzt. Da die Reduktionskette bei 0 endet, muss dies auch für den Leitterm von m in einem der Schritte

gelten. Damit erhalten wir $\mathrm{LT}_\tau(m) \geq_\tau \mathrm{LT}_\tau(w_i g_i w_i')$ für alle $i \in \{1, \ldots, k\}$. Mit Satz 2.2.11 folgt nun die Behauptung. □

Definition 2.4.5 Für einen zweiseitigen Untermodul M von F und ein Element $m \in F$ heißt das oben beschriebene Element $\mathrm{NF}_{\tau,M}(m)$ die **Normalform** von m bzgl. τ.

Es lässt sich in diesem Zusammenhang zeigen, dass die Normalform eines Elements nicht von der gewählten τ-Gröbnerbasis G von M abhängt, sondern nur von der Modultermordnung τ und M selbst.

Bemerkung 2.4.6 Mit der Aussage d) in Satz 2.4.4 lässt sich die Zugehörigkeit eines Elements m zu einem zweiseitigen Modul M prüfen. Dazu muss zunächst eine τ-Gröbnerbasis G von M berechnet und anschließend getestet werden, ob die Normalform von m bzgl. des zugehörigen Termersetzungssystems $\xrightarrow{G}$ gleich Null ist.

Wir wollen nun einige einfache Eigenschaften der Normalform angeben. Es wird sich dabei herausstellen, dass für eine endliche τ- Gröbnerbasis die Normalform eines Elements gleich dem normalen Rest aus dem Divisionsalgorithmus ist.

Korollar 2.4.7 *Sei M ein zweiseitiger Untermodul von F mit τ-Gröbnerbasis $G \subseteq M \backslash \{0\}$. Dann gilt für $m, m_1, m_2 \in F$:*

a) $\mathrm{NF}_{\tau,M}(m_1 + m_2) = \mathrm{NF}_{\tau,M}(m_1) + \mathrm{NF}_{\tau,M}(m_2)$,
b) $\mathrm{NF}_{\tau,M}(\mathrm{NF}_{\tau,M}(m)) = \mathrm{NF}_{\tau,M}(m)$.
c) Ist $G = \{g_1, \ldots, g_s\}$, so stimmen für $\mathcal{G} = (g_1, \ldots, g_s)$ die Normalform $\mathrm{NF}_{\tau,M}(m)$ und der normale Rest $\mathrm{NR}_{\tau,\mathcal{G}}(m)$ überein.

Beweis. Für den Beweis von a) seien $m_1, m_2 \in F$. Hieraus folgt zunächst

$$\begin{aligned} & m_1 + m_2 - (\mathrm{NF}_{\tau,M}(m_1) + \mathrm{NF}_{\tau,M}(m_2)) \\ = & \underbrace{(m_1 - \mathrm{NF}_{\tau,M}(m_1))}_{\in M} + \underbrace{(m_2 - \mathrm{NF}_{\tau,M}(m_2))}_{\in M} \in M. \end{aligned}$$

Es ergibt sich also $m_1 + m_2 \xrightarrow{G} \mathrm{NF}_{\tau,M}(m_1) + \mathrm{NF}_{\tau,M}(m_2)$. Weiter ist das Element $\mathrm{NF}_{\tau,M}(m_1) + \mathrm{NF}_{\tau,M}(m_2)$ irreduzibel bzgl. $\xrightarrow{G}$ und damit die nach Satz 2.4.4 eindeutig bestimmte Normalform von $m_1 + m_2$.

Der Beweis von b) beruht auf der Tatsache, das die Normalform von m bereits irreduzibel bzgl. $\xrightarrow{G}$ ist. Die Normalform eines irreduziblen Elements ist nun wegen der eben erwähnten Eindeutigkeit stets das Element selbst.

Bleibt noch c) zu beweisen. Dazu sei $m \in F$ und $\mathcal{G} = (g_1, \ldots, g_s)$. Wir erhalten mit $\mathrm{NR}_{\tau,\mathcal{G}}(m)$ ein irreduzibles Element, denn jeder Term im Träger von $\mathrm{NR}_{\tau,\mathcal{G}}(m)$ ist nach Satz 2.3.2 b) nicht in $\mathrm{LT}_\tau\{M\} = \langle \mathrm{LT}_\tau(g_1), \ldots, \mathrm{LT}_\tau(g_s)\rangle$ enthalten. Da weiter $m - \mathrm{NR}_{\tau,\mathcal{G}}(m) \in M$ ist, gilt $m \xrightarrow{G} \mathrm{NR}_{\tau,\mathcal{G}}(m)$. Damit folgt insgesamt $\mathrm{NR}_{\tau,\mathcal{G}}(m) = \mathrm{NF}_{\tau,M}(m)$. □

Für endliche Gröbnerbasen entsprechen sich also die Begriffe der Normalform und des normalen Rests. Damit hängt auch der normale Rest nicht mehr von der Reihenfolge der Elemente in $\mathcal{G}$ ab und ist somit eindeutig bestimmt.

2.5 Der Buchberger-Algorithmus

In diesem Abschnitt geben wir eine Prozedur an, mit der wir anhand eines endlichen Erzeugendensystems eines zweiseitigen Untermoduls M von F eine τ-Gröbnerbasis G von M berechnen können. Es handelt sich dabei um eine sogenannte *aufzählende Prozedur*, d.h. sie muss nicht zwangsläufig terminieren und die Vereinigung aller im Verlauf der Prozedur berechneten Elemente liefert eine τ-Gröbnerbasis von M.

Die zugrundeliegende Idee dabei ist zu überprüfen, ob das gegebene Erzeugendensystem bereits eine τ-Gröbnerbasis ist. Ist dies nicht der Fall, so wird es durch geeignete Elemente solange erweitert, bis es die Bedingungen einer τ-Gröbnerbasis erfüllt. Wir haben bereits gesehen, dass dies gewährleistet ist, falls für jedes Element $m \in M$ der normale Rest $\mathrm{NR}_{\tau,\mathcal{G}}(m)$ gleich Null ist. Nun ist es natürlich nicht effektiv, dies für jedes Element nachzuweisen. Aber es lässt sich zeigen, dass es genügt, nur ganz bestimmte Elemente auf diese Bedingung hin zu überprüfen, die sogenannten *S-Vektoren*.

Definition 2.5.1 Sei I eine Indexmenge und $G = \{g_i \,|\, i \in I\} \subseteq F\backslash\{0\}$. Ein Paar (i,j) mit $i,j \in I$ und $i < j$ heißt **kritisches Paar** von G, falls Terme $w_i, w_i', w_j, w_j' \in \Sigma^*$ existieren, so dass $w_i \mathrm{LT}_\tau(g_i) w_i' = w_j \mathrm{LT}_\tau(g_j) w_j'$ gilt. Die Menge aller kritischen Paare sei mit B bezeichnet. Zu jedem solchen kritischen Paar (i,j) ist der **S-Vektor** wie folgt definiert:

$$S_{ij} = \tfrac{1}{\mathrm{LC}_\tau(g_i)} w_i g_i w_i' - \tfrac{1}{\mathrm{LC}_\tau(g_j)} w_j g_j w_j',$$

wobei $w_i, w_i', w_j, w_j' \in \Sigma^*$ so gewählt sind, dass w_i und w_j kein gemeinsames Präfix bzw. w_i' und w_j' kein gemeinsames Suffix haben.

Dass die Betrachtung der S-Vektoren eines Erzeugendensystems G von M tatsächlich ausreicht, um G als eine τ-Gröbnerbasis von M zu identifizieren, zeigt der folgende Satz.

Satz 2.5.2 (Das Buchberger-Kriterium)
Sei $G = \{g_i \mid i \in I\} \subseteq F\backslash\{0\}$ mit einer Indexmenge I, sei M der von G zweiseitig erzeugte Untermodul von F und B die Menge der kritischen Paare von G. Dann ist G genau dann eine τ-Gröbnerbasis von M, wenn $S_{ij} \xrightarrow{G} 0$ für alle Paare $(i,j) \in B$.

Beweis. Ist G eine τ-Gröbnerbasis von M, so gilt nach Satz 2.4.4, dass $m \xrightarrow{G} 0$ für alle $m \in M$. Nun ist der S-Vektor S_{ij} ein Element von M für jedes kritische Paar $(i,j) \in B$. Damit gilt also $S_{ij} \xrightarrow{G} 0$.

Gelte nun umgekehrt $S_{ij} \xrightarrow{G} 0$ für jedes kritische Paar (i,j) von G. Nach Satz 2.4.4 und Bemerkung 2.4.2 b) genügt es zu zeigen, dass das Termersetzungssystem $\xrightarrow{G}$ lokal konfluent ist. Seien dazu $m, m_1, m_2 \in M$, so dass gilt $m \xrightarrow{g_i} m_1$ und $m \xrightarrow{g_j} m_2$ mit $g_i, g_j \in G$. Wir müssen nun ein Element $m_3 \in M$ finden mit $m_1 \xrightarrow{G} m_3$ und $m_2 \xrightarrow{G} m_3$. Sei $m_1 = m - c_i w_i g_i w_i'$ und $m_2 = m - c_j w_j g_j w_j'$, wobei $c_i, c_j \in K\backslash\{0\}$ und $w_i, w_i', w_j, w_j' \in \Sigma^*$. Angenommen, es gilt $w_i \mathrm{LT}_\tau(g_i) w_i' \neq w_j \mathrm{LT}_\tau(g_j) w_j'$. Dann sei O.B.d.A. $w_i \mathrm{LT}_\tau(g_i) w_i' >_\tau w_j \mathrm{LT}_\tau(g_j) w_j'$. Gilt nun $w_j \mathrm{LT}_\tau(g_j) w_j' \notin \mathrm{Supp}(w_i g_i w_i')$, so erhalten wir mit $m_3 = m - c_i w_i g_i w_i' - c_j w_j g_j w_j'$ ein Element in M und die Reduktionsschritte $m_1 \xrightarrow{g_j} m_3$ und $m_2 \xrightarrow{g_i} m_3$. Für den Fall $w_j \mathrm{LT}_\tau(g_j) w_j' \in \mathrm{Supp}(w_i g_i w_i')$ ergibt sich das Element $m_3 = m - c_i w_i g_i w_i' - (c_j - \frac{c_i c}{\mathrm{LC}_\tau(g_j)}) w_j g_j w_j'$, wobei $c \in K\backslash\{0\}$ der Koeffizient von $w_j \mathrm{LT}_\tau(g_j) w_j'$ in $w_i g_i w_i'$ ist. Die zugehörigen Reduktionsschritte sind $m_1 \xrightarrow{g_j} m_3$ und $m_2 \xrightarrow{g_i} m - c_i w_i g_i w_i' - c_j w_j g_j w_j' \xrightarrow{g_j} m_3$.

Sei also nun $w_i \mathrm{LT}_\tau(g_i) w_i' = w_j \mathrm{LT}_\tau(g_j) w_j'$. Dann ist $m_2 - m_1 = c_i w_i g_i w_i' - c_j w_j g_j w_j' = c_i \mathrm{LC}_\tau(g_i) S_{ij}$ und es folgt nach Voraussetzung $m_2 - m_1 \xrightarrow{G} 0$. Wir erhalten also eine Reduktionskette der Form

$$m_2 - m_1 \xrightarrow{g_{i_1}} m_2 - m_1 - c_{i_1} w_{i_1} g_{i_1} w_{i_1}' = f_1 \xrightarrow{g_{i_2}} \cdots \xrightarrow{g_{i_k}} f_k = 0,$$

wobei $k \in \mathbb{N}_0$, $c_{i_l} \in K\backslash\{0\}$, $w_{i_l} w_{i_l}' \in \Sigma^*$ und $g_{i_l} \in G$ für $l = 1, \ldots, k$. Ist c_1' der Koeffizient von $w_{i_1} \mathrm{LT}_\tau(g_{i_1}) w_{i_1}'$ in m_1 bzw. c_2' der Koeffizient in m_2, so gilt $c_1' \neq c_2'$ und $c_{i_1} = c_2' - c_1'$. Es ergeben sich damit die Reduktionsschritte $m_1 \xrightarrow{g_{i_1}} m_1 - c_1' w_{i_1} g_{i_1} w_{i_1}' = h_1$ und $m_2 \xrightarrow{g_{i_1}} m_2 - c_2' w_{i_1} g_{i_1} w_{i_1}' = h_1'$. Also ist $f_1 = h_1' - h_1$. Mit Induktion nach k folgt nun, dass Elemente $h_k, h_k' \in M$ existieren mit $m_1 \xrightarrow{G} h_k$, $m_2 \xrightarrow{G} h_k'$ und $f_k = h_k' - h_k = 0$. Somit erhalten wir das gesuchte Element $m_3 = h_k = h_k'$ und die lokale Konfluenz des Termersetzungssytems $\xrightarrow{G}$. □

Mit obigem Kriterium gelangen wir nun zu der folgenden Prozedur. Dabei werden aus der Menge B Elemente mit einer „fairen Strategie“ entnom-

men. Der Begriff „fair“ soll dabei andeuten, dass jedes Element, welches irgendwann zu B hinzugefügt wurde, auch tatsächlich im Laufe der Prozedur gewählt wird. Eine faire Strategie könnte z.B. darin bestehen, die Menge B als Liste zu interpretieren, wobei stets das erste Element der Liste ausgewählt und jedes neue am Ende angefügt wird.

Satz 2.5.3 (Der Buchberger-Algorithmus)
Sei $G = \{g_1, \ldots, g_s\} \subseteq F\backslash\{0\}$, sei M der von G erzeugte zweiseitige Untermodul von F und $\mathcal{G} = (g_1, \ldots, g_s)$. Wir betrachten die folgenden Instruktionen:

1) Sei $s' = s$ und B die Menge der kritischen Paare von G.
2) Ist $B = \emptyset$, gib $\mathcal{G}$ aus und stoppe. Andernfalls wähle ein Paar $(i, j) \in B$ unter Verwendung einer fairen Strategie und entferne es aus B.
3) Berechne den S-Vektor S_{ij} und den normalen Rest $\mathrm{NR}_{\tau,\mathcal{G}}(S_{ij})$. Ergibt sich $\mathrm{NR}_{\tau,\mathcal{G}}(S_{ij}) = 0$, so fahre mit Schritt 2) fort.
4) Erhöhe s' um 1. Füge $g_{s'} = \mathrm{NR}_{\tau,\mathcal{G}}(S_{ij})$ zu $\mathcal{G}$ und die Menge der Paare $\{(i, s') \mid 1 \leq i < s' \text{ und } (i, s') \text{ bildet ein kritisches Paar}\}$ zu B hinzu. Fahre dann mit Schritt 2) fort.

Dies ist eine Prozedur, die eine τ-Gröbnerbasis G von M aufzählt. D.h. die Vereinigung aller derjenigen Elemente, die im Verlauf der Prozedur in Schritt 4) zu $\mathcal{G}$ hinzugefügt werden, mit der gegebenen Menge G bildet eine τ-Gröbnerbasis von M. Besitzt M eine endliche τ-Gröbnerbasis, so stoppt sie nach endlich vielen Schritten und das ausgegebene Tupel $\mathcal{G}$ ist eine endliche τ-Gröbnerbasis von M.

Beweis. Wir wollen zunächst zeigen, dass die Prozedur tatsächlich eine τ-Gröbnerbasis berechnet. Nach Satz 2.5.2 muss dazu geprüft werden, ob für jedes kritische Paar (i, j), das irgendwann im Verlauf der Prozedur zu B hinzugefügt wird, der zugehörige S-Vektor zu Null reduziert. Zuerst ist festzustellen, dass aufgrund der in Schritt 2) fair gewählten Strategie jedes kritische Paar auch bearbeitet wird. Für ein solches Paar (i, j) wird nun in Schritt 3) der normale Rest des zugehörigen S-Vektors S_{ij} berechnet. Entweder ist dieser bereits gleich Null oder es wird ein neues Element $g_{s'}$ zu $\mathcal{G}$ hinzugefügt, das nun S_{ij} zu Null reduziert.

Es bleibt jetzt noch zu beweisen, dass bei der Existenz einer endlichen τ-Gröbnerbasis $G' = \{g'_1, \ldots, g'_k\}$ von M die Prozedur auch terminiert. Sei dazu G die von der Prozedur aufgezählte τ-Gröbnerbasis. Dann existiert zu jedem $j \in \{1, \ldots, k\}$ ein Element $g_{i_j} \in G$, so dass $\mathrm{LT}_\tau(g_j)$ ein Vielfaches von $\mathrm{LT}_\tau(g_{i_j})$ ist. Wir erhalten also

$$\begin{aligned}\mathrm{LT}_\tau\{M\} &= \{w_1\mathrm{LT}_\tau(g'_j)w_2 \,|\, j \in \{1,\dots,k\}, w_1, w_2 \in \Sigma^*\} \\ &\subseteq \{w_1\mathrm{LT}_\tau(g_{i_j})w_2 \,|\, j \in \{1,\dots,k\}, w_1, w_2 \in \Sigma^*\} \\ &\subseteq \{w_1\mathrm{LT}_\tau(g_i)w_2 \,|\, i \in \{1,\dots,\max\{i_1,\dots,i_k\}\}, w_1, w_2 \in \Sigma^*\} \\ &\subseteq \mathrm{LT}_\tau\{M\}\end{aligned}$$

und damit eine τ-Gröbnerbasis $\{g_1,\dots,g_{\max\{i_1,\dots,i_k\}}\}$ von M. Wurde nun also das Element $g_{\max\{i_1,\dots,i_k\}}$ an das Tupel $\mathcal{G}$ angehängt, so reduzieren alle S_{ij} zu 0. Es wird also durch die Prozedur kein weiteres Element an $\mathcal{G}$ angefügt und alle Paare $(i,j) \in B$ werden abgearbeitet, d.h. die Prozedur endet. □

Wir haben also nun die Möglichkeit, Gröbnerbasen zu berechnen. Diese sind nicht immer bzw. nur selten endlich. Es kann also passieren, dass die Prozedur nicht endet. In diesem Fall wird sie häufig zu einem gewissen Zeitpunkt abgebrochen und die bis dahin berechneten Elemente der Gröbnerbasis ausgewertet. Es wird oft keine vollständige Gröbnerbasis benötigt. Zumeist interessieren nur Elemente bis zu einem bestimmten Grad, so dass diese Ergebnisse ausreichen.

Des Weiteren stellt die angegebene Prozedur nur die Grundform des Buchberger-Algorithmus dar. Sie lässt sich noch zum Zweck der Effizienz an vielen Stellen optimieren. So bleibt hier zum Beispiel offen, mit welcher Strategie das jeweils nächste kritische Paar ausgewählt wird.

Wir wollen den Buchberger-Algorithmus nun an einem Beispiel demonstrieren.

Beispiel 2.5.4 Sei $K = \mathbb{Q}$ und $\Sigma = \{x_1, x_2\}$. Weiter sei F der freie von $\{e_1, e_2\}$ zweiseitig erzeugte $Q[\Sigma^*]$-Modul und $\tau = \texttt{PosLLex}$ die gewählte Modultermordnung.

a) Sei $M = \langle g_1, g_2\rangle$ ein zweiseitiger Untermodul von F und $\mathcal{G} = (g_1, g_2)$ mit $g_1 = x_2x_1e_1x_2 + e_1$ und $g_2 = e_1x_2^2 + x_1e_2$. Wir erhalten also zunächst $B = \{(1,2)\}$, wählen das kritische Paar $(1,2)$ und entfernen es aus B. Als zugehöriger S-Vektor ergibt sich

$$S_{12} = g_1x_2 - x_2x_1g_2 = e_1x_2 - x_2x_1^2e_2 =: g_3.$$

Es ist nun $g_3 = \mathrm{NR}_{\tau,\mathcal{G}}(S_{12})$ und nach Schritt 4) haben wir $\mathcal{G} = (g_1, g_2, g_3)$ und $B = \{(1,3),(2,3)\}$. Wir wählen $(1,3)$ als nächstes Paar mit

$$S_{13} = g_1 - x_2x_1g_3 = e_1 + x_2x_1x_2x_1^2e_2 =: g_4.$$

Es gilt wieder, dass $g_4 = \mathrm{NR}_{\tau,\mathcal{G}}(S_{13})$ und damit $\mathcal{G} = (g_1, g_2, g_3, g_4)$ sowie $B = \{(2,3),(1,4),(2,4),(3,4)\}$. Für das Paar $(2,3)$ ergibt sich der S-Vektor

$$S_{23} = g_2 - g_3x_2 = x_2x_1^2e_2x_2 + x_1e_2 =: g_5.$$

Mit $g_5 = \mathrm{NR}_{\tau,\mathcal{G}}(S_{23})$ erhalten wir das Tupel $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ und $B = \{(1,4),(2,4),(3,4)\}$. Es lässt sich weiter Folgendes berechnen:

$$\begin{aligned} S_{14} &= g_1 - x_2x_1g_4x_2 = e_1 - x_2x_1x_2x_1x_2x_1^2e_2x_2 \\ &\xrightarrow{g_4} -x_2x_1x_2x_1x_2x_1^2e_2x_2 - x_2x_1x_2x_1^2e_2 \\ &\xrightarrow{g_5} x_2x_1x_2x_1^2e_2 - x_2x_1x_2x_1^2e_2 = 0, \\ S_{24} &= g_2 - g_4x_2^2 = -x_2x_1x_2x_1^2e_2x_2^2 + x_1e_2 \\ &\xrightarrow{g_5} x_2x_1^2e_2x_2 + x_1e_2 \xrightarrow{g_5} -x_1e_2 + x_1e_2 = 0, \\ S_{34} &= g_3 - g_4x_2 = -x_2x_1x_2x_1^2e_2x_2 - x_2x_1^2e_2 \\ &\xrightarrow{g_5} x_2x_1^2e_2 - x_2x_1^2e_2 = 0. \end{aligned}$$

Demnach endet die Prozedur und gibt das Tupel $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ als τ-Gröbnerbasis von M aus. Hierbei ist zu bemerken, dass auch $\{g_4, g_5\}$ eine τ-Gröbnerbasis von M ist, da $\mathrm{LT}_\tau(g_1)$, $\mathrm{LT}_\tau(g_2)$ und $\mathrm{LT}_\tau(g_3)$ Vielfache von $\mathrm{LT}_\tau(g_4)$ sind.

b) Ändern wir die Elemente g_1 und g_2 nur geringfügig ab, so erhalten wir ein ganz anderes Ergebnis. Sei also $g_1 = x_2x_1e_1x_2 + e_2$ und $g_2 = e_1x_2^2 + x_1e_1$. Wir starten wieder mit $\mathcal{G} = (g_1, g_2)$ und $B = \{(1,2)\}$. Für das Paar $(1,2)$ ergibt sich hierbei der S-Vektor

$$S_{12} = g_1x_2 - x_2x_1g_2 = -x_2x_1^2e_1 + e_2x_2 = \mathrm{NR}_{\tau,\mathcal{G}}(S_{12}) =: g_3$$

und es ist $\mathcal{G} = (g_1, g_2, g_3)$ bzw. $B = \{(2,3)\}$. Wir entfernen das Paar $(2,3)$ aus B und erhalten

$$S_{23} = x_2x_1^2g_2 + g_3x_2^2 = x_2x_1^3e_1 + e_2x_2^3 = \mathrm{NR}_{\tau,\mathcal{G}}(S_{23}) =: g_4.$$

Damit ist nun $\mathcal{G} = (g_1, g_2, g_3, g_4)$ und $B = \{(2,4)\}$. Der S-Vektor für das Paar $(2,4)$ ist

$$S_{24} = x_2x_1^3g_2 - g_4x_2^2 = x_2x_1^4e_1 - e_2x_2^5 = \mathrm{NR}_{\tau,\mathcal{G}}(S_{24}) =: g_5$$

Es ergibt sich also $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5)$ bzw. $B = \{(2,5)\}$. Es lässt sich erkennen, dass sich die Prozedur im weiteren Verlauf analog zu den letzten Schritten verhält. D.h. der zu berechnende S-Vektor des jeweiligen kritischen Paares in B hat stets eine von Null verschiedene Normalform und B wird um genau ein neues Paar ergänzt. Die Prozedur wird nicht enden. Also besitzt M keine endliche τ-Gröbnerbasis.

Das Beispiel in a) hat gezeigt, dass es Elemente in einer τ-Gröbnerbasis G geben kann, ohne die G immer noch eine τ-Gröbnerbasis bildet. Das führt uns zu einer speziellen Art von τ-Gröbnerbasen. Bevor wir diese definieren, benötigen wir noch folgendes theoretische Detail.

Satz 2.5.5 *Sei M ein zweiseitiger monomialer Untermodul von F. Dann besitzt M genau ein minimales Erzeugendensystem.*

Beweis. Da M ein monomialer Modul ist, existiert ein Erzeugendensystem $G \subseteq M$ bestehend aus Termen in $\mathbb{T}(F)$. Werden aus dieser Menge nun alle Elemente entfernt, die Vielfache eines anderen sind, so erhalten wir eine Menge $G_1 \subseteq G$, die nicht weiter verkleinert werden kann. Dies zeigt die Existenz eines minimalen Erzeugendensystems.

Für den Beweis der Eindeutigkeit sei G_2 ein weiteres minimales Erzeugendensystem von M. Zu einem Element $g \in G_1$ gibt es nun ein $h \in G_2$, so dass gilt $g = w_1 h w_1'$ für geeignete $w_1, w_1' \in \Sigma^*$. Analog existiert zu h aber auch ein $g' \in G_1$ und $w_2, w_2' \in \Sigma^*$ mit $h = w_2 g' w_2'$. Es folgt also $g = w_1 h w_1' = w_1 w_2 g' w_2' w_1'$ und wegen der Minimalität von G_1 daher $g = g' = h$. Wir haben damit $G_1 \subseteq G_2$ gezeigt. Die andere Inklusion folgt nun analog. □

Definition 2.5.6 Sei M ein zweiseitiger Untermodul von F. Eine τ-Gröbnerbasis $G \subseteq M\backslash\{0\}$ von M heißt **reduzierte τ-Gröbnerbasis** von M, wenn folgende Bedingungen erfüllt sind:

1) $\mathrm{LC}_\tau(g) = 1$ für alle $g \in G$.
2) Die Menge $\{\mathrm{LT}_\tau(g) \mid g \in G\}$ ist ein minimales Erzeugendensystem von $\mathrm{LT}_\tau(M)$.
3) $\mathrm{Supp}(g - \mathrm{LT}_\tau(g)) \cap \mathrm{LT}_\tau\{M\} = \emptyset$ für alle $g \in G$.

Bisher war es nicht möglich, eine eindeutige τ-Gröbnerbasis für einen zweiseitigen Modul M anzugeben. Der Begriff der reduzierten τ-Gröbnerbasis liefert hier nun Abhilfe, wie der folgende Satz zeigt.

Satz 2.5.7 *Ist M ein zweiseitiger Untermodul von F, so existiert genau eine reduzierte τ-Gröbnerbasis von M.*

Beweis. Sei $G \subseteq M\backslash\{0\}$ eine τ-Gröbnerbasis von M. Wir ersetzen nun jedes Element $g \in G$ durch $\frac{1}{\mathrm{LC}_\tau(g)} g$. Damit erfüllt G bereits Bedingung 1) aus Definition 2.5.6. Um auch 2) zu erfüllen, entfernen wir jedes Elemente g aus G, dessen Leitterm ein Vielfaches eines Elements der Menge $\{\mathrm{LT}_\tau(f) \mid f \in G\backslash\{g\}\}$ ist. Wir erhalten somit ein minimales Erzeugendensystem $G' \subseteq G$ von M, welches immer noch eine τ-Gröbnerbasis ist.

Für $g \in G'$ schreiben wir nun $g = \mathrm{LT}_\tau(g) + h$ und $g' = \mathrm{LT}_\tau(g) + \mathrm{NF}_{\tau,M}(h)$. Wir zeigen, dass $G'' = \{g' \mid g \in G'\}$ eine reduzierte τ-Gröbnerbasis von M ist. Es ergibt sich zunächst $G'' \subseteq M\backslash\{0\}$, denn für $g' \in G''$ gilt $g' \neq 0$ und

$$g' = g - (\underbrace{h - \mathrm{NF}_{\tau,M}(h)}_{\in M}) \in M.$$

Weiter ist $\mathrm{LT}_\tau(g') = \mathrm{LT}_\tau(g)$ für alle $g' \in G''$ und damit G'' eine τ-Gröbnerbasis von M, die 1) und 2) erfüllt. G'' erfüllt auch 3), denn für $g' \in G''$ ist

$\mathrm{Supp}(g' - \mathrm{LT}_\tau(g')) = \mathrm{Supp}(\mathrm{NF}_{\tau,M}(h)) \subseteq \mathbb{T}(F)\backslash \mathrm{LT}_\tau\{M\}$, da $\mathrm{NF}_{\tau,M}(h)$ irreduzibel bzgl. $\xrightarrow{G'}$ ist.

Es bleibt noch die Eindeutigkeit zu zeigen. Seien dazu G und H zwei reduzierte τ-Gröbnerbasen von M. Für ein $g \in G$ existiert nun ein $h \in H$, so dass $\mathrm{LT}_\tau(g) = w_1\mathrm{LT}_\tau(h)w_2$ für geeignete $w_1, w_2 \in \Sigma^*$. Ebenso muss es ein $g' \in G$ und $w_1', w_2' \in \Sigma^*$ geben mit $\mathrm{LT}_\tau(h) = w_1'\mathrm{LT}_\tau(g')w_2'$. Es folgt also $\mathrm{LT}_\tau(g) = w_1w_1'\mathrm{LT}_\tau(g')w_2'w_2$ und damit $g = g'$, da G nach Voraussetzung die Bedingung 2) erfüllt. Zugleich ergibt sich auch $\mathrm{LT}_\tau(g) = \mathrm{LT}_\tau(h)$. Ferner haben wir $g - h \in M$ und $g - h$ ist nach 3) irreduzibel bzgl. $\xrightarrow{G}$. Mit Satz 2.4.4 gilt demnach $g = h$. Es folgt also $G \subseteq H$ und mit der anderen, analog zu beweisenden Inklusion erhalten wir die geforderte Gleichheit. □

Reduzierte τ-Gröbnerbasen geben uns nun zum Beispiel die Möglichkeit, zwei Moduln auf Gleichheit zu überprüfen. Dazu müssen wir lediglich die jeweiligen reduzierten τ-Gröbnerbasen berechnen und diese auf Gleichheit testen.

2.6 Gröbnerbasen für Ideale

In diesem Abschnitt wollen wir den Spezialfall der zweiseitigen Ideale von $K[\Sigma^*]$ studieren. Um die im vorherigen Abschnitt erarbeitete Gröbnerbasistheorie für zweiseitige Moduln anwenden zu können, ordnen wir jedem zweiseitigen Ideal eineindeutig einen Restklassenmodul eines zweiseitigen Untermoduls zu. Wir betrachten dazu den Fall $r = 1$, d.h. den freien von $\{e\}$ erzeugten zweiseitigen Modul F_1. Im Folgenden wird der zweiseitige Untermodul $N = \langle x_ie - ex_i \,|\, i = 1, \ldots, n\rangle$ von F_1 eine wichtige Rolle spielen. Weiter sei σ stets eine Termordnung auf Σ^* und $\tau = \mathtt{Pos}\sigma$ die zugehörige Modultermordnung auf $\mathbb{T}(F_1)$. Für $G = \{f_1, \ldots, f_s\} \subseteq K[\Sigma^*]$ bezeichne $(f_1, \ldots, f_s)$ das von G erzeugte zweiseitige Ideal von $K[\Sigma^*]$.

Gröbnerbasen für zweiseitige Ideale lassen sich zunächst analog zu denen für Moduln definieren.

Definition 2.6.1 *Sei σ eine Termordnung auf Σ^* und I ein zweiseitiges Ideal von $K[\Sigma^*]$. Eine Menge $G \subseteq I\backslash\{0\}$ heißt* **(zweiseitige) σ-Gröbnerbasis** *von I, falls gilt*

$$\mathrm{LT}_\sigma\{I\} = \{w_1\mathrm{LT}_\sigma(g)w_2 \,|\, g \in G, w_1, w_2 \in \Sigma^*\}.$$

Es lässt sich nun der folgende Zusammenhang zwischen dem Polynomring $K[\Sigma^*]$ und dem Modul F_1 feststellen.

Satz 2.6.2 *Sei N der von $\{x_i e - e x_i \,|\, i = 1, \ldots, n\}$ erzeugte zweiseitige Untermodul von F_1. Dann induziert die Abbildung $\pi : F_1 \longrightarrow K[\Sigma^*]$ mit $\pi(e) = 1$ einen Isomorphismus $\tilde{\pi}$ von F_1/N nach $K[\Sigma^*]$.*

Beweis. Die Abbildung π ist nach der universellen Eigenschaft des freien zweiseitigen Moduls F_1 aus Satz 2.2.2 ein Homomorphismus und offensichtlich surjektiv.

Es bleibt noch $\mathrm{Kern}(\pi) = N$ zu zeigen. Hierbei ist nur die Inklusion „$\subseteq$“ zu beweisen. Wir nehmen dazu an, dass ein Element $m \in \mathrm{Kern}(\pi) \backslash N$ existiert. Dabei sei m so gewählt, dass $\mathrm{LT}_\tau(m)$ minimal ist. Für $m = \sum_{i=1}^{l} c_i w_i e w_i'$ mit $c_i \in K \backslash \{0\}$ und $w_i, w_i' \in \Sigma^*$ für $i = 1 \ldots, l$ ist also $\pi(m) = \sum_{i=1}^{l} c_i w_i w_i' = 0$. In der Menge $\{w_i w_i' \,|\, i = 1, \ldots, l\}$ gibt es nun bzgl. σ ein maximales Element. O.B.d.A. sei dies $w_1 w_1'$. Ist $A = \{k \,|\, k \in \{1, \ldots, l\}, w_k w_k' = w_1 w_1'\}$, so gilt $|A| \geq 2$. Es existiert demnach ein $j \in A$ mit $j \neq 1$. Wir erhalten mit $m' = m - c_1 w_1 e w_1' + c_1 w_j e w_j'$ wieder ein Element im Kern von π, denn $c_1 w_1 e w_1' - c_1 w_j e w_j' \in N$. Dann ist aber $m' \notin N$, weil sonst auch $m = m' + c_1 w_1 e w_1' - c_1 w_j e w_j' \in N$ gelten würde, und $\mathrm{LT}_\tau(m') <_\tau \mathrm{LT}_\tau(m)$ im Widerspruch zur Wahl von m. □

Welche Auswirkung die Quotientenbildung mit dem zweiseitigen Untermodul N hat, zeigt das folgende Resultat.

Lemma 2.6.3 *Seien $\nu \in \mathbb{N}$ und $i_1, \ldots, i_\nu \in \{1, \ldots, n\}$. Dann gilt*

$$e x_{i_1} \cdots x_{i_\nu} \equiv x_{i_1} \cdots x_{i_\mu} e x_{i_{\mu+1}} \cdots x_{i_\nu} \mod N$$

für jedes $\mu \in \{1, \ldots, \nu\}$.

Beweis. Seien $\nu \in \mathbb{N}$, $i_1, \ldots, i_\nu \in \{1, \ldots, n\}$ und $\mu \in \{1, \ldots, \nu\}$. Wir zeigen nun $e x_{i_1} \cdots x_{i_\nu} - x_{i_1} \cdots x_{i_\mu} e x_{i_{\mu+1}} \cdots x_{i_\nu} \in N$ mit Induktion nach μ. Für $\mu = 1$ erhalten wir direkt $e x_{i_1} \cdots x_{i_\nu} - x_{i_1} e x_{i_2} \cdots x_{i_\nu} = (e x_{i_1} - x_{i_1} e) x_{i_2} \cdots x_{i_\nu} \in N$. Sei jetzt $\mu \geq 2$. Dann ist

$$\begin{aligned} & e x_{i_1} \cdots x_{i_\nu} - x_{i_1} \cdots x_{i_\mu} e x_{i_{\mu+1}} \cdots x_{i_\nu} \\ = {} & e x_{i_1} \cdots x_{i_\nu} - x_{i_1} \cdots x_{i_{\mu-1}} e x_{i_\mu} \cdots x_{i_\nu} + x_{i_1} \cdots x_{i_{\mu-1}} (e x_{i_\mu} - x_{i_\mu} e) x_{i_{\mu+1}} \cdots x_{i_\nu}. \end{aligned}$$

Der letzte Summand ist bereits ein Element von N. Nach Induktionsvoraussetzung umfasst N auch den verbleibenden Teil der Summe, womit wir die Behauptung bewiesen haben. □

Die Menge der zweiseitigen Ideale I von $K[\Sigma^*]$ entsprechen via $\tilde{\pi}$ nun eineindeutig der Menge der Restklassenmoduln zweiseitiger Untermoduln von F_1. Dabei ist $\tilde{\pi}$ der von $\pi : F_1 \longrightarrow K[\Sigma^*]$, $\pi(e) = 1$ induzierte Isomorphismus aus Satz 2.6.2.

Lemma 2.6.4 *Sei $G = \{f_1, \ldots, f_s\} \subseteq K[\Sigma^*]\backslash\{0\}$, sei I das von G erzeugte zweiseitige Ideal von $K[\Sigma^*]$, sei $G_I = \{ef_1, \ldots, ef_s\} \subseteq F_1$ und M_I der von G_I erzeugte zweiseitige Untermodul von F_1. Dann ist $\pi^{-1}(I) = M_I + N$.*

Beweis. Da $N = \text{Kern}(\pi)$ gilt, erhalten wir sofort $\pi(M_I + N) = \pi(M_I) \subseteq I$ und damit die Inklusion „$\supseteq$“.

Sei nun umgekehrt $m \in \pi^{-1}(I)$. Dann ist $\pi(m) \in I$, d.h. wir können $\pi(m)$ schreiben als $\pi(m) = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} f_i w'_{ij}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Mit $m - \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e f_i w'_{ij}$ erhalten wir somit ein Element aus Kern(π). Also ist $m \in \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e f_i w'_{ij} + N \subseteq M_I + N$. □

Wir können jetzt unsere Kenntnisse über die Theorie der Gröbnerbasen auf den Modul $\pi^{-1}(I)$ anwenden. Die dabei gewonnenen Ergebnisse übertragen wir anschließend durch den Homomorphismus π auf das Ideal I. Auf diesem Weg lässt sich nun eine Gröbnerbasis von I bestimmen.

Satz 2.6.5 *Sei $G = \{f_1, \ldots, f_s\} \subseteq K[\Sigma^*]\backslash\{0\}$, sei I das von G erzeugte zweiseitige Ideal von $K[\Sigma^*]$, sei $G_I = \{ef_1, \ldots, ef_s\} \subseteq F_1$ und M_I der von G_I erzeugte zweiseitige Untermodul von F_1.*

a) Es gilt $\text{LT}_\sigma(\pi(m)) = \pi(\text{LT}_\tau(m))$ für alle $m \in F_1$.
b) Ist $\overline{G}$ eine τ-Gröbnerbasis von $M_I + N$, dann ist $\pi(\overline{G})\backslash\{0\}$ eine σ-Gröbnerbasis von I.

Beweis. Wir zeigen zunächst a). Sei dazu $m \in F_1$ und $\text{LT}_\tau(m) = w_1 e w'_1$ mit $w_1, w'_1 \in \Sigma^*$. Für einen von $\pi(\text{LT}_\tau(m)) = w_1 w'_1$ verschiedenen Term t in $\pi(m)$ existiert ein Term $w_2 e w'_2 \in \text{Supp}(m)$ mit $\pi(w_2 e w'_2) = t$. Es gilt nun $\text{LT}_\tau(m) >_\tau w_2 e w'_2$. Wegen $\tau = \texttt{Pos}\sigma$ ergibt sich $w_1 w'_1 >_\sigma w_2 w'_2$ und daher $\pi(\text{LT}_\tau(m)) = w_1 w'_1 >_\sigma w_2 w'_2 = \pi(w_2 e w'_2) = t$. Wir erhalten somit $\pi(\text{LT}_\tau(m)) = \text{LT}_\sigma(\pi(m))$.

Für den Beweis von b) sei $\overline{G}$ eine τ-Gröbnerbasis von $M_I + N$. Weiter sei $f \in I\backslash\{0\}$, d.h. $f = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} f_i w'_{ij}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Zu zeigen ist nun, dass Elemente $g \in \pi(\overline{G})\backslash\{0\}$ und $w, w' \in \Sigma^*$ existieren mit $\text{LT}_\sigma(f) = w\text{LT}_\tau(g)w'$. Es ist $\tilde{f} = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e f_i w'_{ij}$ ein Element in M_I mit $\pi(\tilde{f}) = f$. Nach Lemma 2.6.3 gilt auch $\overline{f} = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} e w_{ij} f_i w'_{ij} \in M_I + N = \pi^{-1}(I)$. Sei dabei $e\overline{w}$ mit $\overline{w} \in \Sigma^*$ der Leitterm von $\overline{f}$. Da $\overline{G}$ eine τ-Gröbnerbasis von $\pi^{-1}(I)$ ist, existieren also ein $\overline{g} \in \overline{G}$ und $w, w' \in \Sigma^*$ mit $\text{LT}_\tau(\overline{f}) = w\text{LT}_\tau(\overline{g})w'$. Dann muss aber $w = 1$ und $\text{LT}_\tau(\overline{g}) = ew''$ gelten für ein $w'' \in \Sigma^*$. Wir erhalten $e\overline{w} = ew''w'$ und mit a)

$$\begin{aligned}\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(\pi(\overline{f})) = \pi(\mathrm{LT}_\tau(\overline{f})) = \overline{w} = w''w' \\ = \pi(\mathrm{LT}_\tau(\overline{g}))w' = \mathrm{LT}_\sigma(\pi(\overline{g}))w'.\end{aligned}$$

Das Element $\pi(\overline{g}) \in \pi(\overline{G})\backslash\{0\}$ erfüllt also die geforderten Bedingungen. □

Bemerkung 2.6.6

a) Ist $\overline{G}$ eine reduzierte τ-Gröbnerbasis von $\pi^{-1}(I)$, so folgt daraus nicht, dass auch $\pi(\overline{G})\backslash\{0\}$ eine reduzierte σ-Gröbnerbasis von I ist. Wir betrachten als Beispiel dazu das zweiseitige Ideal $I = (x_1x_2, x_2x_1, x_1^3, x_2^3)$ von $\mathbb{Q}[\Sigma^*]$ mit $\Sigma = \{x_1, x_2\}$. Als reduzierte `PosLLex`-Gröbnerbasis von $\pi^{-1}(I) = \langle ex_1x_2, ex_2x_1, ex_1^3, ex_2^3, x_1e - ex_1, x_2e - ex_2\rangle$ erhalten wir $\overline{G} = \{ex_1x_2, ex_2x_1, ex_1^3, ex_2^3, x_1e-ex_1, x_2e-ex_2, ex_1^2x_2, ex_2^2x_1\}$ und damit $\pi(\overline{G})\backslash\{0\} = \{x_1x_2, x_2x_1, x_1^3, x_2^3, x_1^2x_2, x_2^2x_1\}$. Dies ist offensichtlich keine reduzierte σ-Gröbnerbasis von I.

b) Trotz der Existenz einer endlichen σ-Gröbnerbasis eines Ideals I führt der Buchberger-Algorithmus wie in Satz 2.5.3 beschrieben nicht immer zu einer endlichen Gröbnerbasis des zugehörigen Moduls $\pi^{-1}(I)$. So ist z.B. $\{x_1\}$ eine `LLex`-Gröbnerbasis des zweiseitigen Ideals $I = (x_1)$ von $\mathbb{Q}[\Sigma^*]$ mit $\Sigma = \{x_1, x_2\}$, aber die Berechnung der `PosLLex`-Gröbnerbasis des Moduls $\pi^{-1}(I) = \langle ex_1, x_1e-ex_1, x_2e-ex_2\rangle$ ergibt die neuen Elemente $\{ex_2x_1, ex_2^2x_1, \ldots\}$ und damit ein unendliches Erzeugendensystem.

Abschließend wollen wir nun anhand von Satz 2.6.5 explizit Gröbnerbasen für zweiseitige Ideale berechnen.

Beispiel 2.6.7 Wir betrachten den Polynomring $\mathbb{Q}[\Sigma^*]$ mit $\Sigma = \{x_1, x_2\}$ und der Termordnung $\sigma =$ `LLex`.

a) Sei I das zweiseitige Ideal von $\mathbb{Q}[\Sigma^*]$ erzeugt von $f_1 = x_1^2 - x_2$ und $f_2 = x_1x_2 - 1$. Als zugehörigen zweiseitigen Untermodul von F_1 erhalten wir $\pi^{-1}(I) = \langle g_1, g_2, g_3, g_4\rangle$ mit

$$\begin{aligned}g_1 &= ef_1 = ex_1^2 - ex_2,\\ g_2 &= ef_2 = ex_1x_2 - e,\\ g_3 &= ef_3 = x_1e - ex_1,\\ g_4 &= ef_4 = x_2e - ex_2.\end{aligned}$$

Wir berechnen nun mit dem Buchberger-Algorithmus eine τ-Gröbnerbasis von $\pi^{-1}(I)$, wobei $\tau =$ `PosLLex` gewählt ist. Wir starten dabei mit $\overline{\mathcal{G}} = (g_1, g_2, g_3, g_4)$ und $B = \{(1,3), (1,4), (2,3), (2,4)\}$ als Menge der kritischen Paare. Für das Paar $(1,3)$ ergibt sich der S-Vektor

$$\begin{aligned}S_{13} = x_1g_1 - g_2x_1^2 = ex_1^3 - x_1ex_2 \xrightarrow{g_1} -x_1ex_2 + ex_2x_1\\ \xrightarrow{g_3} -ex_1x_2 + ex_2x_1 \xrightarrow{g_2} ex_2x_1 - e =: g_5.\end{aligned}$$

Es ist dann $\overline{\mathcal{G}} = (g_1, g_2, g_3, g_4, g_5)$ und $B = \{(1,4),(2,3),(2,4),(3,5),(4,5)\}$. Als S-Vektor zum Paar $(1,4)$ erhalten wir

$$\begin{aligned} S_{14} &= x_2 g_1 - g_4 x_1^2 = e x_2 x_1^2 - x_2 e x_2 \xrightarrow{g_5} -x_2 e x_2 + e x_1 \\ &\xrightarrow{g_4} -e x_2^2 + e x_1 =: g_6 \end{aligned}$$

und damit $\overline{\mathcal{G}} = (g_1, g_2, g_3, g_4, g_5, g_6)$ bzw. die Menge der aktuellen kritischen Paare $B = \{(2,3),(2,4),(3,5),(4,5),(3,6),(4,6)\}$. Alle restlichen S-Vektoren lassen sich wie folgt zu Null reduzieren.

$$S_{23} = x_1 g_2 - g_3 x_1 x_2 = e x_1^2 x_2 - x_1 e \xrightarrow{g_1} e x_2^2 - x_1 e \xrightarrow{g_6} -x_1 e + e x_1 \xrightarrow{g_3} 0$$

$$S_{24} = x_2 g_2 - g_4 x_1 x_2 = e x_2 x_1 x_2 - x_2 e \xrightarrow{g_5} -x_2 e + e x_2 \xrightarrow{g_4} 0$$

$$S_{35} = g_3 x_2 x_1 - x_1 g_5 = -e x_1 x_2 x_1 + x_1 e \xrightarrow{g_2} x_1 e - e x_1 \xrightarrow{g_3} 0$$

$$S_{45} = g_4 x_2 x_1 - x_2 g_5 = -e x_2^2 x_1 + x_2 e \xrightarrow{g_6} -e x_1^2 + x_2 e \xrightarrow{g_1} x_2 e - e x_2 \xrightarrow{g_4} 0$$

$$\begin{aligned} S_{36} &= g_3 x_2^2 + x_1 g_6 = -e x_1 x_2^2 + x_1 e x_1 \xrightarrow{g_2} x_1 e x_1 - e x_2 \\ &\xrightarrow{g_3} e x_1^2 - e x_2 \xrightarrow{g_1} 0 \end{aligned}$$

$$\begin{aligned} S_{46} &= g_4 x_2^2 + x_2 g_6 = -e x_2^3 + x_2 e x_1 \xrightarrow{g_6} -e x_1 x_2 + x_2 e x_1 \xrightarrow{g_2} x_2 e x_1 - e \\ &\xrightarrow{g_4} e x_2 x_1 - e \xrightarrow{g_5} 0 \end{aligned}$$

Da nun $B = \emptyset$ gilt, erhalten wir als τ-Gröbnerbasis von $\pi^{-1}(I)$

$$\begin{aligned} \overline{G} &= \{g_1, g_2, g_3, g_4, g_5, g_6\} \\ &= \{e x_1^2 - e x_2, e x_1 x_2 - e, x_1 e - e x_1, x_2 e - e x_2, e x_2 x_1 - e, -e x_2^2 + e x_1\} \end{aligned}$$

und damit $\pi(\overline{G})\backslash\{0\} = \{x_1^2 - x_2, x_1 x_2 - 1, x_2 x_1 - 1, -x_2^2 + x_1\}$ als σ-Gröbnerbasis von I. Hierbei ist $\pi(\overline{G})\backslash\{0\}$ sogar die reduzierte σ-Gröbnerbasis von I.

b) Sei nun $I = (f_1, f_2, f_3)$ mit $f_1 = x_1^3 - 1$, $f_2 = x_2^2 - 1$ und $f_3 = x_1^2 x_2 - x_2 x_1$. Dieses zweiseitige Ideal wird im Kapitel 4 noch von Bedeutung sein, da die erzeugenden Polynome den Relationen in der Gruppendarstellung der symmetrischen Gruppe S_3 entsprechen. Wir betrachten nun wieder den zweiseitigen Untermodul $\pi^{-1}(I)$ von F_1 erzeugt von $g_1 = e x_1^3 - e$, $g_2 = e x_2^2 - e$, $g_3 = e x_1^2 x_2 - e x_2 x_1$, $g_4 = x_1 e - e x_1$ und $g_5 = x_2 e - e x_2$. Wir beginnen den Buchberger-Algorithmus mit $\overline{\mathcal{G}} = (g_1, g_2, g_3, g_4, g_5)$ und $B = \{(1,4),(2,4),(3,4),(1,5),(2,5),(3,5)\}$. Wir erhalten die folgenden S-Vektoren

$$S_{14} = x_1 g_1 - g_4 x_1^3 = e x_1^4 - x_1 e \xrightarrow{g_1} -x_1 e + e x_1 \xrightarrow{g_4} 0$$

$$S_{24} = x_1 g_2 - g_4 x_2^2 = e x_1 x_2^2 - x_1 e \xrightarrow{g_4} e x_1 x_2^2 - e x_1 =: g_6.$$

$$\begin{aligned} S_{34} &= x_1 g_3 - g_4 x_1^2 x_2 = e x_1^3 x_2 - x_1 e x_2 x_1 \xrightarrow{g_1} -x_1 e x_2 x_1 + e x_2 \\ &\xrightarrow{g_4} -e x_1 x_2 x_1 + e x_2 =: g_7 \end{aligned}$$

$$S_{15} = x_2 g_1 - g_5 x_1^3 = e x_2 x_1^3 - x_2 e \xrightarrow{g_5} e x_2 x_1^3 - e x_2 =: g_8$$

$$S_{25} = x_2g_2 - g_5x_2^2 = ex_2^3 - x_2e \xrightarrow{g_2} -x_2e + ex_2 \xrightarrow{g_5} 0$$
$$S_{35} = x_2g_3 - g_5x_1^2x_2 = ex_2x_1^2x_2 - x_2ex_2x_1 \xrightarrow{g_5} ex_2x_1^2x_2 - ex_2^2x_1$$
$$\xrightarrow{g_2} ex_2x_1^2x_2 - ex_1 =: g_9.$$

Damit ergibt sich jetzt $\overline{\mathcal{G}} = (g_1, \ldots, g_9)$ und $B = \{(4,6),(5,6),(4,7),(5,7),(4,8),(5,8),(4,9),(5,9)\}$. Die zugehörigen S-Vektoren lauten

$$S_{46} = g_4x_1x_2^2 - x_1g_6 = -ex_1^2x_2^2 + x_1ex_1 \xrightarrow{g_3} -ex_2x_1x_2 + x_1ex_1$$
$$\xrightarrow{g_4} -ex_2x_1x_2 + ex_1^2 =: g_{10}.$$
$$S_{56} = g_5x_1x_2^2 - x_2g_6 = -ex_2x_1x_2^2 + x_2ex_1 \xrightarrow{g_{10}} -ex_1^2x_2 + x_2ex_1$$
$$\xrightarrow{g_3} x_2ex_1 - ex_2x_1 \xrightarrow{g_5} 0$$
$$S_{47} = g_4x_1x_2x_1 - x_1g_7 = -ex_1^2x_2x_1 + x_1ex_2 \xrightarrow{g_3} -ex_2x_1^2 + x_1ex_2$$
$$\xrightarrow{g_4} -ex_2x_1^2 + ex_1x_2 =: g_{11}$$
$$S_{57} = g_5x_1x_2x_1 - x_2g_7 = -ex_2x_1x_2x_1 + x_2ex_2 \xrightarrow{g_{10}} -ex_1^3 + x_2ex_2$$
$$\xrightarrow{g_1} x_2ex_2 - e \xrightarrow{g_5} ex_2^2 - e \xrightarrow{g_2} 0$$
$$S_{48} = g_4x_2x_1^3 - x_1g_8 = -ex_1x_2x_1^3 + x_1ex_2 \xrightarrow{g_7} -ex_2x_1^2 + x_1ex_2$$
$$\xrightarrow{g_{11}} x_1ex_2 - ex_1x_2 \xrightarrow{g_4} 0$$
$$S_{58} = g_5x_2x_1^3 - x_2g_8 = -ex_2^2x_1^3 + x_2ex_2 \xrightarrow{g_2} -ex_1^3 + x_2ex_2$$
$$\xrightarrow{g_1} x_2ex_2 - e \xrightarrow{g_5} ex_2^2 - e \xrightarrow{g_2} 0$$
$$S_{49} = g_4x_2x_1^2x_2 - x_1g_9 = -ex_1x_2x_1^2x_2 + x_1ex_1 \xrightarrow{g_7} -ex_2x_1x_2 + x_1ex_1$$
$$\xrightarrow{g_{10}} x_1ex_1 - ex_1^2 \xrightarrow{g_4} 0$$
$$S_{59} = g_5x_2x_1^2x_2 - x_2g_9 = -ex_2^2x_1^2x_2 + x_2ex_1 \xrightarrow{g_2} -ex_1^2x_2 + x_2ex_1$$
$$\xrightarrow{g_3} x_2ex_1 - ex_2x_1 \xrightarrow{g_5} 0$$

und wir haben nun $\overline{\mathcal{G}} = (g_1, \ldots, g_{11})$ bzw. $B = \{(4,10),(5,10),(4,11),(5,11),(8,11),(9,11)\}$. Die entsprechenden S-Vektoren reduzieren alle zu Null:

$$S_{4,10} = g_4x_2x_1x_2 - x_1g_{10} = -ex_1x_2x_1x_2 + x_1ex_1^2 \xrightarrow{g_7} x_1ex_1^2 - ex_2^2$$
$$\xrightarrow{g_2} x_1ex_1^2 - e \xrightarrow{g_4} ex_1^3 - e \xrightarrow{g_1} 0$$
$$S_{5,10} = g_5x_2x_1x_2 - x_2g_{10} = -ex_2^2x_1x_2 + x_2ex_1^2 \xrightarrow{g_2} x_2ex_1^2 - ex_1x_2$$
$$\xrightarrow{g_5} ex_2x_1^2 - ex_1x_2 \xrightarrow{g_{11}} 0$$
$$S_{4,11} = g_4x_2x_1^2 - x_1g_{11} = -ex_1x_2x_1^2 + x_1ex_1x_2 \xrightarrow{g_7} x_1ex_1x_2 - ex_2x_1$$
$$\xrightarrow{g_4} ex_1^2x_2 - ex_2x_1 \xrightarrow{g_3} 0$$
$$S_{5,11} = g_5x_2x_1^2 - x_2g_{11} = -ex_2^2x_1^2 + x_2ex_1x_2 \xrightarrow{g_2} x_2ex_1x_2 - ex_1^2$$
$$\xrightarrow{g_5} ex_2x_1x_2 - ex_1^2 \xrightarrow{g_{10}} 0$$
$$S_{8,11} = g_8 - g_{11}x_1 = ex_1x_2x_1 - ex_2 \xrightarrow{g_7} 0$$
$$S_{9,11} = g_9 - g_{11}x_2 = ex_1x_2^2 - ex_1 \xrightarrow{g_6} 0.$$

Insgesamt erhalten wir also mit $\overline{G} = \{g_1, \ldots, g_{11}\}$ eine τ-Gröbnerbasis von $\pi^{-1}(I)$ und mit

$$\pi(\overline{G})\backslash\{0\} = \{x_1^3 - 1, x_2^2 - 1, x_1^2x_2 - x_2x_1, x_1x_2^2 - x_1, -x_1x_2x_1 + x_2,$$
$$x_2x_1^3 - x_2, x_2x_1^2x_2 - x_1, -x_2x_1x_2 + x_1^2, -x_2x_1^2 + x_1x_2\}$$

eine σ-Gröbnerbasis von I. Die reduzierte σ-Gröbnerbasis von I ist demnach

$$\{x_1^3 - 1, x_2^2 - 1, x_1^2x_2 - x_2x_1, x_1x_2x_1 - x_2, x_2x_1x_2 - x_1^2, x_2x_1^2 - x_1x_2\}.$$

Kapitel 3

Syzygienberechnung

Nachdem wir nun die Theorie der τ-Gröbnerbasen für zweiseitige Untermoduln M zweiseitiger freier $K[\Sigma^*]$-Moduln kennen gelernt haben, wollen wir uns in diesem Kapitel mit dem eigentlichen Thema dieser Arbeit beschäftigen, der Berechnung von *Syzygien*. Die Aufgabe besteht darin, zu einem gegebenen Tupel $(g_1, \ldots, g_s) \in F^s$ Tupel nicht-kommutativer Polynome $q_{ij}, q'_{ij} \in K[\Sigma^*]$ zu finden, so dass die Gleichung $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} q_{ij} g_i q'_{ij} = 0$ erfüllt ist. Hierzu betrachten wir zunächst in Abschnitt 1 den Fall, dass es sich bei $g_1, \ldots, g_s$ um Monome handelt. Die dabei gewonnenen Erkenntnisse versuchen wir im 2. Abschnitt auf beliebige Elemente zu erweitern. Es stellt sich aber heraus, dass dies nicht für alle Tupel möglich ist. Eine zentrale Rolle spielt dabei der Zusammenhang mit den in Kapitel 2 eingeführten τ-Gröbnerbasen. Um auch Syzygien von den übrigen Tupeln berechnen zu können, gehen wir dann auf die Eliminationstheorie ein. Insbesondere stellt die sogenannte Komponenten-Elimination, mit der wir uns im vorletzten Abschnitt befassen, die Lösung dieses Problems dar. Zum Abschluss dieses Kapitels präsentieren wir Prozeduren zur Berechnung aller Syzygien von Tupeln aus Elementen des Moduls F bzw. des Polynomrings $K[\Sigma^*]$.

In diesem Kapitel sei F stets der freie von $\{e_1, \ldots, e_r\}$ zweiseitig erzeugte Modul über $K[\Sigma^*]$ und τ eine Modultermordnung auf $\mathbb{T}(F)$. Weiter sei σ immer eine Termordnung auf Σ^*.

3.1 Syzygien in monomialen Moduln

Das Thema dieses Abschnitts ist die Berechnung der Syzygien von einem Tupel $(m_1, \ldots, m_s)$, das aus Monomen $m_1, \ldots, m_s \in F$ besteht. Wir werden dazu zuerst den Begriff der Syzygie allgemein einführen. Es stellt sich dabei heraus, dass die Syzygien einen zweiseitigen Modul bilden, der sogar endlich

erzeugt ist. Im Folgenden sei E stets der freie von $\{\varepsilon_1, \ldots, \varepsilon_s\}$ zweiseitig erzeugte $K[\Sigma^*]$-Modul.

Definition 3.1.1 Sei $\mathcal{G} = (g_1, \ldots, g_s)$ ein Tupel von Elementen aus F.

1) Eine **(zweiseitige) Syzygie** von $\mathcal{G}$ ist ein Element $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} q_{ij} \varepsilon_i q'_{ij}$ des zweiseitigen freien Moduls E, so dass die folgende Gleichung erfüllt ist:
$$\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} q_{ij} g_i q'_{ij} = 0.$$

2) Die Menge aller Syzygien von $\mathcal{G}$ bilden einen zweiseitigen $K[\Sigma^*]$-Untermodul von E, den sogenannten **(zweiseitigen) Syzygienmodul** $\mathrm{Syz}(\mathcal{G})$ von $\mathcal{G}$.

Das Element Null in E ist stets eine Syzygie von $\mathcal{G}$. Dass der Syzygienmodul $\mathrm{Syz}(\mathcal{G})$ tatsächlich einen zweiseitigen Untermodul von E bildet, lässt sich leicht nachvollziehen. Denn für zwei Syzygien $s_1 = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} q_{ij} \varepsilon_i q'_{ij}$ und $s_2 = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} \tilde{q}_{ij} \varepsilon_i \tilde{q}'_{ij}$ sowie Polynome $f, f' \in K[\Sigma^*]$ sind die Gleichungen
$$\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} q_{ij} g_i q'_{ij} + \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} \tilde{q}_{ij} g_i \tilde{q}'_{ij} = 0$$
und
$$\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} f q_{ij} g_i q'_{ij} f' = 0$$
erfüllt und $s_1 + s_2$ bzw. $f s_1 f'$ somit wieder Elemente von $\mathrm{Syz}(\mathcal{G})$.

Sei nun M der von $\{g_1, \ldots, g_s\}$ erzeugte zweiseitige Untermodul von F. Wir betrachten die Abbildung $\lambda : E \longrightarrow M, \varepsilon_i \mapsto g_i$. Nach der universellen Eigenschaft des freien zweiseitigen Moduls E aus Satz 2.2.2 ist λ ein Homomorphismus und wir erhalten $\mathrm{Kern}(\lambda) = \mathrm{Syz}(\mathcal{G})$. Es ergibt sich die folgende exakte Sequenz
$$0 \longrightarrow \mathrm{Syz}(\mathcal{G}) \longrightarrow E \longrightarrow F \longrightarrow F/M \longrightarrow 0.$$
Diese Überlegungen können wir nun vollkommen analog mit dem Tupel $\mathrm{LM}_\tau(\mathcal{G}) = (\mathrm{LM}_\tau(g_1), \ldots, \mathrm{LM}_\tau(g_s)) \in F^s$ durchführen. Sei dabei M' der von $\{\mathrm{LM}_\tau(g_1), \ldots, \mathrm{LM}_\tau(g_s)\}$ erzeugte zweiseitige Untermodul von F. Durch den Homomorphismus $\Lambda : E \longrightarrow M', \varepsilon_i \mapsto \mathrm{LM}_\tau(g_i)$ erhalten wir hier die exakte Sequenz
$$0 \longrightarrow \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G})) \longrightarrow E \longrightarrow F \longrightarrow F/M' \longrightarrow 0.$$

Es stellt sich nun heraus, dass die Berechnung des Syzygienmoduls von $\mathrm{LM}_\tau(\mathcal{G})$ ein deutlich einfacheres Problem darstellt als die von $\mathrm{Syz}(\mathcal{G})$. Der nun folgende Satz gibt uns die Möglichkeit, ein einfaches und vor allem endliches Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ anzugeben.

Satz 3.1.2 *Sei $\mathcal{G} = (m_1, \ldots, m_s) \in F^s$ ein Tupel aus Monomen von F und $G = \{m_1, \ldots, m_s\}$.*

a) Seien $i, j \in \{1, \ldots, s\}$ mit $i < j$, so dass (i, j) ein kritisches Paar von G ist. D.h. es existieren $w_i, w_i', w_j, w_j' \in \Sigma^*$ mit $w_i \mathrm{LT}_\tau(m_i) w_i' = w_j \mathrm{LT}_\tau(m_j) w_j'$, wobei w_i und w_j kein gemeinsames Präfix bzw. w_i' und w_j' kein gemeinsames Suffix haben. Dann ist

$$\sigma_{ij} = \tfrac{1}{\mathrm{LC}_\tau(m_i)} w_i \varepsilon_i w_i' - \tfrac{1}{\mathrm{LC}_\tau(m_j)} w_j \varepsilon_j w_j'$$

eine Syzygie von $\mathcal{G}$. Das Element $\sigma_{ij} \in E$ wird auch Fundamentalsyzygie von $\mathcal{G}$ genannt.

b) Es gilt

$$\mathrm{Syz}(\mathcal{G}) = \langle \sigma_{ij} \mid 1 \leq i < j \leq s, (i, j) \text{ ist kritisches Paar von } G \rangle,$$

d.h. $\mathrm{Syz}(\mathcal{G})$ *ist ein endlich-erzeugter zweiseitiger Untermodul von E.*

Beweis. Offensichtlich gilt a), denn $\lambda(\sigma_{ij}) = 0$.

Für den Beweis von b) bleibt wegen a) nur die Inklusion "$\subseteq$" zu zeigen. Sei dazu $m_i = c_i t_i$ mit $c_i \in K \backslash \{0\}$ und $t_i \in \mathbb{T}(F)$ für $i = 1, \ldots, s$. Weiter sei $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} w_{ij} \varepsilon_i w_{ij}' \in \mathrm{Syz}(\mathcal{G}) \backslash \{0\}$ mit $a_{ij} \in K$, $w_{ij}, w_{ij}' \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der a_{ij} von Null verschieden sind. Es bezeichne $A(m)$ die Kardinalität der Menge $\{i \in \{1, \ldots, s\} \mid a_{ij} \neq 0$ für mindestens ein $j \in \mathbb{N}\}$. Wegen $\lambda(m) = 0$ ist $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} c_i = 0$ und mit $m \neq 0$ folgt $A(m) \geq 2$. D.h. es existieren Indizes i_1, i_2, j_1, j_2 mit $i_1 < i_2$, $a_{i_1 j_1} \neq 0$, $a_{i_2 j_2} \neq 0$ und $t = w_{i_1 j_1} t_{i_1} w_{i_1 j_1}' = w_{i_2 j_2} t_{i_2} w_{i_2 j_2}'$. Demnach ist (i_1, i_2) ein kritisches Paar von G und t ein Vielfaches von $w_{i_1} t_{i_1} w_{i_1}'$. Es gibt also Elemente $\widetilde{w}, \widetilde{w}' \in \Sigma^*$ mit $t = \widetilde{w} w_{i_1} t_{i_1} w_{i_1}' \widetilde{w}'$. Wir erhalten damit eine neue Syzygie $m' = m - a_{i_1 j_1} c_{i_1} \widetilde{w} \sigma_{i_1 j_1} \widetilde{w}' \in \mathrm{Syz}(\mathcal{G})$ mit $A(m') \leq A(m)$. Eine Wiederholung dieses Verfahrens für alle übrigen kritischen Paare (i_1, j) mit $j \in \mathbb{N}$ ergibt ein Element $m'' \in \mathrm{Syz}(\mathcal{G})$ und $A(m'') < A(m)$. Die Behauptung folgt nun induktiv. □

Der obige Satz ermöglicht uns, Syzygien für ein beliebiges Tupel von Monomen aus F, die demnach einen monomialen zweiseitigen Untermodul von F erzeugen, zu berechnen.

Beispiel 3.1.3 Sei $\Sigma = \{x_1, x_2, x_3\}$, sei $F = \langle e_1, e_2 \rangle$ und $\tau =$ `PosLLex`. Weiter sei $G = \{m_1, m_2, m_3, m_4\} \subseteq F$ und $\mathcal{G} = (m_1, m_2, m_3, m_4)$ mit Monomen $m_1 = x_2 e_1 x_1^2$, $m_2 = x_1 x_2 e_1 x_1$, $m_3 = x_2^2 e_1 x_1$, $m_4 = e_2 x_1$. Die Menge der kritischen Paare von G ist hierbei $B = \{(1, 2), (1, 3)\}$. Für das Paar $(1, 2)$ erhalten wir $x_1 \mathrm{LT}_\tau(m_1) = \mathrm{LT}_\tau(m_2) x_1$ und somit die Syzygie $\sigma_{12} = x_1 \varepsilon_1 - \varepsilon_2 x_1$. Für $(1, 3)$ ist $x_2 \mathrm{LT}_\tau(m_1) = \mathrm{LT}_\tau(m_3) x_1$ und $\sigma_{13} = x_2 \varepsilon_1 - \varepsilon_3 x_1$.

3.2 Liften von Syzygien

Wir haben im vorangehenden Abschnitt gesehen, wie Syzygien von einem Tupel von Monomen berechnet werden können. Es stellt sich nun die Frage, ob wir diese Information verwenden können, um Syzygien von Tupeln beliebiger Elemente $g_1, \ldots, g_s$ zu ermitteln. Die Antwort lautet ja, wenn $\{g_1, \ldots, g_s\}$ eine τ-Gröbnerbasis ist. In diesem Fall lassen sich die Fundamentalsyzygien σ_{ij} von $\mathrm{LM}_\tau(\mathcal{G})$ zu Syzygien von $\mathcal{G}$ „liften“. Ist dies nicht der Fall, so müsste zunächst eine τ-Gröbnerbasis von $\langle G \rangle$ bestimmt und eine Darstellung der Elemente $g_1, \ldots, g_s$ in der neuen Basis gefunden werden. Da diese Gröbnerbasis möglicherweise unendlich ist und das in diesem Abschnitt beschriebene Verfahren nur für Tupel endlich vieler Elemente funktioniert, werden wir für diesen Fall im dritten Abschnitt einen anderen Weg diskutieren. Es sei an dieser Stelle darauf hingewiesen, dass der letzte Fall der für uns wichtige ist und die Prozedur in diesem Abschnitt aus Gründen der Vollständigkeit angesprochen wird.

Doch zunächst wollen wir einige Grundbegriffe einführen. Wie im letzten Abschnitt sei wieder E der freie von $\{\varepsilon_1, \ldots, \varepsilon_s\}$ zweiseitig erzeugte $K[\Sigma^*]$-Modul.

Definition 3.2.1 Sei $\mathcal{G} = (g_1, \ldots, g_s) \in (F \backslash \{0\})^s$ und $m \neq 0$ ein Element von E, d.h. $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} w_{ij} \varepsilon_i w'_{ij}$ mit $a_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele a_{ij} von Null verschieden sind.

1) Der Term
$$\deg_{\tau,\mathcal{G}}(m) = \max_\tau \{ w_{ij} \mathrm{LT}_\tau(g_i) w'_{ij} \mid w_{ij} \varepsilon_i w'_{ij} \in \mathrm{Supp}(m) \}$$
heißt der **Grad** von m.
2) Sei t ein Term aus $\mathbb{T}(F)$. Das Element m heißt **homogen** vom Grad t, falls $\deg_{\tau,\mathcal{G}}(w_{ij} \varepsilon_i w'_{ij}) = t$ für alle $w_{ij} \varepsilon_i w'_{ij} \in \mathrm{Supp}(m)$.
3) Sei $m = \sum_{t \in \mathbb{T}(F)} m_t$ die Zerlegung von m in seine homogenen Komponenten, d.h. m_t ist homogen vom Grad t. Dann heißt die homogene Komponente vom Grad $\deg_{\tau,\mathcal{G}}(m)$ die **Leitform** $\mathrm{LF}_{\tau,\mathcal{G}}(m)$ von m.

Es ergeben sich nun die folgenden Eigenschaften für die eben definierten Begriffe.

Lemma 3.2.2 *Sei $G = \{g_1, \ldots, g_s\} \subseteq F \backslash \{0\}$ und $\mathcal{G} = (g_1, \ldots, g_s)$. Weiter sei $m \in E \backslash \mathrm{Syz}(\mathcal{G})$ und $m' \in \mathrm{Syz}(\mathcal{G}) \backslash \{0\}$.*

a) Sei σ_{ij} eine Fundamentalsyzygie von $\mathcal{G}$. Dann ist σ_{ij} homogen vom Grad $\deg_{\tau,\mathcal{G}}(\sigma_{ij}) = w_i \mathrm{LT}_\tau(g_i) w'_i$.
b) $\mathrm{LT}_\tau(\lambda(m)) \leq_\tau \deg_{\tau,\mathcal{G}}(m)$.

c) $\mathrm{LF}_{\tau,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ *genau dann, wenn* $\mathrm{LT}_\tau(\lambda(m)) <_\tau \deg_{\tau,\mathcal{G}}(m)$.
d) $\mathrm{LF}_{\tau,\mathcal{G}}(m') \in \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$.

Beweis. Für den Beweis von a) sei $\sigma_{ij} = \frac{1}{\mathrm{LC}_\tau(g_i)} w_i \varepsilon_i w_i' - \frac{1}{\mathrm{LC}_\tau(g_j)} w_j \varepsilon_j w_j'$ eine Fundamentalsyzygie von $\mathcal{G}$. Dann gilt

$$\deg_{\tau,\mathcal{G}}(w_i \varepsilon_i w_i') = w_i \mathrm{LT}_\tau(g_i) w_i' = w_j \mathrm{LT}_\tau(g_j) w_j' = \deg_{\tau,\mathcal{G}}(w_j \varepsilon_j w_j').$$

Also ist σ_{ij} homogen vom Grad $\deg_{\tau,\mathcal{G}}(\sigma_{ij}) = w_i \mathrm{LT}_\tau(g_i) w_i'$.

Um b) zu zeigen, sei $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w_{ij}'$ mit $c_{ij} \in K, w_{ij}, w_{ij}' \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Für den Leitterm von $\lambda(m)$ ergibt sich

$$\begin{aligned}
\mathrm{LT}_\tau(\lambda(m)) &= \mathrm{LT}_\tau(\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w_{ij}') \\
&\leq_\tau \max_\tau\{\mathrm{LT}_\tau(w_{ij} g_i w_{ij}') \mid i \in \{1, \ldots, s\}, j \in \mathbb{N}, c_{ij} \neq 0\} \\
&= \max_\tau\{w_{ij} \mathrm{LT}_\tau(g_i) w_{ij}' \mid i \in \{1, \ldots, s\}, j \in \mathbb{N}, c_{ij} \neq 0\} \\
&= \deg_{\tau,\mathcal{G}}(m).
\end{aligned}$$

Ferner ist die Aussage $\Lambda(\mathrm{LF}_{\tau,\mathcal{G}}(m)) = 0$ äquivalent dazu, dass der Term $\deg_{\tau,\mathcal{G}}(m)$ in $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w_{ij}'$ verschwindet. Dies ist wiederum äquivalent zu $\mathrm{LT}_\tau(\lambda(m)) <_\tau \deg_{\tau,\mathcal{G}}(m)$. Also ist auch c) gezeigt.

Es bleibt noch d) zu beweisen. Sei dazu $m' = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} w_{ij} \varepsilon_i w_{ij}' \in \mathrm{Syz}(\mathcal{G}) \backslash \{0\}$. Nun ist $0 = \lambda(m') = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} a_{ij} w_{ij} g_i w_{ij}'$ und insbesondere der Koeffizient von $\deg_{\tau,\mathcal{G}}(m')$ in $\lambda(m')$ gleich Null. Wir erhalten also

$$\mathrm{LT}_\tau(\lambda(\mathrm{LF}_{\tau,\mathcal{G}}(m'))) <_\tau \deg_{\tau,\mathcal{G}}(m')$$

und damit $\Lambda(\mathrm{LF}_{\tau,\mathcal{G}}(m')) = 0$. □

Wir kommen jetzt zu dem bereits angesprochenen „Liften“ von Elementen aus E.

Definition 3.2.3 Sei $\overline{m} \in E \backslash \{0\}$. Ein Element $m \in E \backslash \{0\}$ heißt eine **Liftung** von $\overline{m}$, falls $\mathrm{LF}_{\tau,\mathcal{G}}(m) = \overline{m}$.

Da für $m \in E \backslash \{0\}$ die Leitform $\mathrm{LF}_{\tau,\mathcal{G}}(m)$ nach Definition homogen ist, existieren Liftungen nur für homogene Elemente $\overline{m} \in E \backslash \{0\}$. Unter dieser Voraussetzung ist $\overline{m}$ offensichtlich stets eine Liftung von sich selbst.

Satz 3.2.4 *Sei* $\mathcal{G} = (g_1, \ldots, g_s) \in (F \backslash \{0\})^s$ *und* $\{\overline{m}_1, \ldots, \overline{m}_u\} \subseteq E$ *ein homogenes Erzeugendensystem von* $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$. *Seien* $m_1, \ldots, m_u \in \mathrm{Syz}(\mathcal{G})$ *mit* $\mathrm{LF}_{\tau,\mathcal{G}}(m_i) = \overline{m}_i$ *für* $i = 1, \ldots, u$. *Dann gilt:*

a) $\{m_1, \ldots, m_u\}$ *ist ein Erzeugendensystem von* $\mathrm{Syz}(\mathcal{G})$.
b) Jedes homogene Element in $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ *hat eine Liftung in* $\mathrm{Syz}(\mathcal{G})$.

Beweis. Für den Beweis von a) nehmen wir an, dass $\{m_1, \ldots, m_u\}$ kein Erzeugendensystem von $\mathrm{Syz}(\mathcal{G})$ ist. Dann gibt es in $\mathrm{Syz}(\mathcal{G})\backslash\langle m_1, \ldots, m_u\rangle$ ein Element m mit minimalem Grad $\deg_{\tau,\mathcal{G}}(m)$. Da $\mathrm{LF}_{\tau,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ nach Lemma 3.2.2 d), erhalten wir $\mathrm{LF}_{\tau,\mathcal{G}}(m) = \sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\overline{m}_i w'_{ij}$ mit $c_{ij} \in K, w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, u$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Für das Element $m' = m - \sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}m_i w'_{ij}$ gilt nun $m' = 0$ oder $\deg_{\tau,\mathcal{G}}(m') <_\tau \deg_{\tau,\mathcal{G}}(m)$, da sich gerade die Terme vom Grad $\deg_{\tau,\mathcal{G}}(m)$ wegheben. Im Fall $m' = 0$ wäre nun aber m in $\langle m_1, \ldots, m_u\rangle$ enthalten im Widerspruch zur Voraussetzung. Im Fall $m' \neq 0$ erhielten wir mit $m' \in \mathrm{Syz}(\mathcal{G})\backslash\langle m_1, \ldots, m_u\rangle$ ein Element mit kleinerem Grad als dem von m im Widerspruch zur Wahl von m.

Es bleibt noch b) zu beweisen. Sei dazu mit $\overline{m} \in \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))\backslash\{0\}$ ein homogenes Element gegeben. Da $\{\overline{m}_1, \ldots, \overline{m}_u\}$ ein Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ ist, können wir $\overline{m}$ schreiben als $\overline{m} = \sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\overline{m}_i w'_{ij}$ mit $c_{ij} \in K, w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, u$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Da $\overline{m}$ homogen ist, gilt $\deg_{\tau,\mathcal{G}}(w_{ij}\overline{m}_i w'_{ij}) = \deg_{\tau,\mathcal{G}}(\overline{m})$ für alle i und j mit $c_{ij} \neq 0$. Wegen $\mathrm{LF}_{\tau,\mathcal{G}}(w_{ij}m_i w'_{ij}) = w_{ij}\overline{m}_i w'_{ij}$ ergibt sich nun $\deg_{\tau,\mathcal{G}}(w_{ij}m_i w'_{ij}) = \deg_{\tau,\mathcal{G}}(\overline{m})$. Wir erhalten also

$$\begin{aligned}\mathrm{LF}_{\tau,\mathcal{G}}(\sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}m_i w'_{ij}) &= \sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}\mathrm{LF}_{\tau,\mathcal{G}}(w_{ij}m_i w'_{ij}) \\ &= \sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\overline{m}_i w'_{ij} = \overline{m}\end{aligned}$$

und demnach mit $\sum_{i=1}^{u}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}m_i w'_{ij}$ eine Liftung von $\overline{m}$. □

Zum Abschluss dieses Abschnitts diskutieren wir den Zusammenhang zwischen τ-Gröbnerbasen und der Existenz von Liftungen der Elemente eines homogenen Erzeugendensystems von $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$.

Satz 3.2.5 *Sei $G = \{g_1, \ldots, g_s\} \subseteq F\backslash\{0\}$, sei $\mathcal{G} = (g_1, \ldots, g_s)$ und M der von G erzeugte zweiseitige Untermodul von F. Dann sind folgende Aussagen äquivalent:*

a) G ist eine τ-Gröbnerbasis von M.
b) Für $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ existiert ein endliches homogenes Erzeugendensystem aus Elementen mit Liftungen in $\mathrm{Syz}(\mathcal{G})$.

Beweis. Seien zunächst $\{\overline{m}_1, \ldots, \overline{m}_u\}$ ein homogenes Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ und $m_1, \ldots, m_u \in \mathrm{Syz}(\mathcal{G})$ mit $\mathrm{LF}_{\tau,\mathcal{G}}(m_i) = \overline{m}_i$ für $i = 1, \ldots, u$. Nach Satz 2.2.11 genügt es nun zu zeigen, dass jedes Element $v \in M\backslash\{0\}$ eine Darstellung $v = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_i w'_{ij}$ besitzt mit $\mathrm{LT}_\tau(v) \geq_\tau \mathrm{LT}_\tau(w_{ij}g_i w'_{ij})$

für alle $i \in \{1, \ldots, s\}$ und $j \in \mathbb{N}$ mit $c_{ij} \neq 0$. Wir nehmen also einmal an, dass ein $v \in M \backslash \{0\}$ existiert, welches nicht derart geschrieben werden kann. Für $m' = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij} \in E$ gilt nun $\lambda(m') = v$. Wir wählen jetzt $m \in E$ so, dass $\lambda(m) = v$ und der Grad von m minimal ist. Dabei ist $\deg_{\tau,\mathcal{G}}(m) \neq \mathrm{LT}_\tau(v)$, da ansonsten v von obiger Form wäre. Mit Lemma 3.2.2 b) folgt daher $\deg_{\tau,\mathcal{G}}(m) >_\tau \mathrm{LT}_\tau(v)$. Also ergibt sich $\mathrm{LF}_{\tau,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ nach Lemma 3.2.2 c). Wir erhalten nun mit Satz 3.2.4 b) ein Element $m'' \in \mathrm{Syz}(\mathcal{G})$ mit $\mathrm{LF}_{\tau,\mathcal{G}}(m'') = \mathrm{LF}_{\tau,\mathcal{G}}(m)$. Es gilt dann $\deg_{\tau,\mathcal{G}}(m - m'') <_\tau \deg_{\tau,\mathcal{G}}(m)$ und $\lambda(m - m'') = v$ wegen $m'' \in \mathrm{Syz}(\mathcal{G})$ im Widerspruch zur Minimalität des Grades von m.

Umgekehrt sei nun G eine τ-Gröbnerbasis von M. Nach Satz 3.1.2 ist $\{\sigma_{ij} \mid 1 \leq i < j \leq s, (i,j) \text{ ist kritisches Paar von } G\}$ ein endliches homogenes Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$. Wir werden nun zu jedem kritischen Paar (i,j) von G ein Element $s_{ij} \in \mathrm{Syz}(\mathcal{G})$ konstruieren mit $\mathrm{LF}_{\tau,\mathcal{G}}(s_{ij}) = \sigma_{ij}$. Wir betrachten dazu den zugehörigen S-Vektor

$$S_{ij} = \tfrac{1}{\mathrm{LC}_\tau(g_i)} w_i g_i w'_i - \tfrac{1}{\mathrm{LC}_\tau(g_j)} w_j g_j w'_j \in M.$$

Da G eine τ-Gröbnerbasis von M ist, finden wir eine Darstellung

$$S_{ij} = \sum_{k=1}^{s} \sum_{l \in \mathbb{N}} c_{kl} w_{kl} g_k w'_{kl}$$

mit $c_{kl} \in K$, $w_{kl}, w'_{kl} \in \Sigma^*$ für $k = 1, \ldots, s$ und $l \in \mathbb{N}$, wobei nur endlich viele der c_{kl} von Null verschieden sind und $\mathrm{LT}_\tau(S_{ij}) \geq_\tau \mathrm{LT}_\tau(w_{kl} g_k w'_{kl})$ für $c_{kl} \neq 0$. Für das Element

$$s_{ij} = \sigma_{ij} - \sum_{k=1}^{s} \sum_{l \in \mathbb{N}} c_{kl} w_{kl} \varepsilon_k w'_{kl}$$

gilt nun $\mathrm{LF}_{\tau,\mathcal{G}}(s_{ij}) = \sigma_{ij}$ wegen $\deg_{\tau,\mathcal{G}}(\sigma_{ij}) = \mathrm{LT}_\tau(w_i g_i w'_i) >_\tau \mathrm{LT}_\tau(S_{ij})$. Also ist s_{ij} eine Liftung von σ_{ij}. Des Weiteren gilt

$$\lambda(s_{ij}) = S_{ij} - \sum_{k=1}^{s} \sum_{l \in \mathbb{N}} c_{kl} w_{kl} g_k w'_{kl} = 0$$

und damit $s_{ij} \in \mathrm{Syz}(\mathcal{G})$, womit die Behauptung bewiesen ist. □

Der zweite Teil des Beweises zeigt, wie wir Liftungen der Fundamentalsyzygien σ_{ij} in $\mathrm{Syz}(\mathcal{G})$ bestimmen können. Wir erhalten auf diese Weise nach Satz 3.2.4 a) ein endliches Erzeugendensystem des Syzygienmoduls $\mathrm{Syz}(\mathcal{G})$.

Wir betrachten das folgende Beispiel.

Beispiel 3.2.6 Sei $\Sigma = \{x_1, x_2, x_3\}$ und $\tau = \texttt{PosLLex}$ die gewählte Modultermordnung auf $\mathbb{T}(F)$ mit $F = \langle e_1, e_2 \rangle$. Weiter sei $\mathcal{G} = (g_1, g_2, g_3, g_4)$ mit

$g_1 = x_2e_1x_1^2 + x_3e_2x_1, g_2 = x_1x_2e_1x_1 + x_1x_3e_2, g_3 = x_2^2e_1x_1 + e_2, g_4 = e_2x_1$. In Beispiel 3.1.3 haben wir das homogene Erzeugendensystem $\{\sigma_{12}, \sigma_{13}\}$ von $\mathrm{Syz}(\mathrm{LM}_\tau(\mathcal{G}))$ bestimmt, wobei $\sigma_{12} = x_1\varepsilon_1 - \varepsilon_2x_1$ und $\sigma_{13} = x_2\varepsilon_1 - \varepsilon_3x_1$. Nun ist $G = \{g_1, g_2, g_3, g_4\}$ eine τ-Gröbnerbasis von $\langle G\rangle$, denn durch Nachrechnen ergibt sich

$$\begin{aligned} S_{12} &= x_1g_1 - g_2x_1 = 0, \\ S_{13} &= x_2g_1 - g_3x_1 = x_2x_3e_2x_1 - e_2x_1 \xrightarrow{g_4} 0. \end{aligned}$$

Da $S_{12} = 0$ gilt, ist $\sigma_{12} \in \mathrm{Syz}(\mathcal{G})$ und somit $s_{12} = \sigma_{12}$. Für die Berechnung von s_{13} bestimmen wir eine Darstellung des S-Vektors S_{13} in den Elementen von G wie im Beweis von Satz 3.2.5. Wir erhalten $S_{13} = (x_2x_3 - 1)g_4$ und damit $s_{13} = \sigma_{13} - (x_2x_3 - 1)\varepsilon_4 = x_2\varepsilon_1 - \varepsilon_3x_1 - (x_2x_3 - 1)\varepsilon_4$. Also ist

$$\mathrm{Syz}(\mathcal{G}) = \langle s_{12}, s_{13}\rangle = \langle x_1\varepsilon_1 - \varepsilon_2x_1, x_2\varepsilon_1 - \varepsilon_3x_1 - (x_2x_3 - 1)\varepsilon_4\rangle.$$

3.3 Elimination

Die Eliminationstheorie spielt eine wichtige Rolle in der Computeralgebra. Sie beschäftigt sich z.B. mit der Frage, wie zu einem zweiseitigen $K[\Sigma^*]$-Modul M mit $\Sigma = \{x_1, \ldots, x_n\}$ all diejenigen Elemente aus M ermittelt werden können, die nur die Unbestimmten $x_1, \ldots, x_j$ für ein $j \in \{1, \ldots, n\}$ beinhalten. Da diese Elemente einen zweiseitigen Untermodul von M bilden, ist es hierbei auch von Interesse, eine entsprechende Gröbnerbasis anzugeben.

In diesem Abschnitt sei $L \subseteq \{x_1, \ldots, x_n\}$ eine Teilmenge des Systems der Unbestimmten und $\widehat{\Sigma} = \Sigma\backslash L$. Dann bezeichnen wir mit $K[\widehat{\Sigma}^*]$ den nicht-kommutativen Polynomring in den verbleibenden Unbestimmten. Weiter sei $\widehat{F}$ der freie zweiseitige Modul über $K[\widehat{\Sigma}^*]$ erzeugt von $\{e_1, \ldots, e_r\}$, d.h.

$$\widehat{F} = \bigoplus_{i\in\{1,\ldots,r\}} K[\widehat{\Sigma}^*]e_iK[\widehat{\Sigma}^*].$$

Definition 3.3.1 Sei $L \subseteq \{x_1, \ldots, x_n\}$.

1) Eine Modultermordnung τ auf $\mathbb{T}(F)$ heißt **Eliminationsordnung** für L, falls jedes Element $m \in F\backslash\{0\}$ mit $\mathrm{LT}_\tau(m) \in \widehat{F}$ in $\widehat{F}$ enthalten ist.
2) Ist M ein zweiseitiger Untermodul von F, so heißt der zweiseitige $K[\widehat{\Sigma}^*]$-Untermodul $M \cap \widehat{F}$ von $\widehat{F}$ der **Eliminationsmodul** von M bzgl. L.

In der kommutativen Theorie ist `LexPos` eine Eliminationsordnung für $L = \{x_1, \ldots, x_i\}$ mit $i \in \{1, \ldots, n\}$. Dies gilt natürlich nicht in der hier behandelten nicht-kommutativen Theorie, wie wir bereits in Beispiel 2.1.4 a) festgestellt haben. Um ein entsprechendes Beispiel für eine Eliminationsordnung anzugeben, definieren wir zunächst die folgende Termordnung auf Σ^*.

Definition 3.3.2 Sei σ eine Termordnung auf Σ^*. Die **nicht-kommutative lexikographische** Termordnung $\texttt{ncLex}\sigma$ auf Σ^* ist wie folgt definiert. Für Terme $w_1, w_2 \in \Sigma^*$ ist $w_1 >_{\texttt{ncLex}\sigma} w_2$ genau dann, wenn $w_1 >_{\texttt{Lex}} w_2$, wobei w_1 und w_2 als kommutative Terme $w_1 = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ bzw. $w_2 = x_1^{\beta_1} \cdots x_n^{\beta_n}$ mit $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{N}_0$ betrachtet werden, oder $w_1 = w_2$ als kommutative Terme und $w_1 >_\sigma w_2$.

Beispiel 3.3.3 Mit $\tau = \texttt{ncLex}\sigma\texttt{Pos}$ erhalten wir so für jede Termordnung σ eine Eliminationsordnung für $L = \{x_1, \ldots, x_i\}$. Ist nämlich $m \in F\backslash\{0\}$ mit $\mathrm{LT}_\tau(m) = w_1 e_j w_1' \in \widehat{F}$, so gilt für einen Term $t = w_2 e_k w_2' \in \mathrm{Supp}(m)$, dass $w_2 w_2' \leq_{\texttt{Lex}} w_1 w_1'$ als kommutative Terme. Damit enthalten auch w_2 und w_2' keine der Unbestimmten $x_1, \ldots, x_i$ und es folgt $t \in \widehat{F}$. Also ist m ein Element in $\widehat{F}$.

Nachdem wir gesehen haben, dass es solche Ordnungen gibt, stellt sich nun die Frage, wie wir zu einem Modul M den zugehörigen Eliminationsmodul $M \cap \widehat{F}$ berechnen können.

Hierzu benötigen wir noch das folgende theoretische Detail.

Lemma 3.3.4 *Sei $\mathbb{T}(\widehat{F})$ die Menge aller Terme in $\widehat{F}$. Dann ist die Restriktion $\widehat{\tau}$ von τ auf $\mathbb{T}(\widehat{F})$ wieder eine Modultermordnung.*

Beweis. Die Behauptung ergibt sich aus der Tatsache, dass $\mathbb{T}(\widehat{F})$ eine Teilmenge von $\mathbb{T}(F)$ ist. Damit folgt aus $t_1 \leq_\tau t_2$ für $t_1, t_2 \in \mathbb{T}(\widehat{F})$ immer $t_1 \leq_{\widehat{\tau}} t_2$. □

Satz 3.3.5 (Berechnung des Eliminationsmoduls)
Sei M ein zweiseitiger Untermodul von F, sei τ eine Eliminationsordnung für L und $\widehat{\tau}$ die Restriktion von τ auf $\mathbb{T}(\widehat{F})$. Ist nun $G \subseteq M$ eine τ-Gröbnerbasis von M, dann ist $\widehat{G} = G \cap \widehat{F}$ eine $\widehat{\tau}$-Gröbnerbasis des Eliminationsmoduls $M \cap \widehat{F}$ von M bzgl. L.

Beweis. Sei $m \in (M \cap \widehat{F})\backslash\{0\}$. Es ist nun zu zeigen, dass $\mathrm{LT}_{\widehat{\tau}}(m) = w\mathrm{LT}_{\widehat{\tau}}(g)w'$ für ein $g \in \widehat{G}$ und $w, w' \in \widehat{\Sigma}^*$. Zunächst ist $\mathrm{LT}_{\widehat{\tau}}(m) = \mathrm{LT}_\tau(m) \in \mathrm{LT}_\tau\{M\}$, da $\widehat{\tau}$ nur eine Restriktion von τ ist. Da nun G eine τ-Gröbnerbasis von M ist, existieren ein $g \in G$ und $w, w' \in \Sigma^*$ mit $\mathrm{LT}_{\widehat{\tau}}(m) = w\mathrm{LT}_\tau(g)w'$. Aus $m \in \widehat{F}$ folgt dabei $w, w' \in \widehat{\Sigma}^*$ und $\mathrm{LT}_\tau(g) \in \widehat{F}$. Nach Voraussetzung ist τ eine Eliminationsordnung für L, also gilt $g \in \widehat{F}$ und damit $g \in \widehat{G}$. Mit $\mathrm{LT}_\tau(g) = \mathrm{LT}_{\widehat{\tau}}(g)$ folgt nun die Behauptung. □

Ist G im obigen Satz zudem eine reduzierte τ-Gröbnerbasis von M, so gilt wegen $\widehat{G} \subseteq G$, dass auch $\widehat{G}$ eine reduzierte $\widehat{\tau}$-Gröbnerbasis von $M \cap \widehat{F}$ ist.

3.4 Komponenten-Elimination

Nachdem wir im vorigen Abschnitt die Grundlagen der Eliminationstheorie kennen gelernt haben, wollen wir nun eine andere Art von Eliminationsordnungen, sogenannte Komponenten-Eliminationsordnungen, studieren. Mit deren Hilfe können Erzeugende anstatt von Unbestimmten aus einem Modul eliminiert werden.

In diesem Abschnitt sei $L \subseteq \{1, \ldots, r\}$ und $\widehat{F}$ der von $\{e_1, \ldots, e_r\} \backslash L$ erzeugte zweiseitige Untermodul von F, d.h.

$$\widehat{F} = \bigoplus_{i \in \{1,\ldots,r\} \backslash L} K[\Sigma^*] e_i K[\Sigma^*].$$

Definition 3.4.1 Sei $L \subseteq \{1, \ldots, r\}$.

1) Eine Modultermordnung τ auf $\mathbb{T}(F)$ heißt **Komponenten-Eliminationsordnung** für L, falls jedes Element $m \in F \backslash \{0\}$ mit $\mathrm{LT}_\tau(m) \in \widehat{F}$ in $\widehat{F}$ enthalten ist.
2) Ist M ein zweiseitiger Untermodul von F, so heißt der zweiseitige Untermodul $M \cap \widehat{F}$ von $\widehat{F}$ der **Komponenten-Eliminationsmodul** von M bzgl. L.

Beispiel 3.4.2 Sei $i \in \{1, \ldots, r\}$ und $L = \{1, \ldots, i\}$. Ist `To` eine Termordnung auf Σ^*, so ist die Modultermordnung $\tau =$ `PosTo` eine Komponenten-Eliminationsordnung für L. Denn für ein Element $m \in F \backslash \{0\}$ mit $\mathrm{LT}_\tau(m) = w_1 e_j w_1' \in \widehat{F}$ und einen Term $t = w_2 e_k w_2' \in \mathrm{Supp}(m)$ ist $t \leq_\tau \mathrm{LT}_\tau(m)$ und damit $k \geq j$. Also ist auch $t \in \widehat{F}$ und m ein Element in $\widehat{F}$.

Eine dem Lemma 3.3.4 entsprechende Aussage gilt auch hier und bleibt deshalb ohne Beweis.

Lemma 3.4.3 *Sei $\mathbb{T}(\widehat{F})$ die Menge aller Terme in $\widehat{F}$. Dann ist die Restriktion $\widehat{\tau}$ von τ auf $\mathbb{T}(\widehat{F})$ wieder eine Modultermordnung.* □

Wir erhalten wie im vorherigen Abschnitt den folgenden Satz für die Berechnung des Komponenten-Eliminationsmoduls.

Satz 3.4.4 *Sei M ein zweiseitiger Untermodul von F und $L \subseteq \{1, \ldots, r\}$. Weiter sei τ eine Komponenten-Eliminationsordnung für L und $\widehat{\tau}$ die Restriktion von τ auf $\mathbb{T}(\widehat{F})$. Ist nun G eine τ-Gröbnerbasis von M, dann ist $\widehat{G} = G \cap \widehat{F}$ eine $\widehat{\tau}$-Gröbnerbasis des Komponenten-Eliminationsmoduls $M \cap \widehat{F}$ von M bzgl. L.*

Beweis. Sei $m \in (M \cap \widehat{F}) \backslash \{0\}$. Es ist nun zu zeigen, dass $\mathrm{LT}_{\widehat{\tau}}(m) = w\mathrm{LT}_{\widehat{\tau}}(g)w'$ für ein $g \in \widehat{G}$ und $w, w' \in \Sigma^*$. Zunächst ist $\mathrm{LT}_{\widehat{\tau}}(m) = \mathrm{LT}_{\tau}(m) \in \mathrm{LT}_{\tau}\{M\}$, da $\widehat{\tau}$ nur eine Restriktion von τ ist. Da nun G eine τ-Gröbnerbasis von M ist, existieren ein $g \in G$ und $w, w' \in \Sigma^*$ mit $\mathrm{LT}_{\widehat{\tau}}(m) = w\mathrm{LT}_{\tau}(g)w'$. Aus $m \in \widehat{F}$ folgt dabei $\mathrm{LT}_{\tau}(g) \in \widehat{F}$. Nach Voraussetzung ist τ eine Komponenten-Eliminationsordnung für L, also gilt $g \in \widehat{F}$ und damit $g \in \widehat{G}$. Mit $\mathrm{LT}_{\tau}(g) = \mathrm{LT}_{\widehat{\tau}}(g)$ folgt nun die Behauptung. □

Wir wollen nun kurz die Anwendung von Komponenten-Elimination auf Moduloperationen ansprechen. Dies soll andeuten, wie vielfältig diese eingesetzt werden kann. Wir demonstrieren hier aber lediglich die Berechnung des Durchschnitts von zwei zweiseitigen Untermoduln von F.

Satz 3.4.5 (Durchschnitte von Moduln)
Seien M und N zweiseitige Untermoduln von F erzeugt von $\{g_1, \ldots, g_s\}$ bzw. von $\{h_1, \ldots, h_t\}$. Weiter sei F_{2r} der freie von $\{e_1, \ldots, e_r, e_{r+1}, \ldots, e_{2r}\}$ zweiseitig erzeugte Modul. Dabei bezeichne $\overline{m}$ das $m \in F$ entsprechende Element in F_{2r}. Für $h_k = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_i w'_{ij}$ sei $h'_k = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij}$. Ist V der von $\{\overline{g}_1, \ldots, \overline{g}_s, \overline{h}_1 - h'_1, \ldots, \overline{h}_t - h'_t\}$ zweiseitig erzeugte Untermodul von F_{2r}, so gilt:

$$V \cap \langle e_{r+1}, \ldots, e_{2r} \rangle \cong M \cap N.$$

Beweis. Sei wieder $\widehat{F}$ der freie von $\{e_{r+1}, \ldots, e_{2r}\}$ zweiseitig erzeugte Modul. Wir betrachten die Abbildung $\psi : \widehat{F} \longrightarrow F$ mit $\psi(e_{r+i}) = e_i$ für $i = 1, \ldots, r$. Nach der universellen Eigenschaft von $\widehat{F}$ aus Satz 2.2.2 ist ψ ein Homomorphismus und damit auch $\varphi = \psi|_{V \cap \widehat{F}}$. Nun ist φ offensichtlich auch injektiv. Zusätzlich gilt $M \cap N \subseteq \mathrm{Bild}(\varphi)$, denn für $m \in M \cap N$ ist zum einen $\overline{m} = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{h}_i w'_{ij}$ und zum anderen $\overline{m} = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} b_{ij} v_{ij} \overline{g}_i v'_{ij}$ für gewisse $b_{ij}, c_{ij} \in K$, $v_{ij}, v'_{ij}, w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, r$ und $j \in \mathbb{N}$, wobei nur endlich viele der b_{ij} bzw. c_{ij} von Null verschieden sind. Es folgt nun $\overline{m} \in V$ und

$$\sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} h'_i w'_{ij} = \underbrace{\sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (h'_i - \overline{h}_i) w'_{ij}}_{\in V} + \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{h}_i w'_{ij} \in V.$$

Also gilt $m' = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} h'_i w'_{ij} \in V \cap \widehat{F}$ mit $\varphi(m') = m$.

Sei nun umgekehrt $\overline{m} \in V \cap \widehat{F}$, d.h. $\overline{m} \in \widehat{F}$ mit

$$\overline{m} = \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} b_{ij} v_{ij} \overline{g}_i v'_{ij} + \sum_{i=1}^{r} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{h}_i - h'_i) w'_{ij}$$

für gewisse $b_{ij}, c_{ij} \in K$, $v_{ij}, v'_{ij}, w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, r$ und $j \in \mathbb{N}$, wobei nur endlich viele der b_{ij} bzw. c_{ij} von Null verschieden sind. Dann erhalten wir $\varphi(\overline{m}) = \sum_{i=1}^{r} \sum_{j\in\mathbb{N}} b_{ij} v_{ij} g_i v'_{ij} \in M$. Aus $\overline{m} \in \widehat{F}$ folgt aber auch $\sum_{i=1}^{r} \sum_{j\in\mathbb{N}} b_{ij} v_{ij} \overline{g}_i v'_{ij} + \sum_{i=1}^{r} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \overline{h}_i w'_{ij} = 0$, also

$$\varphi(\overline{m}) = -\sum_{i=1}^{r} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} h_i w'_{ij} \in N.$$

Insgesamt haben wir $\text{Bild}(\varphi) = M \cap N$ und die Behauptung bewiesen. □

3.5 Syzygienberechnung

Zum Abschluss dieses Kapitels beschäftigen wir uns nun mit der Lösung unseres Problems, der Berechnung der Syzygien für ein beliebiges Tupel von Elementen aus dem freien zweiseitigen Modul $F = F_r$. Hierbei findet vor allem die im letzten Abschnitt behandelte Theorie der Komponenten-Elimination ihre Anwendung.

Wir gelangen direkt zu dem folgenden zentralen Ergebnis.

Satz 3.5.1 *Sei $G = \{g_1, \ldots, g_s\} \subseteq F_r \backslash \{0\}$, sei $\mathcal{G} = (g_1, \ldots, g_s)$ und F_{r+s} der freie zweiseitige Modul erzeugt von $\{e_1, \ldots, e_r, e_{r+1}, \ldots, e_{r+s}\}$. Dabei bezeichne $\overline{g}_i$ das g_i entsprechende Element in $\overline{F}$. Ist U der von $\{\overline{g}_1 - e_{r+1}, \ldots, \overline{g}_s - e_{r+s}\}$ erzeugte zweiseitige Untermodul von $\overline{F}$, so gilt:*

$$U \cap \langle e_{r+1}, \ldots, e_{r+s} \rangle \cong \text{Syz}(\mathcal{G}).$$

Beweis. Sei zunächst $\widehat{F} = \langle e_{r+1}, \ldots, e_{r+s} \rangle$. Wir betrachten nun die Abbildung $\psi : \widehat{F} \longrightarrow E$ mit $\psi(e_{r+i}) = \varepsilon_i$ für $i = 1, \ldots, s$. Nach der universellen Eigenschaft von $\widehat{F}$ aus Satz 2.2.2 ist ψ ein Homomorphismus und damit auch $\varphi = \psi|_{U\cap\widehat{F}}$. Weiter hat φ offensichtlich einen trivialen Kern und es bleibt daher nur $\text{Bild}(\varphi) = \text{Syz}(\mathcal{G})$ zu zeigen.

Für die Inklusion „$\supseteq$“ sei $m = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij} \in \text{Syz}(\mathcal{G})$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Es ergibt sich das Element

$$\begin{aligned} \overline{m} &= \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij} \\ &= \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij} - \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} (\overline{g}_i - e_{r+i}) w'_{ij} \end{aligned}$$

mit $\varphi(\overline{m}) = m$ und $\overline{m} \in U \cap \widehat{F}$ wegen $\sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij} = 0$.

Sei nun $m \in U \cap \widehat{F}$, d.h. $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Dann ist

$$\begin{aligned} & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij} \\ = & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (\overline{g}_i - e_{r+i}) w'_{ij} + \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{r+i} w'_{ij} \in U. \end{aligned}$$

Wir erhalten also $\lambda(\varphi(m)) = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \overline{g}_i w'_{ij} \in U$. Da in $\lambda(\varphi(m))$ keines der Elemente $e_{r+1}, \ldots, e_{r+s}$ vorkommt und U von $\{\overline{g}_1 - e_{r+1}, \ldots, \overline{g}_s - e_{r+s}\}$ erzeugt wird, muss $\lambda(\varphi(m)) = 0$ gelten. Damit folgt $\varphi(m) \in \mathrm{Syz}(\mathcal{G})$. □

Aus obigem Satz erhalten wir nun die folgende Prozedur zur Berechnung des Syzygienmoduls.

Korollar 3.5.2 (Berechnung des Syzygienmoduls)
Sei $G = \{g_1, \ldots, g_s\} \subseteq F \backslash \{0\}$ und $\mathcal{G} = (g_1, \ldots, g_s)$. Weiter sei F_{r+s} der freie zweiseitige Modul erzeugt von $\{e_1, \ldots, e_r, e_{r+1}, \ldots, e_{r+s}\}$ und $\widehat{F}$ der zweiseitige Untermodul von F_{r+s} erzeugt von $\{e_{r+1}, \ldots, e_{r+s}\}$. Dabei bezeichne $\overline{g}$ das $g \in F$ entsprechende Element in F_{r+s}. Wir betrachten die folgenden Instruktionen:

1) *Wähle eine Komponenten-Eliminationsordnung τ für $L = \{1, \ldots, r\}$ auf $\mathbb{T}(\overline{F})$.*
2) *Berechne eine τ-Gröbnerbasis G des Untermoduls $U = \langle \overline{g}_1 - e_{r+1}, \ldots, \overline{g}_s - e_{r+s} \rangle$ von F_{r+s}.*
3) *Bestimme $\widehat{G} = G \cap \widehat{F}$ und gib $\varphi(\widehat{G})$ aus.*

Dies ist eine Prozedur, die eine $\widehat{\tau}$-Gröbnerbasis des Syzygienmoduls $\mathrm{Syz}(\mathcal{G})$ *von $\mathcal{G}$ aufzählt, wobei $\widehat{\tau}$ die Restriktion von τ auf $\mathbb{T}(\widehat{F})$ ist.*

Beweis. In Satz 3.5.1 haben wir gezeigt, dass der Modul $U \cap \widehat{F}$ isomorph zu $\mathrm{Syz}(\mathcal{G})$ ist. Dabei ist $U \cap \widehat{F}$ aber nichts anderes als der Komponenten-Eliminationsmodul von U bzgl. L. Nach Satz 3.4.4 ist nun die in Schritt 3) berechnete Menge $\widehat{G}$ eine $\widehat{\tau}$-Gröbnerbasis von $U \cap \widehat{F}$, d.h. $\varphi(\widehat{G})$ ist eine $\widehat{\tau}$-Gröbnerbasis des Syzygienmoduls $\mathrm{Syz}(\mathcal{G})$. □

Beispiel 3.5.3 Sei $K = \mathbb{Q}$, $\Sigma = \{x_1, x_2\}$ und F der freie zweiseitige $\mathbb{Q}[\Sigma^*]$-Modul erzeugt von $\{e_1, e_2\}$. Wir wollen nun von Tupeln $\mathcal{G} = (g_1, g_2, g_3) \in F^3$ den zugehörigen Syzygienmodul $\mathrm{Syz}(\mathcal{G})$ berechnen und gehen dabei wie in Korollar 3.5.2 vor. Als Komponenten-Eliminationsordnung für $L = \{1, 2\}$ auf

$\mathbb{T}(F_5)$ wählen wir $\tau = \texttt{PosLLex}$, wobei $F_5 = \langle e_1, \ldots, e_5 \rangle$ ist.

a) Seien zunächst $g_1 = e_1x_1 + e_2, g_2 = x_2e_1x_1x_2 + x_2e_1, g_3 = x_2^2e_2x_2 + x_1e_2$. In Schritt 2) erfolgt die Berechnung einer τ-Gröbnerbasis des Moduls $U = \langle e_1x_1 + e_2 - e_3, x_2e_1x_1x_2 + x_2e_1 - e_4, x_2^2e_2x_2 + x_1e_2 - e_5 \rangle$. Dabei ergeben sich die folgenden S-Vektoren:

$$\begin{aligned}
S_{12} &= x_2(g_1 - e_3)x_2 - (g_2 - e_4) = -x_2e_1 + x_2e_2x_2 - x_2e_3x_2 + e_4 =: g_4 \\
S_{14} &= x_2(g_1 - e_3) + g_4x_1 \\
&= x_2e_2x_2x_1 + x_2e_2 - x_2e_3x_2x_1 - x_2e_3 + e_4x_1 =: g_5 \\
S_{24} &= (g_2 - e_4) + g_4x_1x_2 \\
&= x_2e_1 + x_2e_2x_2x_1x_2 - x_2e_3x_2x_1x_2 + e_4x_1x_2 - e_4 \\
&\xrightarrow{g_4} x_2e_2x_2x_1x_2 + x_2e_2x_2 - x_2e_3x_2x_1x_2 - x_2e_3x_2 + e_4x_1x_2 \\
&\xrightarrow{g_5} 0 \\
S_{35} &= (g_3 - e_5)x_1 - x_2g_5 \\
&= x_1e_2x_1 - e_5x_1 - x_2^2e_2 + x_2^2e_3x_2x_1 + x_2^2e_3 - x_2e_4x_1 =: g_6.
\end{aligned}$$

Wir erhalten somit $G = \{g_1 - e_2, g_2 - e_3, g_3 - e_4, g_4, g_5, g_6\}$ als τ-Gröbnerbasis von U und folglich $G \cap \langle e_3, e_4, e_5 \rangle = \emptyset$. Der Syzygienmodul von $\mathcal{G} = (g_1, g_2, g_3)$ ist demnach $\mathrm{Syz}(\mathcal{G}) = \{0\}$.

b) Wir betrachten nun die Elemente $g_1 = e_1x_1 + x_1e_2$, $g_2 = x_2e_1x_1x_2 + e_2x_2^2$ und $g_3 = x_2x_1e_2 - e_2x_2$. Bei der Bestimmung einer τ-Gröbnerbasis von $U = \langle e_1x_1 + x_1e_2 - e_3, x_2e_1x_1x_2 + e_2x_2^2 - e_4, x_2x_1e_2 - e_2x_2 - e_5 \rangle$ erhalten wir den S-Vektor

$$\begin{aligned}
S_{12} &= x_2(g_1 - e_3)x_2 - (g_2 - e_4) = x_2x_1e_2x_2 - e_2x_2^2 - x_2e_3x_2 + e_4 \\
&\xrightarrow{g_3 - e_5} -x_2e_3x_2 + e_4 + e_5x_2 =: g_4.
\end{aligned}$$

Es ergibt sich die τ-Gröbnerbasis $G = \{g_1 - e_2, g_2 - e_3, g_3 - e_4, g_4\}$ von U. Also gilt $\widehat{G} = G \cap \langle e_3, e_4, e_5 \rangle = \{g_4\}$. Der Syzygienmodul von $\mathcal{G}$ wird demnach erzeugt von

$$\varphi(g_4) = -x_2\varepsilon_1x_2 + \varepsilon_2 + \varepsilon_3x_2.$$

Es lässt sich nun auch der Syzygienmodul für ein Tupel $\mathcal{G} = (g_1, \ldots, g_s)$ aus nicht-kommutativen Polynomen $g_1, \ldots, g_s \in K[\Sigma^*]$ berechnen. Wir betrachten dazu das folgende Satz 3.5.1 entsprechende Resultat.

Satz 3.5.4 *Sei $G = \{g_1, \ldots, g_s\} \subseteq K[\Sigma^*]\backslash\{0\}$ und $\mathcal{G} = (g_1, \ldots, g_s)$. Weiter sei F_{s+1} der freie zweiseitige Modul erzeugt von $\{e_1, e_2, \ldots, e_{s+1}\}$. Ist U der von $\{e_1g_1 - e_2, \ldots, e_1g_s - e_{s+1}, x_1e_1 - e_1x_1, \ldots, x_ne_1 - e_1x_n\}$ zweiseitig erzeugte Untermodul von F_{s+1}, so gilt:*

$$U \cap \langle e_2, \ldots, e_{s+1} \rangle \cong \mathrm{Syz}(\mathcal{G}).$$

Beweis. Sei zunächst $\widehat{F} = \langle e_2, \ldots, e_{s+1} \rangle$. Wir betrachten wieder die Abbildung $\psi : \widehat{F} \longrightarrow E$ mit $\psi(e_{i+1}) = \varepsilon_i$ für $i = 1, \ldots, s$. Nach der universellen Eigenschaft von $\widehat{F}$ aus Satz 2.2.2 ist ψ ein Homomorphismus und damit auch $\varphi = \psi|_{U \cap \widehat{F}}$. Weiter gilt offensichtlich $\mathrm{Kern}(\varphi) = \{0\}$ und es bleibt daher nur $\mathrm{Bild}(\varphi) = \mathrm{Syz}(\mathcal{G})$ zu zeigen.

Für die Inklusion „$\supseteq$“ sei $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij} \in \mathrm{Syz}(\mathcal{G})$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Es ergibt sich das Element

$$\begin{aligned} \overline{m} &= \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+1} w'_{ij} \\ &= \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} - \underbrace{\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (e_1 g_i - e_{i+1}) w'_{ij}}_{\in U} \end{aligned}$$

mit $\overline{m} \in \widehat{F}$ und $\varphi(\overline{m}) = m$. Weiter ist

$$\begin{aligned} & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} \\ = \; & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} e_1 w_{ij} g_i w'_{ij} + \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} (w_{ij} e_1 - e_1 w_{ij}) g_i w'_{ij}. \end{aligned}$$

Nach Lemma 2.6.3 ist dabei $w_{ij} e_1 - e_1 w_{ij} \in N = \langle x_i e_1 - e_1 x_i \,|\, i = 1, \ldots, n \rangle$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$. Also ist auch die rechte Summe in N und damit in U enthalten. Die linke Summe ist aber Null wegen $m \in \mathrm{Syz}(\mathcal{G})$. Also folgt $\overline{m} \in U \cap \widehat{F}$.

Sei nun $m \in U \cap \widehat{F}$, d.h. $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+1} w'_{ij}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Dann ist

$$\begin{aligned} & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} \\ = \; & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (e_1 g_i - e_{i+1}) w'_{ij} + \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+1} w'_{ij} \in U. \end{aligned}$$

Wir erhalten sogar $\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} \in N$, da in der Summe keines der Elemente $e_2, \ldots, e_{s+1}$ vorkommt. Nun lässt sich N auch als zweiseitiger Untermodul von $F_1 = \langle e_1 \rangle$ auffassen. Dann wissen wir aber, dass $N = \mathrm{Kern}(\pi)$ gilt mit dem Homomorphismus π aus Abschnitt 2.6. Also ist $\lambda(\varphi(m)) = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} = \pi(\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij}) = 0$ und damit $\varphi(m) \in \mathrm{Syz}(\mathcal{G})$. □

Mit diesem Ergebnis erhalten wir die folgende Prozedur zur Berechnung des Syzygienmoduls für ein Tupel aus nicht-kommutativen Polynomen.

Korollar 3.5.5 *Sei* $G = \{g_1, \ldots, g_s\} \subseteq K[\Sigma^*]\backslash\{0\}$ *und* $\mathcal{G} = (g_1, \ldots, g_s)$. *Weiter sei* F_{s+1} *der freie zweiseitige Modul erzeugt von* $\{e_1, e_2, \ldots, e_{s+1}\}$ *und* $\widehat{F} = \langle e_2, \ldots, e_{s+1}\rangle$. *Wir betrachten die folgenden Instruktionen:*

1) *Wähle eine Komponenten-Eliminationsordnung* τ *für* $L = \{1\}$ *auf* $\mathbb{T}(F_{s+1})$.
2) *Berechne eine* τ*-Gröbnerbasis* G *des Untermoduls* $U = \langle e_1g_1 - e_2, \ldots, e_1g_s - e_{s+1}, x_1e_1 - e_1x_1, \ldots, x_ne_1 - e_1x_n\rangle$ *von* F_{s+1}.
3) *Bestimme* $\widehat{G} = G \cap \widehat{F}$ *und gib* $\varphi(\widehat{G})$ *aus.*

Dies ist eine Prozedur, die eine $\widehat{\tau}$*-Gröbnerbasis des Syzygienmoduls* $\mathrm{Syz}(\mathcal{G})$ *von* $\mathcal{G}$ *aufzählt, wobei* $\widehat{\tau}$ *die Restriktion von* τ *auf* $\mathbb{T}(\widehat{F})$ *ist.*

Beweis. In Satz 3.5.4 haben wir gezeigt, dass der Modul $U \cap \widehat{F}$ isomorph zu $\mathrm{Syz}(\mathcal{G})$ ist. Dabei ist $U \cap \widehat{F}$ aber nichts anderes als der Komponenten-Eliminationsmodul von U bzgl. L. Nach Satz 3.4.4 ist nun die in Schritt 3) berechnete Menge $\widehat{G}$ eine $\widehat{\tau}$-Gröbnerbasis von $U \cap \widehat{F}$, d.h. $\varphi(\widehat{G})$ ist eine $\widehat{\tau}$-Gröbnerbasis des Syzygienmoduls $\mathrm{Syz}(\mathcal{G})$. □

Kapitel 4

Anwendungen

In diesem Kapitel beschäftigen wir uns mit der Berechnung zweiseitiger Syzygien über Restklassenringen von $K[\Sigma^*]$. Dazu sei σ stets eine Termordnung auf Σ^* und die Menge $G_I = \{f_1, \ldots, f_t\} \subseteq K[\Sigma^*]$ eine σ-Gröbnerbasis des zweiseitigen Ideals I von $K[\Sigma^*]$. Im Folgenden betrachten wir den Restklassenring $R = K[\Sigma^*]/I$ des Polynomrings $K[\Sigma^*]$.

Wir diskutieren nun zunächst den Begriff der Gröbnerbasis für Restklassenmoduln. Diesen führen wir über einen neuen Reduktionsbegriffs ein und orientieren uns dabei an der von Madlener und Reinert ([6], [7]) beschriebenen Präfix-Reduktion, d.h. wir setzen diese als zweiseitige Reduktion fort. Die daraus entwickelte Theorie ermöglicht uns nun wieder, in Abschnitt 2 eine Prozedur zur Berechnung zweiseitiger Syzygien eines Tupel $(\overline{g}_1, \ldots, \overline{g}_s) \in R^s$ anzugeben. Dabei führen wir die Berechnung dieser Syzygien zurück auf die Berechnungen in $K[\Sigma^*]$. Im Wesentlichen betrachten wir dabei das Tupel $(g_1, \ldots, g_s, f_1, \ldots, f_t) \in K[\Sigma^*]^{s+t}$.

Den Abschluss dieser Arbeit stellt die Übertragung unserer Erkenntnisse auf Monoidringe dar. Als Anwendung befassen wir uns in diesem Zusammenhang mit dem sogenannten *Konjugationssuchproblem* in Monoidringen. Die Aufgabe besteht hierbei darin zu überprüfen, ob zu Elementen g_1 und g_2 ein f existiert, so dass die Gleichung $fg_1f^{-1} = g_2$ erfüllt ist, und dieses gegebenenfalls anzugeben. Dieses Problem lässt sich nun entscheiden, wenn alle Syzygien des Tupels (g_1, g_2) bekannt sind. Die Syzygienberechnung wird somit zum zentralen Bestandteil der Lösung dieses Problems.

4.1 Gröbnerbasen für Restklassenmoduln

In diesem Abschnitt befassen wir uns mit der Gröbnerbasistheorie für zweiseitige Moduln über einem Restklassenring R. Dazu müssen wir zunächst er-

klären, was unter einem solchen Modul zu verstehen ist. Wir definieren dazu analog zu Abschnitt 2.2 zunächst den freien zweiseitigen R-Modul $\overline{E}_1$ vom Rang 1 als das Tensorprodukt $R \otimes_K R$ mit der entsprechenden zweiseitigen skalaren Multiplikation. Der freie zweiseitige R-Modul $\overline{E}_s$ vom Rang s ist nun wieder die direkte Summe $\bigoplus_{i=1}^{s} R \otimes_K R$, die wir zur besseren Verständlichkeit wieder schreiben als $\overline{E} = \overline{E}_s = \bigoplus_{i=1}^{s} R\varepsilon_i R$. Schließlich überträgt sich aufgrund der gleichen Konstruktion des Moduls auch die universelle Eigenschaft aus Satz 2.2.2 auf freie zweiseitige R-Moduln.

Sei ab jetzt $\overline{E}$ der freie von $\{\varepsilon_1, \ldots, \varepsilon_s\}$ zweiseitig erzeugte R-Modul und $\overline{M}$ ein zweiseitiger R-Untermodul von $\overline{E}$. Wir interessieren uns nun für die Frage, ob für $\overline{M}$ ein Erzeugendensystem mit den Eigenschaften einer Gröbnerbasis existiert.

Wir führen zunächst einige Notationen ein. Für ein Element $f \in K[\Sigma^*]$ bezeichne $\overline{f}$ die zugehörige Restklasse in R. Da G_I nach Voraussetzung eine σ-Gröbnerbasis von I ist, erhalten wir mit $\xrightarrow{G_I}$ nach Satz 2.4.4 ein konvergentes Termersetzungssytem. D.h jedes Element in $K[\Sigma^*]$ besitzt eine eindeutige Normalform. Wir repräsentieren im Folgenden jede Restklasse $\overline{f} \in P$ stets mit dem zugehörigen irreduziblen Element f in $K[\Sigma^*]$ bzgl. $\xrightarrow{G_I}$.

Die Menge der Terme von R sei definiert als $\mathbb{T}(R) = \{\overline{w} \,|\, w \in \Sigma^*, w \text{ ist irreduzibel bzgl. } \xrightarrow{G_I}\}$ und für $w_1, w_2 \in \mathbb{T}(R)$ schreiben wir $w_1 w_2$ für das Produkt von w_1 und w_2 in $\mathbb{T}(R)$ und $w_1 \cdot w_2$ für die Konkatenation der zugehörigen Elemente in Σ^*. Ferner sei die Identität in $K[\Sigma^*]$ mit $\equiv$ notiert.

Bei der Definition einer Gröbnerbasis für $\overline{M}$ ergibt sich zunächst das Problem, dass auf $\mathbb{T}(\overline{E})$ keine Modultermordnung τ existiert. Denn für Terme $t_1, t_2 \in \mathbb{T}(\overline{E})$ und $w, w' \in \mathbb{T}(R)$ muss aus $t_1 \geq_\tau t_2$ nicht zwangsläufig $wt_1w' \geq_\tau wt_2w'$ folgen. Mögliche Reduktionen durch $\xrightarrow{G_I}$ können dies verhindern. Wir führen deshalb den Begriff der Gröbnerbasis anhand von Termersetzungssytemen ein. Dabei ergibt sich aber ein weiteres Problem. Um zu entscheiden, ob ein Element $m \in \overline{E}$ mit einem $g \in \overline{E}$ reduziert werden kann, muss nach Definition 2.4.1 1) die Gleichung $w\mathrm{LT}_\tau(g)w' = t$ für ein $t \in \mathrm{Supp}(m)$ gelöst werden. Zu dieser Schwierigkeit kommt noch hinzu, dass hierbei nicht $w\mathrm{LT}_\tau(g)w' = \mathrm{LT}_\tau(wgw')$ gelten muss. Wir werden deshalb einen neuen Reduktionsbegriff einführen. Wir greifen dabei auf die in [6] bzw. [7] beschriebene Präfix-Reduktion zurück. Diese beinhaltet nun die Bedingung, dass $t \equiv \mathrm{LT}_\tau(g) \cdot w$ gilt für ein $w \in R$. Da wir in dieser Arbeit zweiseitige Moduln betrachten, verwenden wir also die Bedingung $t \equiv w \cdot \mathrm{LT}_\tau(g) \cdot w'$.

Sei ab jetzt τ eine mit σ verträgliche Modultermordnung auf $\mathbb{T}(E)$, wobei E wieder der freie von $\{\varepsilon_1, \ldots, \varepsilon_s\}$ zweiseitig erzeugte $K[\Sigma^*]$-Modul ist. Es lässt sich τ nun zumindest als Ordnung auf $\mathbb{T}(\overline{E})$ interpretieren.

Für die Definition des Reduktionsbegriffs benötigen wir noch das folgende

theoretische Detail.

Lemma 4.1.1 *Seien $\overline{g} \in R\backslash\{0\}$ und $\overline{w}, \overline{w}' \in \mathbb{T}(R)$, so dass das Element $\overline{w} \cdot \mathrm{LT}_\tau(\overline{g}) \cdot \overline{w}'$ irreduzibel bzgl. $\xrightarrow{G_I}$ ist. Dann gilt*

$$\overline{w} \cdot \mathrm{LT}_\tau(\overline{g}) \cdot \overline{w}' \equiv \overline{w}\,\mathrm{LT}_\tau(\overline{g})\overline{w}' = \mathrm{LT}_\tau(\overline{wgw}').$$

Beweis. Da $\overline{w} \cdot \mathrm{LT}_\tau(\overline{g}) \cdot \overline{w}'$ nach Voraussetzung irreduzibel bzgl. $\xrightarrow{G_I}$ ist, erhalten wir direkt $\overline{w} \cdot \mathrm{LT}_\tau(\overline{g}) \cdot \overline{w}' \equiv \overline{w}\,\mathrm{LT}_\tau(\overline{g})\overline{w}'$. Weiter ergibt sich mit $g \in K[\Sigma^*]$ und $w, w' \in \Sigma^*$ als irreduzible Repräsentanten von $\overline{g}$ bzw. $\overline{w}, \overline{w}'$ die Gleichung $\overline{w}\,\mathrm{LT}_\tau(\overline{g})\overline{w}' = \overline{w\mathrm{LT}_\tau(g)w'}$. Sei nun $\overline{t} \in \mathrm{Supp}(\overline{g})$. Dann gilt

$$\overline{w}\,\overline{t}\,\overline{w}' \leq_\tau \overline{w} \cdot \overline{t} \cdot \overline{w}' \equiv wtw' \leq_\tau w\mathrm{LT}_\tau(g)w' \equiv \overline{w\mathrm{LT}_\tau(g)w'}.$$

Also ist $\overline{w\mathrm{LT}_\tau(g)w'} \geq_\tau \overline{w}\,\overline{t}\,\overline{w}'$ für jeden Term $\overline{w}\,\overline{t}\,\overline{w}' \in \mathrm{Supp}(\overline{wgw}')$ und $\overline{w\mathrm{LT}_\tau(g)w'}$ damit der Leitterm von $\overline{wgw}'$. □

Definition 4.1.2 Seien $g, m \in \overline{E}$ und $\overline{G} \subseteq \overline{E}$.

1) Existieren ein Term $w_1\varepsilon_i w_1' \in \mathrm{Supp}(m)$ und Elemente $w_2, w_2' \in \mathbb{T}(R)$ mit $w_2 \cdot \mathrm{LT}_\tau(g) \cdot w_2' \equiv w_1\varepsilon_i w_1'$, dann sagen wir g **reduziert** m **zweiseitig in einem Schritt** zu $m' = m - \frac{c}{\mathrm{LC}(g)} w_2 g w_2'$. Wir notieren dies mit $m \xrightarrow{g}_z m'$. Hierbei ist c der Koeffizient von $w_1\varepsilon_i w_1'$ in m.
2) Wie in Definition 2.4.1 bezeichne $\xrightarrow{\overline{G}}_z$ den reflexiven und transitiven bzw. $\xleftrightarrow{\overline{G}}_z$ den reflexiven, symmetrischen und transitiven Abschluss von $\bigcup_{g\in\overline{G}} \xrightarrow{g}_z$.

Bemerkung 4.1.3

a) Mit Lemma 4.1.1 folgt direkt $\mathrm{LT}_\tau(m) \geq \mathrm{LT}_\tau(m')$ und analog zu Bemerkung 2.4.2 a) die Tatsache, dass das Termersetzungsystem $\xrightarrow{\overline{G}}_z$ für ein $\overline{G} \subseteq \overline{E}$ stets noethersch ist.
b) Im Gegensatz zu den Termersetzungssystemen aus Kapitel 2 gilt hier für eine Teilmenge $\overline{G} \subseteq \overline{E}$ mit $\overline{M} = \langle\overline{G}\rangle$ nicht zwangsläufig $m \xleftrightarrow{\overline{G}}_z 0$ für alle $m \in \overline{M}$.

Mit dem oben eingeführten Reduktionsbegriff lässt sich nun sinnvoll der Begriff der Gröbnerbasis für einen zweiseitigen R-Untermodul eines freien zweiseitigen R-Moduls definieren.

Definition 4.1.4 Sei $\overline{M}$ ein zweiseitiger R-Untermodul von $\overline{E}$. Eine Menge $\overline{G} \subset \overline{M}$ heißt **(zweiseitige) Gröbnerbasis** von $\overline{M}$, falls das Termersetzungssystem $\xrightarrow{\overline{G}}_z$ konfluent ist und $m \xleftrightarrow{\overline{G}}_z 0$ für alle $m \in \overline{M}$.

Dass diese Definition mit unserem bisherigen Verständnis von Gröbnerbasen aus Kapitel 2 übereinstimmt, zeigt der folgende Satz.

Satz 4.1.5 *Sei $\overline{M}$ ein zweiseitiger R-Untermodul von $\overline{E}$ und $\overline{G} \subset \overline{M}$. Dann sind die folgenden Aussagen äquivalent:*

a) $\overline{G}$ ist eine Gröbnerbasis von $\overline{M}$.
b) Jedes von Null verschiedene Element $m \in \overline{M}$ besitzt eine Darstellung der Form $m = \sum_{i=1}^{t} c_i w_i g_i w_i'$ mit $c_i \in K\backslash\{0\}$, $w_i, w_i' \in \mathbb{T}(R)$, $g_i \in \overline{G}$ und $\mathrm{LT}_\tau(m) \geq_\tau w_i \cdot \mathrm{LT}_\tau(g_i) \cdot w_i' \geq_\tau \mathrm{LT}_\tau(w_i g_i w_i')$ für $i = 1, \ldots, t$.
c) Es gilt $\mathrm{LT}_\tau\{\overline{M}\} = \{w \cdot \mathrm{LT}_\tau(g) \cdot w' \mid g \in \overline{G}, w, w' \in \mathbb{T}(R)\}$.

Beweis. Sei zunächst $\overline{G}$ eine Gröbnerbasis von $\overline{M}$ und $m \in \overline{M}\backslash\{0\}$. Nach Definition gilt also $m \xleftrightarrow{\overline{G}}_z 0$. Es gilt sogar $m \xrightarrow{\overline{G}}_z 0$, da 0 stets irreduzibel und das Termersetzungssystem $\xrightarrow{\overline{G}}_z$ konfluent ist, d.h. dass jedes Element genau eine Normalform besitzt. Wir können m also schreiben als $m = \sum_{i=1}^{t} c_i w_i g_i w_i'$ mit $c_i \in K\backslash\{0\}$, $w_i, w_i' \in \mathbb{T}(R)$ und $g_i \in \overline{G}$ für $i = 1, \ldots, t$. Dabei ist jeweils $\mathrm{LT}_\tau(m) \geq w_i \cdot \mathrm{LT}_\tau(g_i) \cdot w_i' \equiv \mathrm{LT}_\tau(w_i g_i w_i')$ nach obiger Bemerkung und damit b) erfüllt.

Für die Implikation b) $\Rightarrow$ c) sei nun m von solcher Gestalt. Es muss ein $i \in \{1, \ldots, t\}$ geben, so dass $\mathrm{LT}_\tau(m) = \mathrm{LT}_\tau(w_i g_i w_i')$. Dann ist aber $\mathrm{LT}_\tau(m) \equiv w_i \cdot \mathrm{LT}_\tau(g_i) \cdot w_i'$ und c) gezeigt.

Um c) $\Rightarrow$ a) zu zeigen, sei $m \in \overline{M}\backslash\{0\}$. Es existieren nun ein $g_1 \in \overline{G}$ und Terme $w_1, w_1' \in \mathbb{T}(R)$ mit $\mathrm{LT}_\tau(m) \equiv w_1 \cdot \mathrm{LT}_\tau(g_1) \cdot w_1'$. Wir können m zweiseitig reduzieren zu $m_1 = m - \frac{\mathrm{LC}_\tau(m)}{\mathrm{LC}_\tau(g_1)} w_1 g_1 w_1' \in \overline{M}$. Nach Bemerkung 4.1.3 ist dabei $\mathrm{LT}_\tau(m) >_\tau \mathrm{LT}_\tau(m_1)$. Zu m_1 gibt es wieder ein Element $g_2 \in \overline{G}$, welches m_1 zu $m_2 \in \overline{E}$ zweiseitig reduziert mit $\mathrm{LT}_\tau(m_1) >_\tau \mathrm{LT}_\tau(m_2)$. Da das Termersetzungsystem $\xrightarrow{\overline{G}}_z$ noethersch ist, endet eine Iteration dieses Verfahrens in endlich vielen Schritten. Wir erhalten demnach Elemente $g_1, \ldots, g_l \in \overline{G}$ und $m_1, \ldots, m_l \in \overline{E}$ mit $m \xrightarrow{g_1}_z m_1 \xrightarrow{g_2}_z \cdots \xrightarrow{g_l}_z m_l$. Aufgrund der Irreduzibilität von m_l folgt direkt $m_l = 0$ und damit $m \xrightarrow{\overline{G}}_z 0$. Die Konfluenz von $\xrightarrow{\overline{G}}_z$ folgt analog zum Beweis von Satz 2.4.4. □

4.2 Syzygien in Restklassenringen

In diesem Abschnitt wollen wir uns mit der Syzygienberechnung in Restklassenringen $R = K[\Sigma^*]/I$ beschäftigen. Wir führen diese auf die Syzygienberechnung im Polynomring $K[\Sigma^*]$ zurück, um dann die Ergebnisse aus

Abschnitt 3.5 anwenden zu können.

Im Folgenden betrachten wir Abbildungen zwischen $K[\Sigma^*]$-Moduln und R-Moduln. Sei dazu $\eta : K[\Sigma^*] \longrightarrow R$, $f \mapsto \overline{f}$ der kanonische Epimorphismus. Mit $\tilde{\eta} : E_1 = K[\Sigma^*] \otimes_K K[\Sigma^*] \longrightarrow \overline{E}_1 = R \otimes_K R$, $\tilde{\eta} = \eta \otimes_K \eta$ erhalten wir nun einen Homomorphismus zweiseitiger $K[\Sigma^*]$-Moduln. Diesen können wir auf $E = E_s$ fortsetzen und erhalten $\vartheta : E \longrightarrow \overline{E}$, $\vartheta = \bigoplus_{i=1}^{s} \tilde{\eta}$.

Im Weiteren sei $\overline{G} = \{\overline{g}_1, \ldots, \overline{g}_s\} \subseteq R$ und $\overline{\mathcal{G}} = (\overline{g}_1, \ldots, \overline{g}_s)$. Wir wollen nun zunächst formal den Begriff einer Syzygie von $\overline{\mathcal{G}}$ definieren.

Definition 4.2.1 Sei $m \in \overline{E}$, d.h. $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \varepsilon_i \overline{w}'_{ij}$ mit $c_{ij} \in K$, $\overline{w}_{ij}, \overline{w}'_{ij} \in \mathbb{T}(R)$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Das Element m heißt **(zweiseitige) Syzygie** von $\overline{\mathcal{G}}$, falls die Gleichung

$$\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \overline{g}_i \overline{w}'_{ij} = 0$$

erfüllt ist.

Wir erhalten mit $\overline{\lambda} : \overline{E} \longrightarrow \overline{M}$, $\varepsilon_i \mapsto \overline{g}_i$ nach der universellen Eigenschaft von $\overline{E}$ wieder einen Homomorphismus mit $\mathrm{Kern}(\overline{\lambda}) = \mathrm{Syz}(\overline{\mathcal{G}})$. Die Menge aller Syzygien $\mathrm{Syz}(\overline{\mathcal{G}})$ bildet also einen zweiseitigen R-Untermodul von $\overline{E}$. Im Folgenden wollen wir für diesen Modul eine Gröbnerbasis berechnen. Wir erhalten mit unseren Kenntnissen aus Kapitel 2 das folgende Resultat. Dabei sei E_{s+t} der von $\{\varepsilon_1, \ldots, \varepsilon_{s+t}\}$ erzeugte zweiseitige freie $K[\Sigma^*]$-Modul und ψ der von $\tilde{\eta}$ induzierte Homomorphismus $\psi : E_{s+t} \longrightarrow \overline{E}$ mit $\psi(\sum_{i=1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij}) = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \varepsilon_i \overline{w}'_{ij}$.

Satz 4.2.2 *Sei $\overline{G} = \{\overline{g}_1, \ldots, \overline{g}_s\} \subseteq R$ und $\overline{\mathcal{G}} = (\overline{g}_1, \ldots, \overline{g}_s)$. Weiter sei $\mathcal{G} = (g_1, \ldots, g_s, f_1, \ldots, f_t) \in (K[\Sigma^*])^{s+t}$ und $\tilde{\tau}$ eine Modultermordnung auf $\mathbb{T}(E_{s+t})$ mit $\varepsilon_i >_{\tilde{\tau}} \varepsilon_j$ für alle $i \in \{1, \ldots, s\}$ und $j \in \{s+1, \ldots, s+t\}$, so dass τ die Restriktion von $\tilde{\tau}$ auf $\mathbb{T}(E)$ ist. Ist G eine $\tilde{\tau}$-Gröbnerbasis von $\mathrm{Syz}(\mathcal{G})$, dann ist $\psi(G)\backslash\{0\}$ eine Gröbnerbasis von $\mathrm{Syz}(\overline{\mathcal{G}})$.*

Beweis. Wir zeigen zunächst, dass $\psi(G) \subseteq \mathrm{Syz}(\overline{\mathcal{G}})$ gilt. Sei dazu $g \in G$, also $g = \sum_{i=1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s+t$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Dann ist

$$\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} + \sum_{i=s+1}^{s+t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} f_{i-s} w'_{ij} = 0.$$

Es folgt also $\psi(g) = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \overline{g}_i \overline{w}'_{ij} = \overline{0}$ und wir erhalten damit wie gewünscht $\psi(g) \in \mathrm{Syz}(\overline{\mathcal{G}})$.

Sei nun G eine $\tilde{\tau}$-Gröbnerbasis von $\mathrm{Syz}(\mathcal{G})$ und $m \in \mathrm{Syz}(\overline{\mathcal{G}})\backslash\{0\}$, d.h. $m = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}\overline{w}_{ij}\varepsilon_i\overline{w}'_{ij}$ mit $c_{ij} \in K$, $\overline{w}_{ij}, \overline{w}'_{ij} \in \mathbb{T}(R)$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Zu zeigen ist, dass ein $\overline{g} \in \psi(G)\backslash\{0\}$ und Elemente $\overline{w}, \overline{w}' \in \mathbb{T}(R)$ existieren mit $\mathrm{LT}_\tau(m) \equiv \overline{w}\cdot\mathrm{LT}_\tau(g)\cdot\overline{w}'$. Da $m \in \mathrm{Syz}(\overline{\mathcal{G}})$ ist, gilt $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}\overline{w}_{ij}\overline{g}_i\overline{w}'_{ij} = \overline{0}$. Das bedeutet, dass $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}\overline{w}_{ij}\cdot\overline{g}_i\cdot\overline{w}'_{ij} \in I = \langle f_1, \ldots, f_t\rangle_{K[\Sigma^*]}$. Wir erhalten demnach

$$\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}\overline{w}_{ij}\cdot\overline{g}_i\cdot\overline{w}'_{ij} = \sum_{i=1}^{t}\sum_{j\in\mathbb{N}} d_{ij}v_{ij}f_iv'_{ij}$$

mit $d_{ij} \in K$, $v_{ij}, v'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele d_{ij} von Null verschieden sind. Wir können dafür auch schreiben

$$\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij} - \sum_{i=1}^{t}\sum_{j\in\mathbb{N}} d_{ij}v_{ij}f_iv'_{ij} = 0.$$

Es folgt also $m' = \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\varepsilon_iw'_{ij} - \sum_{i=1}^{t}\sum_{j\in\mathbb{N}} d_{ij}v_{ij}\varepsilon_{s+i}v'_{ij} \in \mathrm{Syz}(\mathcal{G})$, wobei $\psi(m') = m$ gilt. Da nun G eine $\tilde{\tau}$-Gröbnerbasis von $\mathrm{Syz}(\mathcal{G})$ und das Leitmonom von m' nach Voraussetzung ein Summand in der ersten Summe ist, existieren Elemente $g \in G$ und $w, w' \in \Sigma^*$ mit $w\mathrm{LT}_{\tilde{\tau}}(g)w' = \mathrm{LT}_{\tilde{\tau}}(m') \equiv \mathrm{LT}_\tau(m)$. Es bleibt nun noch zu zeigen, dass $\overline{w}\cdot\mathrm{LT}_\tau(\psi(g))\cdot\overline{w}' \equiv \mathrm{LT}_\tau(m)$ erfüllt ist. Sei also $\mathrm{LT}_{\tilde{\tau}}(m') = w_{ij}\varepsilon_iw'_{ij}$ für ein $i \in \{1, \ldots, s\}$ und $j \in \mathbb{N}$. Dann sind w_{ij} und w'_{ij} irreduzibel bzgl. $\xrightarrow{G_I}$. Ist $\mathrm{LT}_{\tilde{\tau}}(g) = w_1\varepsilon_iw_2$ für $w_1, w_2 \in \Sigma^*$, so sind demnach auch w_1 und w_2 irreduzibel. Es gilt also $\mathrm{LT}_\tau(\psi(g)) = \psi(\mathrm{LT}_{\tilde{\tau}}(g))$ und folglich $\mathrm{LT}_\tau(m) \equiv \overline{w}\cdot\mathrm{LT}_{\tilde{\tau}}(g)\cdot\overline{w}' \equiv \overline{w}\cdot\psi(\mathrm{LT}_{\tilde{\tau}}(g))\cdot\overline{w}' \equiv \overline{w}\cdot\mathrm{LT}_\tau(\psi(g))\cdot\overline{w}'$. Damit haben wir die Behauptung bewiesen. □

Um nun eine Gröbnerbasis von $\mathrm{Syz}(\overline{\mathcal{G}})$ zu berechnen, benötigen wir nach obigem Satz eine Gröbnerbasis des Syzygienmoduls von $\mathcal{G}$. Eine solche sind wir aber bereits im Stande zu berechnen, denn Korollar 3.5.5 stellt eine entsprechende Prozedur zur Verfügung. Dabei muss lediglich in Schritt 1) die Komponenten-Eliminationsordnung so gewählt werden, dass deren Restriktion auf $\mathbb{T}(E)$ der Modultermordnung τ entspricht. Es bietet sich deshalb an, direkt $\tau = \mathtt{Pos}\sigma$ zu setzen. Dies vereinfacht auch die Wahl von $\tilde{\tau}$ im vorangehenden Satz.

In der Prozedur zur Berechnung einer Gröbnerbasis von $\mathrm{Syz}(\mathcal{G})$ wird bekanntlich der entsprechende zweiseitige Modul U mit den zusätzlichen Erzeugenden $\{e_2, \ldots, e_{s+t+1}\}$ betrachtet. Der Rechenaufwand für die Bestimmung einer Gröbnerbasis von U hängt natürlich von der Anzahl der Erzeugenden ab. Dieser lässt sich nun reduzieren, indem wir die t Erzeugenden, die die Elemente $f_1, \ldots, f_t$ betreffen, vermeiden. Terme in diesen Erzeugenden werden

sowieso aufgrund der späteren Anwendung der Abbildung ψ ohnehin nicht berücksichtigt. Wir kommen so zu der folgenden Variation von Korollar 3.5.5.

Satz 4.2.3 *Sei $\overline{G} = \{\overline{g}_1, \ldots, \overline{g}_s\} \subseteq R$, sei $\overline{\mathcal{G}} = (\overline{g}_1, \ldots, \overline{g}_s)$, sei F_{s+1} der freie zweiseitige $K[\Sigma^*]$-Modul erzeugt von $\{e_1, e_2, \ldots, e_{s+1}\}$ und $\widehat{F}$ erzeugt von $\{e_2, \ldots, e_{s+1}\}$. Weiter sei $U = \langle e_1 g_1 - e_2, \ldots, e_1 g_s - e_{s+1}, e_1 f_1, \ldots, e_1 f_t, x_1 e_1 - e_1 x_1, \ldots, x_n e_1 - e_1 x_n \rangle$ ein zweiseitiger $K[\Sigma^*]$-Untermodul von F_{s+1} und φ eine Abbildung mit $\varphi = \psi|_{U \cap \widehat{F}}$. Wir betrachten die folgenden Instruktionen:*

1) *Wähle eine Komponenten-Eliminationsordnung $\tilde{\tau}$ für $L = \{1\}$ auf $\mathbb{T}(F_{s+1})$, so dass τ die Restriktion von $\tilde{\tau}$ auf $\mathbb{T}(E)$ ist.*
2) *Berechne eine $\tilde{\tau}$-Gröbnerbasis G von U.*
3) *Bestimme $\widehat{G} = G \cap \widehat{F}$ und gib $\varphi(\widehat{G}) \backslash \{0\}$ aus.*

Dies ist eine Prozedur, die eine Gröbnerbasis des Syzygienmoduls von $\overline{\mathcal{G}}$ aufzählt.

Beweis. Wir zeigen zunächst, dass $\varphi(U \cap \widehat{F}) = \mathrm{Syz}(\overline{\mathcal{G}})$ erfüllt ist. Sei also $m \in U \cap \widehat{F}$, d.h. $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+1} w'_{ij}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \Sigma^*$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Ein früher bereits verwendetes Argument liefert

$$\begin{aligned} m &= \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_{i+1} w'_{ij} \\ &= \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} - \underbrace{\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (e_1 g_i - e_{i+1}) w'_{ij}}_{\in U} \in U \end{aligned}$$

und damit $m' = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} e_1 g_i w'_{ij} \in U$. Da in m' keines der Erzeugenden $e_2, \ldots, e_{s+1}$ vorkommt, muss m' in dem zweiseitigen $K[\Sigma^*]$-Untermodul $\langle e_1 f_1, \ldots, e_1 f_t, x_1 e_1 - e_1 x_1, \ldots, x_n e_1 - e_1 x_n \rangle$ von F_{s+1} enthalten sein. Also lässt sich m' schreiben als $m' = \sum_{i=1}^{t} \sum_{j \in \mathbb{N}} d_{ij} v_{ij} e_1 f_i v'_{ij} + m''$ mit $m'' \in N$, $d_{ij} \in K$, $v_{ij}, v'_{ij} \in \Sigma^*$ für $i = 1, \ldots, t$ und $j \in \mathbb{N}$, wobei nur endlich viele d_{ij} von Null verschieden sind. Es folgt nun mit den Abbildungen π aus Kapitel 2 und $\overline{\lambda}$

$$\begin{aligned} \overline{\lambda}(\varphi(m)) &= \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} \overline{g}_i \overline{w}'_{ij} = \overline{\pi(m')} \\ &= \sum_{i=1}^{t} \sum_{j \in \mathbb{N}} d_{ij} \overline{v}_{ij} \overline{f}_i \overline{v}'_{ij} = \overline{0}. \end{aligned}$$

Also ist $\varphi(m) \in \mathrm{Syz}(\overline{\mathcal{G}})$.

Nach Satz 3.4.4 ist die in den Schritten 2) und 3) berechnete Menge $\widehat{G}$ eine τ-Gröbnerbasis von $U \cap \widehat{F}$. Es bleibt nun noch zu zeigen, dass für alle $m \in \mathrm{Syz}(\overline{\mathcal{G}}) \backslash \{0\}$ Elemente $\overline{g} \in \varphi(\widehat{G})$ und $\overline{w}, \overline{w}' \in \mathbb{T}(R)$ existieren, so dass

$\mathrm{LT}_\tau(m) \equiv \overline{w} \cdot \mathrm{LT}_\tau(\overline{g}) \cdot \overline{w}'$ erfüllt ist.

Sei also $m \in \mathrm{Syz}(\overline{\mathcal{G}})\backslash\{0\}$, d.h. $m = \sum_{i=1}^{s} \sum_{j\in\mathbb{N}} c_{ij}\overline{w}_{ij}\varepsilon_i\overline{w}'_{ij}$ mit $c_{ij} \in K$, $\overline{w}_{ij}, \overline{w}'_{ij} \in \mathbb{T}(R)$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Wir gehen nun ähnlich wie im Beweis zu Satz 3.5.4 vor. Es ergibt sich zunächst das Element

$$\begin{aligned} m' &= \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_{i+1}w'_{ij} \\ &= \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_1g_iw'_{ij} - \underbrace{\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}(e_1g_i - e_{i+1})w'_{ij}}_{\in U} \end{aligned}$$

mit $m' \in \widehat{F}$ und $\varphi(m') = m$. Weiter ist

$$\begin{aligned} &\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}e_1g_iw'_{ij} \\ = &\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}e_1w_{ij}g_iw'_{ij} + \sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}(w_{ij}e_1 - e_1w_{ij})g_iw'_{ij}. \end{aligned}$$

Die rechte Summe ist nun wieder in N und damit in U enthalten. Wegen $m \in \mathrm{Syz}(\overline{\mathcal{G}})$ ist $\sum_{i=1}^{s}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_iw'_{ij} \in I$ und die linke Summe damit in dem $K[\Sigma^*]$-Untermodul $\langle e_1f_1, \ldots, e_1f_t, x_1e_1 - e_1x_1, \ldots, x_ne_1 - e_1x_n\rangle \subseteq U$ von F_{s+1}. Also folgt $m' \in U \cap \widehat{F}$. Es existieren nun Elemente $g \in \widehat{G}$ und $w, w' \in \Sigma^*$ mit $\mathrm{LT}_\tau(m') = w\mathrm{LT}_\tau(g)w'$. Ist $\mathrm{LT}_\tau(g) = w_1\varepsilon_iw_2$ für ein $i \in \{1, \ldots, s\}$ und $w_1, w_2 \in \Sigma^*$, so sind w_1 und w_2 irreduzibel bzgl. $\xrightarrow{G_I}$, denn w_{ij} und w'_{ij} sind nach Voraussetzung irreduzibel für alle $j \in \mathbb{N}$. Also folgt $\mathrm{LT}_\tau(\varphi(g)) = \varphi(\mathrm{LT}_\tau(g))$ und damit $\mathrm{LT}_\tau(m) \equiv \mathrm{LT}_\tau(m') = w\mathrm{LT}_\tau(g)w' \equiv \overline{w}\cdot\varphi(\mathrm{LT}_\tau(g))\cdot\overline{w}' \equiv \overline{w} \cdot \mathrm{LT}_\tau(\varphi(g)) \cdot \overline{w}'$. Demnach erfüllt das Element $\varphi(g) \in \varphi(\widehat{G})$ die gewünschte Eigenschaft und die Behauptung ist bewiesen. □

Bemerkung 4.2.4 In diesem Kapitel ist vorausgesetzt, dass die Elemente $f_1, \ldots, f_t$ eine σ-Gröbnerbasis des zweiseitigen Ideals I bilden. Dies kann durch die Bedingung ersetzt werden, dass sich die Menge $\{f_1, \ldots, f_t\}$ zu einer endlichen σ-Gröbnerbasis von I ergänzen lässt. Denn ist $\{f_1, \ldots, f_{t+u}\}$ eine solche σ-Gröbnerbasis, so gilt für jede Syzygie $m = \sum_{i=1}^{s+t}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\varepsilon_iw'_{ij}$ in $\mathrm{Syz}(g_1, \ldots, g_s, f_1, \ldots, f_t)$ auch $m \in \mathrm{Syz}(g_1, \ldots, g_s, f_1, \ldots, f_{t+u})$.

4.3 Das Konjugationssuchproblem

In diesem Abschnitt befassen wir uns mit dem Konjugationssuchproblem in Monoidringen. Dazu sei Σ ein endliches Alphabet und $\sim_W$ eine Äquiva-

lenzrelation auf der Menge der Wörter Σ^* erzeugt durch endlich viele Relationen $w_1 \sim w_1', \ldots, w_t \sim w_t'$. Wir nehmen hierbei an, dass eine Termordnung σ auf Σ^* existiert, so dass $w_i >_\sigma w_i'$ für $i = 1, \ldots, t$ erfüllt ist. Weiter sei vorausgesetzt, dass das von $w_i \xrightarrow{W} w_i'$ erzeugte Termersetzungssytem $\xrightarrow{W}$ konvergent ist und jedes Element in $\mathcal{M} = \Sigma^*/\sim_W$ durch sein zugehöriges irreduzibles Wort in Σ^* bzgl. $\xrightarrow{W}$ präsentiert wird. Für Elemente $w, w' \in \mathcal{M}$ bezeichne ww' wieder das Produkt von w und w' in $\mathcal{M}$ und $w \cdot w'$ die Konkatenation in Σ^*, sowie $\equiv$ die Identität als Wort. Für das endlich präsentierte Monoid $\mathcal{M}$ erhalten wir mit

$$K[\mathcal{M}] = \{\sum_{i=1}^{k} c_i v_i \,|\, k \in \mathbb{N}_0,\, c_i \in K\backslash\{0\},\, v_i \in M \text{ für } i = 1, \ldots, k\}$$

den **Monoidring** von $\mathcal{M}$ über K.

Das Konjugationssuchproblem lässt sich nun wie folgt formulieren. Entscheide, ob zu Elementen $g_1, g_2 \in K[\mathcal{M}]$ ein $f \in K[\mathcal{M}]$ existiert, so dass $g_2 = f g_1 f^{-1}$ gilt. Diese Gleichung lässt sich auch umstellen zu $fg_1 - g_2 f = 0$. Wir suchen also eine Syzygie des Tupels (g_1, g_2) mit einer speziellen Gestalt. Den verbleibenden Teil dieser Arbeit wollen wir nun der Berechnung des Syzygienmoduls von (g_1, g_2) bzw. allgemeiner von $(g_1, \ldots, g_s)$ widmen.

Im Folgenden sei also $\widetilde{G} = \{g_1, \ldots, g_s\} \subseteq K[\mathcal{M}]$ und $\widetilde{\mathcal{G}} = (g_1, \ldots, g_s)$. Ferner sei $\widetilde{E}$ der freie von $\{\varepsilon_1, \ldots, \varepsilon_s\}$ zweiseitig erzeugte $K[\mathcal{M}]$-Modul.

Definition 4.3.1 *Sei $m \in \widetilde{E}$, d.h. $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w_{ij}'$ mit $c_{ij} \in K$, $w_{ij}, w_{ij}' \in \mathcal{M}$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Das Element m heißt* **(zweiseitige) Syzygie** *von $\widetilde{\mathcal{G}}$, falls die Gleichung*

$$\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w_{ij}' = 0$$

erfüllt ist.

Die Menge aller Syzygien $\mathrm{Syz}(\widetilde{\mathcal{G}})$ bilden wieder einen zweiseitigen $K[\mathcal{M}]$-Untermodul von $\widetilde{E}$. Diesen haben wir bereits im ersten Abschnitt dieses Kapitels für Elemente $g_1, \ldots, g_s \in R = K[\Sigma^*]/I$ bestimmt. Die dort gewonnenen Ergebnisse können wir nun auf Monoidringe übertragen. Dabei sei $I_{\mathcal{M}}$ das zweiseitige Ideal von $K[\Sigma^*]$ erzeugt von $G_{\mathcal{M}} = \{w_1 - w_1', \ldots, w_t - w_t'\}$ und für ein $w \in \Sigma^*$ bezeichne $\overline{w}$ wieder die zugehörige Äquivalenzklasse in $\mathcal{M}$ bzgl. $\sim_W$. Da $\xrightarrow{W}$ als konvergent vorausgesetzt ist, ist dabei $G_{\mathcal{M}}$ bereits eine σ-Gröbnerbasis von $I_{\mathcal{M}}$. Wir erhalten zunächst das folgende Resultat. Dabei sei $\varphi : K[\Sigma^*] \longrightarrow K[\mathcal{M}]$ der von $\Sigma^* \longrightarrow \mathcal{M}$, $w \mapsto \overline{w}$ induzierte Homomorphismus (siehe [2], Kapitel 3 § 2.6, Korollar zu Proposition 6).

Satz 4.3.2 *Ist $\mathcal{M}$ ein endlich präsentiertes Monoid, dann induziert die Abbildung $\varphi : K[\Sigma^*] \longrightarrow K[\mathcal{M}]$ mit $\sum_{i=1}^{k} c_i v_i \mapsto \sum_{i=1}^{k} c_i \overline{v}_i$ einen Isomorphismus $\widetilde{\varphi}$ von $K[\Sigma^*]/I_{\mathcal{M}}$ nach $K[\mathcal{M}]$.*

Beweis. Die Abbildung φ ist offensichtlich ein surjektiver Homomorphismus. Zu zeigen ist nun, dass der Kern von φ dem zweiseitigen Ideal $I_{\mathcal{M}}$ entspricht.

Sei zunächst $f \in I_{\mathcal{M}} \backslash \{0\}$, d.h. $f = \sum_{i=1}^{t} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} (w_i - w_i') w_{ij}'$ mit $c_{ij} \in K$, $w_{ij}, w_{ij}' \in \Sigma^*$ für $i = 1, \ldots, t$ und $j \in \mathbb{N}$, wobei nur endlich viele der c_{ij} von Null verschieden sind. Dann ist

$$\varphi(f) = \sum_{i_1}^{t} \sum_{j \in \mathbb{N}} c_{ij} \overline{w}_{ij} (\overline{w}_i - \overline{w}_i') \overline{w}_{ij}' = \overline{0}.$$

Sei nun umgekehrt $f = \sum_{i=1}^{k} c_i v_i \in \mathrm{Kern}(\varphi) \backslash \{0\}$ mit $c_i \in K \backslash \{0\}$, $v_i \in \Sigma^*$ für $i = 1, \ldots, k$ und $\varphi(f) = \overline{0}$. Es ist also $\sum_{i=1}^{k} c_i \overline{v}_i = \overline{0}$. Ist $k = 1$, so folgt aus $c_1 \overline{v}_1 = \overline{0}$ sofort $c_1 = 0$ und daraus $0 = f \in I_{\mathcal{M}}$. Für $k \geq 2$ ergibt sich $-c_k \overline{v}_k = \sum_{i=1}^{k-1} c_i \overline{v}_i$ und damit $\overline{v}_k = \overline{v}_j$ für ein $j \in \{1, \ldots, k-1\}$. Wir erhalten also $v_k - v_j \in I_{\mathcal{M}}$. Für das Element $f' = \sum_{i=1}^{k-1} c_i' v_i \in K[\Sigma^*]$ mit $c_i' = c_i$ für $i \neq j$ und $c_j' = c_j + c_k$ gilt $\varphi(f') = \varphi(f) = \overline{0}$ und $f = f' + c_k(v_k - v_j)$. Die Behauptung folgt nun induktiv. □

In Anlehnung an Satz 4.1.5 definieren wir eine Gröbnerbasis von einem zweiseitigen $K[\mathcal{M}]$-Untermodul von $\widetilde{E}$ wie folgt. Dabei sei τ wieder eine mit σ verträgliche Modultermordnung auf $\mathbb{T}(E)$.

Definition 4.3.3 *Sei $\widetilde{M}$ ein zweiseitiger $K[\mathcal{M}]$-Untermodul von $\widetilde{E}$. Eine Menge $\widetilde{G} \subseteq \widetilde{M}$ heißt* **(zweiseitige) Gröbnerbasis** *von $\widetilde{M}$, falls gilt*

$$\mathrm{LT}_\tau\{\widetilde{M}\} = \{w \cdot \mathrm{LT}_\tau(g) \cdot w' \mid g \in \widetilde{G}, w, w' \in \mathcal{M}\}.$$

Sei nun die Abbildung ϕ definiert als $\phi : \overline{E} \longrightarrow \widetilde{E}$ mit $\phi = \bigoplus_{i=1}^{s} \widetilde{\varphi} \otimes_K \widetilde{\varphi}$. Wir erhalten so mit ϕ als direkte Summe von Homomorphismen $\widetilde{\varphi} \otimes_K \widetilde{\varphi}$ wieder einen Homomrphismus zweiseitiger Moduln.

Satz 4.3.4 *Sei $\widetilde{G} = \{g_1, \ldots, g_s\} \subseteq K[\mathcal{M}]$ und $\widetilde{\mathcal{G}} = (g_1, \ldots, g_s)$. Dann gilt:*

a) $\mathrm{LT}_\tau(\phi(m)) = \phi(\mathrm{LT}_\tau(m))$ *für alle $m \in \overline{E}$.*

b) Ist $\overline{G}$ eine Gröbnerbasis von $\mathrm{Syz}(\overline{\mathcal{G}})$ *mit $\overline{\mathcal{G}} = (\widetilde{\varphi}^{-1}(g_1), \ldots, \widetilde{\varphi}^{-1}(g_s))$, dann ist $\phi(\overline{G})$ eine Gröbnerbasis von* $\mathrm{Syz}(\widetilde{\mathcal{G}})$.

Beweis. Für den Beweis von a) sei $m \in \overline{E}$ und $t \in \mathrm{Supp}(m)$, d.h. $t = w\varepsilon_i w'$ mit $w, w' \in \mathbb{T}(R)$ und $i \in \{1, \ldots, s\}$. Dann werden w und $\varphi(w)$ bzw. w' und

$\varphi(w')$ durch dasselbe irreduzible Element in Σ^* repräsentiert. Denn wäre dieses Element reduzibel bzgl. $\xrightarrow{W}$, so enthielte es ein w_j für ein $j \in \{1, \ldots, t\}$. Damit wäre es aber auch ein Vielfaches von $\mathrm{LT}_\sigma(w_j - w'_j)$ und reduzibel bzgl. $\xrightarrow{G_\mathcal{M}}$. Dies gilt nun insbesondere für $t = \mathrm{LT}_\tau(m)$. Damit erhalten wir a).

Es bleibt noch b) zu zeigen. Sei dazu $\overline{\mathcal{G}} = (\widetilde{\varphi}^{-1}(g_1), \ldots, \widetilde{\varphi}^{-1}(g_s))$ und $\overline{G}$ eine Gröbnerbasis von $\mathrm{Syz}(\overline{\mathcal{G}})$. Des Weiteren sei $m = \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \varepsilon_i w'_{ij} \in \mathrm{Syz}(\widetilde{\mathcal{G}}) \backslash \{0\}$ mit $c_{ij} \in K$, $w_{ij}, w'_{ij} \in \mathcal{M}$ für $i = 1, \ldots, s$ und $j \in \mathbb{N}$, wobei nur endlich viele c_{ij} von Null verschieden sind. Also ergibt sich

$$\begin{aligned} & \sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} \widetilde{\varphi}^{-1}(w_{ij}) \widetilde{\varphi}^{-1}(g_i) \widetilde{\varphi}^{-1}(w'_{ij}) \\ = \;& \widetilde{\varphi}^{-1}\Big(\sum_{i=1}^{s} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} g_i w'_{ij}\Big) \\ = \;& \widetilde{\varphi}^{-1}(0) \;=\; 0 \end{aligned}$$

und damit $\phi^{-1}(m) \in \mathrm{Syz}(\overline{\mathcal{G}})$. Es existieren nun Elemente $w, w' \in \mathbb{T}(R)$ und $g \in \overline{G}$, so dass gilt $\phi^{-1}(m) \equiv w \cdot \mathrm{LT}_\tau(g) \cdot w'$. Mit a) folgt schließlich $m \equiv \phi(w \cdot \mathrm{LT}_\tau(g) \cdot w') = \varphi(w) \cdot \phi(\mathrm{LT}_\tau(g)) \cdot \varphi(w') = \varphi(w) \cdot \mathrm{LT}_\tau(\phi(g)) \cdot \varphi(w')$ und die Behauptung ist bewiesen. □

Bemerkung 4.3.5 Analog zu Bemerkung 4.2.4 gilt auch hier, dass das Termersetzungssystem $\xrightarrow{W}$ nicht konvergent sein muss. Es genügt die Voraussetzung, dass es durch Hinzunahme endlich vieler Relationen zu einem konvergenten Termersetzungssystem erweitert werden kann.

Beispiel 4.3.6 Die symmetrische Gruppe S_3 wird endlich präsentiert durch $\Sigma = \{x_1, x_2\}$ und die Relationen $x_1^3 \sim 1$, $x_2^2 \sim 1$ und $x_1^2 x_2 \sim x_2 x_1$. Ist $g_1 = x_2$ und $f = x_1 x_2$, so erhalten wir mit $f g_1 f^{-1} = x_1 x_2 x_2 (x_1 x_2)^{-1} = x_1 x_2^{-1} x_1^{-1} = x_1 x_2 x_1^2 = x_2 x_1 = g_2$ ein Konjugat von g_1. Wir wollen nun die Syzygien für das Tupel $\widetilde{\mathcal{G}} = (g_1, g_2)$ berechnen und zeigen, dass $x_1 x_2 \varepsilon_1 - \varepsilon_2 x_1 x_2$ in $\mathrm{Syz}(\widetilde{\mathcal{G}})$ liegt. Nach Satz 4.3.2 müssen wir dazu den Polynomring $K[\Sigma^*]$ mit $\Sigma = \{x_1, x_2\}$ und das zweiseitige von $\{x_1^3 - 1, x_2^2 - 1, x_1^2 x_2 - x_2 x_1\}$ erzeugte Ideal $I_\mathcal{M}$ von $K[\Sigma^*]$ betrachten. Wir wählen dabei die Modultermordnung $\tau = \texttt{PosLLex}$ auf $\mathbb{T}(E)$, wobei E der freie von $\{\varepsilon_1, \varepsilon_2\}$ erzeugte zweiseitige $K[\Sigma^*]$-Modul ist. Wir müssen die Menge der Erzeugenden von $I_\mathcal{M}$ zunächst zu einer LLex-Gröbnerbasis ergänzen. Nach Beispiel 2.6.7 b) erfüllen dies die Elemente $x_1 x_2 x_1 - x_2, x_2 x_1^2 - x_1 x_2$ und $x_2 x_1 x_2 - x_1^2$. Zur Berechnung von $\mathrm{Syz}(\overline{\mathcal{G}})$ gehen wir nun nach Satz 4.2.3 vor. Der zweiseitige Untermodul U von $\langle e_1, e_2, e_3 \rangle_{K[\Sigma^*]}$ wird hierbei erzeugt von $\overline{G} = \{f_1, \ldots, f_{10}\}$ mit

$$
\begin{aligned}
f_1 &= e_1x_2 - e_2, & f_6 &= e_1x_1x_2x_1 - e_1x_2,\\
f_2 &= e_1x_2x_1 - e_3, & f_7 &= e_1x_2x_1^2 - e_1x_1x_2,\\
f_3 &= e_1x_1^3 - e_1, & f_8 &= e_1x_2x_1x_2 - e_1x_1^2,\\
f_4 &= e_1x_2^2 - e_1, & f_9 &= x_1e_1 - e_1x_1,\\
f_5 &= e_1x_1^2x_2 - e_1x_2x_1, & f_{10} &= x_2e_1 - e_1x_2.
\end{aligned}
$$

Wir berechnen nun Elemente einer `PosLLex`-Gröbnerbasis von U. Wir erhalten dabei die folgenden S-Vektoren:

$$
\begin{aligned}
S_{1,2} &= f_1x_1 - f_2 = -e_2x_1 + e_3 =: f_{11}\\
S_{1,4} &= f_1x_2 - f_4 = e_1 - e_2x_2 =: f_{12}\\
S_{1,12} &= f_1 - f_{12}x_2 = e_2x_2^2 - e_2 =: f_{13}\\
S_{10,12} &= f_{10} - x_2f_{12} = -e_1x_2 + x_2e_2x_2 \xrightarrow{f_{12}} x_2e_2x_2 - e_2x_2^2\\
&\xrightarrow{f_{13}} x_2e_2x_2 - e_2 =: f_{14}\\
S_{9,12} &= f_9 - x_1f_{12} = -e_1x_1 + x_1e_2x_2 \xrightarrow{f_{12}} x_1e_2x_2 - e_2x_2x_1 =: f_{15}\\
S_{7,12} &= f_7 - f_{12}x_2x_1^2 = -e_1x_1x_2 + e_2x_2^2x_1^2 \xrightarrow{f_{12}} e_2x_2^2x_1^2 - e_2x_2x_1x_2\\
&\xrightarrow{f_{13}} e_2x_1^2 - e_2x_2x_1x_2 \xrightarrow{f_{11}} -e_2x_2x_1x_2 + e_3x_1 =: f_{17}\\
S_{13,14} &= x_2f_{13} - f_{14}x_2 = -x_2e_2 + e_2x_2 =: f_{18}\\
S_{13,15} &= x_1f_{13} - f_{15}x_2 = -x_1e_2 + e_2x_2x_1x_2 \xrightarrow{f_{17}} -x_1e_2 + e_3x_1 =: f_{19}
\end{aligned}
$$

Es ergibt sich also das Element $f = -x_1f_{18} - f_{19}x_2 = x_1x_2e_2 - e_3x_1x_2 \in \overline{G}$ und damit $\phi(f) = x_1x_2\varepsilon_1 - \varepsilon_2x_1x_2 \in \phi(\overline{G})$.

Kapitel 5

Ausblick

Wir haben in den vorangegangenen Kapiteln grundlegende Aussagen über Syzygien von Tupeln aus Elementen eines zweiseitigen freien Moduls F über einem nicht-kommutativen Polynomring $K[\Sigma^*]$ erarbeitet. Der Schwerpunkt lag dabei auf der Entwicklung einfacher Algorithmen zur Berechnung solcher Syzygien. Dazu war unter anderem ein intensives Studium der Gröbnerbasen für zweiseitige Untermoduln von zweiseitigen freien $K[\Sigma^*]$-Moduln nötig. Das Aufstellen effizienterer Algorithmen sollte ein erster Punkt in weiteren Betrachtungen darstellen. Der Blick auf Rechenzeiten und -resourcen ist hier zugunsten der Erarbeitung der theoretischen Grundlagen vernachlässigt worden. Hierbei wäre auch zu untersuchen, in wie weit sich die Ergebnisse aus der kommutativen Theorie zu diesem Thema übertragen lassen.

Ein weiterer Punkt in tiefer gehenden Betrachtungen könnte die in Kapitel 4 angesprochene Anwendung auf das Konjugationssuchproblem über Monoidringen $K[\mathcal{M}]$ einnehmen. Hierbei stellt sich unter anderem die Frage, wie dieses Thema für nicht endlich präsentierte Monoide $\mathcal{M}$ angegangen werden kann. Auch das Fehlen der hier vorausgesetzten Konvergenz des durch die Relationen erzeugten Termersetzungssystems könnte Teil neuer Untersuchungen sein. Dies entspricht der Situation, dass die den Relationen entsprechenden Polynome zu keiner endlichen Gröbnerbasis des von ihnen erzeugten Ideals ergänzt werden können.

Im letzten Kapitel wurde im Zusammenhang mit dem Konjugationssuchproblem diskutiert, wie der Syzygienmodul für ein Tupel (g_1, g_2) von Elementen aus einem zweiseitigen freien Modul über $K[\mathcal{M}]$ bestimmt werden kann. Doch in diesem Kontext wurde eine wichtige Frage in dieser Arbeit nicht beantwortet. Wie finden wir in der Menge aller Syzygien genau diejenige der Form $f\varepsilon_1 - \varepsilon_2 f$ heraus, die das Problem löst. Wir haben bisher nur mögliche „Kandidaten“ hierfür bestimmt.

Literaturverzeichnis

[1] P. Ackermann, M. Kreuzer, *Gröbner Basis Cryptosystems*. Appl. Alg. in Eng., Comm. and Comp., Springer, 2005 (erscheint).

[2] N. Bourbaki, *Elements of Mathematics Algebra 1*. Addison Wesley, 1974.

[3] E. Green, *Multiplicative Bases, Gröbner Bases, and Right Gröbner Bases*. Journal Symbolic Computation **29** (2000), S. 601-623.

[4] D. Knuth, P. Bendix, *Simple Word Problems in Universal Algebras*. J. Leech (editor), Computational Problems in Abstract Algebra, S. 263-297, Pergamon Press, 1970.

[5] M. Kreuzer, L. Robbiano, *Computational Commutative Algebra 1*. Springer, 2000.

[6] K. Madlener, B. Reinert, *Computing Gröbner Bases in Monoid and Group Rings*. In: M. Bronstein (ed.), Proc. Conf. ISSAC 1993, ACM Press, New York, 1993, S. 254-263.

[7] B. Reinert, *On Gröbner Bases in Monoid and Group Rings*. Dissertation, Universität Kaiserslautern, 1995.

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen verfasst habe.

Dortmund, den 02. Mai 2005