Algebraische Potenzreihen

DIPLOMARBEIT

AUS DEM FACH MATHEMATIK ZUR ERLANGUNG DES
AKADEMISCHEN GRADES EINES DIPLOMINGENIEURS

EINGEREICHT BEI
HERWIG HAUSER
AM INSTITUT FÜR MATHEMATIK AN DER
LEOPOLD-FRANZENS-UNIVERSITÄT INNSBRUCK
IM OKTOBER 2005 VON

Dominique Wagner

Inhaltsverzeichnis

Vorwort

In dieser Arbeit wird ein endlicher Algorithmus für die Division eines algebraischen Potenzreihevektors f durch einen Modul $I \subseteq K[\![x]\!]$, der von algebraischen Potenzreihenvektoren erzeugt wird und Hironaka's Box-Bedingung erfüllt, entwickelt.

Die dafür benötigten Methoden - Normalisierung, Standardbasen und Babylonische Division - werden im ersten Kapitel beschrieben.
Das zweite Kapitel beschäftigt sich mit allgemeinen Eigenschaften von algebraischen Potenzreihen.
Um konstruktiv mit algebraischen Potenzreihen arbeiten zu können, führen wir in Kapitel drei den Begriff eines Codes ein. Wir werden sehen, dass für jede algebraische Potenzreihe g ein sie eindeutig beschreibender Code $(H, G) \in K[x, y]^p \times K[x, y]$ existiert. Weiters werden wir für konkrete algebraische Potenzreihen solche Codes berechnen.
Das vierte Kapitel wird das Rechnen mit Codes von algebraischen Potenzreihen erörtern.
In Kapitel fünf beweisen wir einige wichtige Lemmata, die den Zusammenhang zwischen Moduln von algebraischen Potenzreihenvektoren und deren Codes beschreiben.
Das sechste Kapitel befasst sich mit der Konstruktion eines Codes einer minimalen Standardbasis eines Moduls, der von algebraischen Potenzreihenvektoren erzeugt wird. Dies wird dann an einigen expliziten Beispielen demonstriert.
Das Ziel von Kapitel sieben ist die Beschreibung eines endlichen Algorithmus für die Division eines algebraischen Potenzreihenvektors durch einen Modul, der von algebraischen Potenzreihenvektoren erzeugt wird und Hironaka's Box-Bedingung erfüllt. Dazu wird zuerst ein Algorithmus zur Konstruktion einer reduzierten Standardbasis derartiger Modulen beschrieben. Die Konstruktion einer reduzierten Standardbasis und die effektive Division werden dabei zuerst für x_n-reguläre Moduln bewiesen, dann wird der Fall eines allgemeinen Moduls mittels Induktion auf den x_n-regulären Fall zurückgeführt. Weiters werden in diesem Kapitel einige Beispiele zu diesen Algorithmen gerechnet.

An dieser Stelle möchte ich mich bei meiner Familie für die moralische und finanzielle Unterstützung während meines gesamten Studiums und Prof. Herwig Hauser für die gute Betreuung bei meiner Diplomarbeit bedanken. Weiters ein recht herzliches Dankeschön an Thomas Bruschek für das Korrekturlesen dieser Arbeit, an meinem Freund Clemens für die immerwährende moralische Unterstützung und an meine Mitstudenten Romana und Florian für die vielen netten Stunden während unserer Studentenzeit.

Innsbruck, Oktober 2005

Dominique Wagner

1 Vorbereitungen

1.1 Notationen

In den Kapiteln 3 bis 7 seien die Buchstaben n, p, r und s für fixierte Zahlen in $\mathbb{N}$ reserviert. Die Buchstaben i, j, k und l werden immer zwischen $1 \leq i \leq p$, $1 \leq j \leq n$, $1 \leq k \leq r$ und $1 \leq l \leq s$ variieren. Weiters werden in Kapitel 7 die Buchstaben l' und l'' zwischen $1 \leq l' \leq r$ und $r+1 \leq l'' s$ variieren.

Weiters sei $\{x_1, \ldots, x_n\}$ eine Menge von Variablen, wobei wir gelegentlich x als Abkürzung für $(x_1, \ldots, x_n)$ verwenden. Mit $K[x]$, $K[\![x]\!]$ und $K\{x\}$ bezeichnen wir den Polynomring, den (formalen) Potenzreihenring bzw. den Ring der konvergenten Potenzreihen in den n Variablen $x_1, \ldots, x_n$ über einem Körper K der Charakteristik 0. Elemente in $K[x]^s$ und $K[\![x]\!]^s$ werden wir *Polynome-* bzw. *(formale) Potenzreihenvektoren* nennen. Dabei stehen Großbuchstaben stets für Polynome und Kleinbuchstaben für Potenzreihen.
Weiters setzen wir $x' = (x_1, \ldots, x_{n-1})$ und bezeichnen mit $y = (y_1, \ldots, y_p)$ zusätzliche Variablen.

Vektoren $g \in K[\![x]\!]^s$ werden wir als

$$g = \sum_{\alpha, l} c_{\alpha l} x^\alpha e_l$$

entwickeln, wobei $c_{\alpha l} \in K$ und $e_l = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{N}^s$ die kanonische $K[\![x]\!]$-Basis von $K[\![x]\!]^s$ sind. Als *Träger* von g bezeichnen wir die Menge

$$\operatorname{supp}(g) = \{(\alpha, l) \in \mathbb{N}^n \times \{1, \ldots, s\}; c_{\alpha l} \neq 0\}.$$

Wir sagen, ein Vektor $g \in K[\![x]\!]^s$ ist durch einen Vektor h in $K[\![x]\!]^s$ teilbar, falls es eine Potenzreihe $a \in K[\![x]\!]$ mit $g = ah$ gibt.

Vektoren der Form $x^\alpha e_l$ nennen wir *Monomvektoren*. Ein *monomialer Untermodul* von $K[\![x]\!]^s$ ist ein Untermodul M von $K[\![x]\!]^s$, der von Monomvektoren erzeugt wird. Er ist also ein kartesisches Produkt $M = \prod_{l=1}^s M_l$ von Monomidealen M_l in $K[\![x]\!]$. Die Elemente von M sind gerade jene Potenzreihenvektoren mit Träger in $\Gamma = \{(\alpha, l) \in \mathbb{N}^n \times \{1, \ldots, s\}; x^\alpha e_l \in M\}$. Das *kanonische direkte monomiale Komplement* von M in $K[\![x]\!]^s$ ist der Untervektorraum $\operatorname{co}(M)$ von $K[\![x]\!]^s$ der Potenzreihenvektoren mit Träger in $\Gamma' = (\mathbb{N}^n \times \{1, \ldots, s\}) \setminus \Gamma$. Klarerweise gilt: $M \oplus \operatorname{co}(M) = K[\![x]\!]^s$.

Mit $\langle g_1, \ldots, g_r \rangle$ bezeichnen wir jenen Untermodul von $K[\![x]\!]^s$, der von den Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ erzeugt wird. Manchmal werden wir ihn auch mit $\langle g_k \rangle$ abkürzen (falls der Bereich, in dem k variiert, aus dem Kontext heraus klar ist).

Ein formale Potenzreihe $h \in K[\![x]\!]^s$ heißt eine *algebraische Potenzreihe*, wenn sie eine polynomiale Relation $P(x, h(x)) = 0$ erfüllt, wobei P ein von 0 verschiedenes Polynom in $K[x_1, \ldots, x_n, t]$ in $n+1$ Variablen ist, d.h.

$$P(x, h(x)) = p_0 h^d + \ldots + p_{d-1} h + p_d = 0$$

mit Polynomen $p_i = p_i(x) \in K[x]$. Ein *algebraischer Potenzreihenvektor* ist ein Vektor in $K[\![x]\!]^s$, dessen Komponenten alle algebraische Potenzreihen sind.
Für Details über algebraische Potenzreihen siehe Kapitel 2.

1.2 Normalisierung

Wie wir in Kapitel 3 sehen werden, benötigen wir die Normalisierung, um einen Code einer algebraischen Potenzreihe zu konstruieren.

1.2.1 Algebraische Seite der Normalisierung

Definition 1.1. Seien R ein kommutativer Ring mit Einselement 1_R und S eine multiplikativ abgeschlossene Menge. Dann definieren wir den *Ring der Brüche* R_S, der manchmal auch mit $S^{-1}R$ bezeichnet wird, als

$$R_S = \left\{ \frac{r}{s}; r \in R, s \in S \right\}.$$

Wählt man speziell S als die Menge aller Nicht-Nullteiler von R, so nennt man den resultierenden Ring R_S den *totalen Quotientenring* (oder *totalen Ring der Brüche*) von R und bezeichnet ihn mit Quot(R).

Definition 1.2. Seien $R \subseteq S$ kommutative Ringe mit $1_R = 1_S$.

- Ein Element $a \in S$ heißt *ganz über* R, wenn es eine algebraische Gleichung der Form
$$a^n + c_1 a^{n-1} + \ldots + c_{n-1}a + c_n = 0 \quad (*)$$
erfüllt, wobei $c_i \in R$. Die Gleichung $(*)$ nennt man dann eine *Ganzheitsgleichung*.
- S heißt *ganz über* R oder eine *ganze Erweiterung von* R, wenn jedes Element $b \in S$ ganz über R ist.
- R heißt *ganz abgeschlossen in* S, wenn jedes Element von S, das ganz über R ist, bereits in R liegt.
- R heißt *ganz abgeschlossen*, wenn R in Quot(R) - dem totalen Quotientenring von R - ganz abgeschlossen ist.
- R heißt *normal*, wenn R ein reduzierter (d.h., R besitzt keine nilpotenten Elemente) und ganz abgeschlossener Ring ist.

Bemerkung. In einem Körper sind algebraische Elemente auch ganze Elemente (und umgekehrt), denn dort macht die Normierung der Ganzheitsgleichung keine Probleme.

Lemma 1.1. *Seien $R \subseteq S$ eine Ringerweiterung und $a \in S$. Dann gilt:*

$$a \text{ ist ganz über } R \iff R[a] \text{ ist ein endlich erzeugter } R\text{-Modul.}$$

Speziell ist jede endliche Erweiterung $R \subseteq S$ eine ganze Erweiterung.

Beweis. Sei $a \in S$ ganz über R. Dann existiert eine algebraische Gleichung $P(a) = 0$, wobei $P \in R[X]$ ein normiertes Polynom vom Grad n ist. Sei weiters $G(a) \in R[a]$ für ein Polynom $G \in R[X]$. Division mit Rest von G durch P liefert $G = QP + R'$ mit $\deg(R') < n$. Wertet man diese Gleichung in a aus, so ergibt sich $G(a) = R'(a)$. Dies zeigt, dass $R[a]$ als R-Modul von den Elementen $1, a, \ldots, a^{n-1}$ erzeugt wird.
Umgekehrt: Seien $q_1, \ldots, q_t$ endlich viele Erzeuger von $R[a]$ als R-Modul. Dann sind die q_i Polynome vom Grad d_i in a. Setzt man nun $n-1$ gleich dem Maximum der d_i, so folgt, dass das Element $a^n \in R[a]$ eine R-Linearkombination der q_i ist. Damit erhält man eine Ganzheitsgleichung für a. □

Folgerung 1.2. *Sei $R \subseteq S$ eine Ringerweiterung und seien $a_1, \ldots, a_k \in S$ ganz über R. Dann ist der Ring $R[a_1, \ldots, a_k]$ ein endlich erzeugter R-Modul.*

Beweis. Verwendet das letzte Lemma und Induktion über k. □

Lemma 1.3. *Seien $R \subseteq S \subseteq T$ Ringerweiterungen. Ist $a \in T$ ganz über S und S ganz über R, so ist a auch ganz über R.*
Speziell gilt: Seien $R \subseteq S$ und $S \subseteq T$ ganze Ringerweiterungen. Dann ist auch $R \subseteq T$ eine ganze Ringerweiterung.

Beweis. Sei $a \in T$ ganz über S. Dann existiert eine Ganzheitsgleichung der Form

$$a^n + c_1 a^{n-1} + \ldots + c_{n-1} a + c_n = 0,$$

wobei $c_i \in S$. Nach dem letzten Lemma ist der Ring $S' := R[c_1, \ldots, c_n]$ ein endlich erzeugter R-Modul. Weiters ist $S'[a]$ ein endlich erzeugter S'-Modul, denn a ist ganz über S'. Folglich ist $S'[a]$ ein endlich erzeugter R-Modul und damit ist a ganz über R. Die Zusatzfolgerung ist klar. □

Definition 1.3. Sei $R \subseteq S$ eine Ringerweiterung. Der *ganze Abschluss $\overline{R}_S$ von R in S* ist die Menge aller Elemente von S, die ganz über R sind.
Ist $S = \text{Quot}(R)$, so bezeichnen wir den ganzen Abschluss von R mit $\overline{R}$. Der wichtigste Fall ist jener, bei dem R ein Integritätsbereich und $S = \text{Quot}(R)$ sein Quotientenkörper ist.
Ist R ein reduzierter Ring, so nennt man $\overline{R}$ die *Normalisierung von R*. Wir werden sie im Folgenden mit $\tilde{R}$ bezeichnen.

Beispiel 1.1. (Spitze) Wir betrachten den Ring

$$R := \mathbb{C}[x, y]/\langle y^2 - x^3 \rangle.$$

Wie wir schon gesehen haben, ist R kein normaler Ring, denn für

$$t := \frac{y}{x} \in \text{Quot}(R)$$

gilt $t^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x$. Damit ist t ganz über R und erfüllt die Ganzheitsgleichung

$$X^2 - x = 0.$$

Tatsächlich ergibt sich für die Normalisierung von R:

$$\tilde{R} = \mathbb{C}[x, y, t]/\langle y^2 - x^3, x - t^2, y - t^3 \rangle \cong \mathbb{C}[t].$$

Um zu zeigen, dass t kein Element von R ist, betrachten wir die folgende Abbildung:

$$\phi : \mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]; x \to t^2, y \to t^3.$$

Man sieht leicht, dass $y^2 - x^3$ im Kern von ϕ enthalten ist. Es gilt sogar

$$\text{Ker}(\phi) = \langle x^2 - y^3 \rangle.$$

Denn: Sei $P \in \text{Ker}(\phi)$. Dann können wir P folgendermaßen schreiben:

$$P = Q(y^2 - x^3) + r_0 + r_1 \cdot y,$$

wobei $r_i \in \mathbb{C}[x]$. Damit ist $0 = \phi(P) = P(t^2, t^3) = r_0(t^2) + r_1(t^2) \cdot t^3$. Der Term $r_0(t^2)$ besteht nur aus geraden t-Potenzen, hingegen besteht der Term $r_1(t^2)t^3$ nur aus ungeraden t-Potenzen. Daraus folgt, dass $r_0 = r_1 = 0$ gelten muss. Daher folgt mittels des Homomorphiesatzes für Ringe

$$R = \mathbb{C}[x, y]/\langle x^2 - y^3 \rangle \cong \mathbb{C}[t^2, t^3],$$

und somit ist $t = \frac{x}{y}$ klarerweise kein Element von R.

Beispiel 1.2. (Schleife) Wir betrachten den Ring

$$R := \mathbb{C}[x, y]/\langle y^2 - x^3 - x^2 \rangle.$$

Wiederum ist

$$t := \frac{y}{x} \in \text{Quot}(R)$$

ganz über R , denn t erfüllt die Ganzheitsgleichung

$$X^2 - x - 1 = 0.$$

Der Ring R besitzt die Normalisierung

$$\tilde{R} = \mathbb{C}[x, y, t]/\langle y^2 - x^3 - x^2, x + 1 - t^2, y + t - t^3 \rangle \cong \mathbb{C}[t].$$

Um zu zeigen, dass t tatsächlich kein Element von R ist, gehen wir wie im letzten Beispiel vor und erhalten

$$R = \mathbb{C}[x, y]/\langle y^2 - x^3 - x^2 \rangle \cong \mathbb{C}[t^2 - 1, t^3 - t],$$

woraus sofort $t \notin R$ folgt.

Beispiel 1.3. (Achsenkreuz) Wir betrachten folgenden Ring:

$$R := \mathbb{C}[x, y]/\langle x \cdot y \rangle.$$

Dieser Ring ist nicht normal.
Denn: Betrachte

$$u := \frac{x}{x + y} \in \text{Quot}(R).$$

Dann gilt

$$u^2 = u,$$

denn in R gilt $x^2(x + y) = x^3 = x(x + y)^2$. Weiters kann leicht nachgeprüft werden, dass u kein Element von R ist.

Beispiel 1.4. In diesem Beispiel betrachten wir den Ring

$$R := \mathbb{C}[x]/\langle x^2 \rangle.$$

Für diesen Ring gilt

$$\text{Quot}(R) = R.$$

Denn: Für Elemente in

$$\text{Quot}(R) = \left\{ \frac{a + bx}{c + dx}; a, b, c, d \in \mathbb{C}, c \neq 0 \right\}$$

(wäre $c = 0$, so wäre $c + dx$ ein Nullteiler in R) gilt

$$\frac{a+bx}{c+dx} = \frac{(a+bx)(c-dx)}{(c+dx)(c-dx)} = \frac{ac + x(bc-ad)}{c^2} \in R.$$

Damit ist R ganz abgeschlossen.
R ist jedoch nicht normal, denn R ist nicht reduziert (zum Beispiel ist x ein nilpotentes Element von R).

Lemma 1.4. *Seien $R \subseteq S$ Ringe. Dann ist der ganze Abschluss $\overline{R}_S$ von R in S ein Unterring von S, der R enthält. Weiters ist $\overline{R}_S$ ganz abgeschlossen in S. Speziell gilt also, dass die Normalisierung eines Ringes normal ist.*

Ich werde hier den Beweis nur für den Fall, dass R noethersch ist, anführen. Die Aussage gilt auch für nicht-noethersche Ringe, ist dann jedoch schwerer zu beweisen. Siehe etwa [dJP00].

Beweis. Sei also R ein noetherscher Ring. Es ist zu zeigen, dass für ganze Elemente a und b auch $a - b$ und ab ganz sind. Aber diese Elemente liegen im Ring $R[a, b]$, der nach Folgerung 1.2 ein endlich erzeugter R-Modul ist. Da wir R als noethersch angenommen haben, folgt daraus, dass $R[ab]$ und $R[a-b]$ endlich erzeugte R-Moduln sind. Daraus folgt mit Hilfe von Lemma 1.1, dass $a - b$ und ab ganz sind. Der Rest der Behauptung folgt aus Lemma 1.3. □

Beispiel 1.5. Jeder ZPE-Ring ist ganz abgeschlossen:
Sei $\frac{x}{y}$ $(x, y \in R)$ ganz über R. Weiters sei o.B.d.A. ggT$(x, y) = 1$. Dann existieren $c_i \in R$ mit

$$\left(\frac{x}{y}\right)^n + c_1\left(\frac{x}{y}\right)^{n-1} + \ldots + c_{n-1}\left(\frac{x}{y}\right) + c_n = 0.$$

Multipliziert man die Gleichung mit y^n, so ergibt sich

$$x^n = -y(c_1 x^{n-1} + \ldots + c_n y^{n-1}).$$

Folglich ist y ein Teiler von x^n. Da aber ggT$(x, y) = 1$ vorausgesetzt wurde, folgt $y \in R^*$ und somit $\frac{x}{y} \in R$.

Beispiel 1.6. Seien R ein ganz abgeschlossener Integritätsbereich und A eine multiplikativ abgeschlossene Menge von Nicht-Nullteilern in R. Dann ist der Quotiententring R_A ganz abgeschlossen:
Sei x ein Element des Quotientenkörpers von R_A, das ganz über R_A ist. Da endlich viele Elemente von R_A einen gemeinsamen Nenner $a \in A$ haben, existieren $c_i \in R$ mit

$$x^n + \frac{c_1}{a}x^{n-1} + \ldots + \frac{c_{n-1}}{a}x + \frac{c_n}{a} = 0.$$

Multipliziert man die Gleichung mit a^n, so erhält man

$$(ax)^n + c_1(ax)^{n-1} + \ldots + c_{n-1}a^{n-2}(ax) + c_0 a^{n-1} = 0.$$

Somit ist ax ganz über R. Da R ein ganz abgeschlossener Integritätsbereich ist, folgt daraus $ax \in R$. Setzt man nun $z := ax \in R$, so erhält man $x = \frac{z}{a} \in R_A$.

Lemma 1.5. *Sei R ein Integritätsbereich. Dann ist der ganze Abschluss $\overline{R}$ von R in* Quot(R) *ganz abgeschlossen.*

Beweis. Sei $x \in \text{Quot}(R)$ ganz über $\overline{R}$. Da $\overline{R}$ ganz über R ist, folgt, dass x ganz über R ist. Somit gilt: $x \in \overline{R}$. □

Lemma 1.6. (Normalisierungslemma) *Sei $R = K[x_1, \ldots, x_n]$ ein endlicher Integritätsbereich über einem unendlichen Körper K. Weiters sei d der Transzendenzgrad von $K(x_1, \ldots, x_n)$ über K. Dann existieren d Linearkombinationen $y_1, \ldots, y_d$ der x_i mit Koeffizienten in K, sodass R ganz über $K[y_1, \ldots, y_d]$ ist. ($y_1, \ldots, y_d$ sind dann algebraisch unabhängig und $K[y_1, \ldots, y_d]$ ein Polynomring.)*

Beweis. Siehe etwa [ZS75]. □

Satz 1.1. *Sei $R = K[x_1, \ldots, x_n]$ ein endlicher Integritätsbereich über einem Körper K. Weiters sei F eine algebraische Erweiterung des Quotientenkörpers $K(x_1, \ldots, x_n)$ von R. Dann ist der ganze Abschluss $\overline{R}_F$ von R in F ein endlicher Integritätsbereich über K und ein endlicher R-Modul.*

Beweis. Verwendet das Normalisierungslemma; siehe etwa [ZS75]. □

Satz 1.2. *Sei X ein lokaler algebraischer Integritätsbereich, $\hat{R}$ eine Komplettierung von R und $\overline{R}$ der ganze Abschluss von R. Dann gilt: Der ganze Abschluss von $\hat{R}$ ist gleich der Komplettierung von $\overline{R}$, d.h.*

$$\overline{\hat{R}} = \widehat{\overline{R}}.$$

Beweis. Siehe etwa [Rui93]. □

Satz 1.2 ist eine spezielle Version von Zariski's Main Theorem (vgl. Satz 1.10).

Lemma 1.7. *Sei R ein noetherscher reduzierter Ring und $\tilde{R}$ seine Normalisierung. Sei $I \subseteq R$ ein Ideal, das einen Nicht-Nullteiler von R beinhaltet. Dann gilt:*

1. *$R \subseteq \mathit{Hom}_R(I, I) \subseteq \tilde{R}$.*
2. *Ist I weiters ein Radikalideal, so gilt: $\mathit{Hom}_R(I, I) = \tilde{R} \cap \mathit{Hom}_R(I, R)$.*

Beweis. Siehe etwa [dJP00]. □

Satz 1.3. (Kriterium für Normalität von Grauert und Remmert) *Sei R ein noetherscher reduzierter Ring. Weiters sei $I = \sqrt{I} \subseteq R$ ein Radikalideal mit folgenden Eigenschaften:*

1. *I enthält einen Nicht-Nullteiler von R.*
2. *Sei $\wp$ ein Primideal in R, sodass $R_\wp$ nicht normal ist. Dann folgt: $\wp \supseteq I$.*

Dann ist R genau dann normal, wenn $R = \mathit{Hom}_R(I, I)$ gilt.

Beweis. Der Beweis dieses Satzes verwendet das letzte Lemma; siehe etwa [dJP00]. □

Bemerkung. Im Computeralgebrasystem SINGULAR wird genau dieses Kriterium zur Berechnung der Normalisierung $\tilde{R}$ eines reduzierten noetherschen Ringes R verwendet. Die Idee dabei ist, dass man den Ring $R_0 = R$ mittels eines geeigneten Ideals I_0 auf den Endomorphismenring $R_1 = \text{Hom}_{R_0}(I_0, I_0) \subseteq \tilde{R}$ vergrößert. Dieser Vorgang wird nun mit R_1 wiederholt. Damit erhält man eine aufsteigende Folge von Ringen

$$R = R_0 \subsetneqq R_1 \subsetneqq \cdots \subsetneqq R_k = \text{Hom}_{R_k}(I_k, I_k),$$

sodass auf Grund des Kriteriums von Grauert und Remmert $R_k = \tilde{R}$ gilt. (Der Algorithmus muss irgendwann stoppen, denn nach Satz 1.1 ist $\tilde{R}$ endlich über R.)

1.2.2 Geometrische Seite der Normalisierung

In diesem Abschnitt sei $\mathbb{K}$ stets ein algebraisch abgeschlossener Körper.

Seien X eine Varietät über $\mathbb{K}$ und

$$\mathbb{K}[X] = \mathbb{K}[Z_1, \ldots, Z_n]/I$$

der affine Koordinatenring von X (mit $I \leq \mathbb{K}[Z_1, \ldots, Z_n]$ Primideal).
Weiters sei $\mathcal{O}_a$ der lokale Ring von X in $a \in X$, $\mathcal{O}_a = \mathbb{K}[X]_{\mathfrak{m}_a}$.

Definition 1.4. Sei X eine Varietät über $\mathbb{K}$. Dann nennt man einen Punkt $a \in X$ einen *normalen Punkt von* X (oder X *normal in* a), wenn der Ring $\mathcal{O}_a$ ganz abgeschlossen in seinem Quotientenkörper $\mathbb{K}(X)$ ist. Die Varietät X heißt *normal*, wenn sie in jedem Punkt normal ist.

Beispiel 1.7. Jeder reguläre Punkt von X ist ein normaler Punkt.

Beispiel 1.8. Die Spitze $x^2 = y^3$ ist in 0 nicht normal (vergleiche Beispiel 1.1).

Beispiel 1.9. Die Schleife $x^2 = y^2 + y^3$ ist in 0 nicht normal, denn $u := \frac{x}{y}$ ist kein Element des Ringes $\mathcal{O}_a$, aber $u \in \mathbb{K}(X)$ ist ganz über $\mathcal{O}_a$, da $u^2 = 1+y$ gilt (vergleiche Beispiel 1.2).

Satz 1.4. *Sei X eine normale Varietät und sei $S = \mathrm{Sing}(X) \subseteq X$ der singuläre Ort von X. Dann gilt:*

$$\mathrm{codim}_X(S) \geq 2.$$

Beweis. Siehe etwa [Mum99]. □

Korollar 1.8. *Sei X eine Kurve. Dann gilt:*

$$X \text{ ist nichtsingulär} \quad \Longleftrightarrow \quad X \text{ ist normal.}$$

Definition 1.5. Man nennt eine Varietät X *nichtsingulär in Kodimension* 1, wenn sie in allen Punkten $a \in X$ mit $\mathrm{codim}_X(\overline{\{a\}}) = 1$ nichtsingulär ist.

Satz 1.5. *Sei $X \subseteq \mathbb{A}^n$ eine irreduzible affine Hyperfläche. Ist X nichtsingulär in Kodimension 1, so ist X eine normale Varietät.*

Beweis. Siehe etwa [Mum99]. □

Beispiel 1.10. Der Kegel $x^2 + y^2 = z^2$ ist in 0 singulär. Er ist dort aber nach dem letzten Satz normal.

Bemerkung. Für eine Varietät X gilt:

$$X \text{ nichtsingulär} \Rightarrow X \text{ normal} \Rightarrow X \text{ normal in Kodimension } 1.$$

Die umgekehrten Richtungen gelten jedoch im Allgemeinen nicht!

Definition 1.6. Seien X eine Varietät und L eine endliche algebraische Erweiterung von $\mathbb{K}(X)$. Eine *Normalisierung von X in L* ist eine normale Varietät $\tilde{X}$ mit $\mathbb{K}(\tilde{X}) = L$ zusammen mit einem endlichen surjektiven Morphismus $\pi : \tilde{X} \to X$, sodass die induzierte Abbildung $\pi^* : \mathbb{K}(X) \to \mathbb{K}(\tilde{X}) = L$ die gegebene Inklusion von $\mathbb{K}(X)$ in L ist.
Ist $L = \mathbb{K}(X)$, also π birational, so nennt man $\tilde{X}$ und π eine *Normalisierung von X*.

Beispiel 1.11. Wie wir in Beispiel 1.1 gesehen haben, ist

$$(\mathbb{A}^1, f)$$

mit $f : \mathbb{A}^1 \longrightarrow C, t \to (t^2, t^3)$ die Normalisierung der Spitze

$$C = V(Y^2 - X^3) \subseteq \mathbb{A}^2.$$

Weiters ist

$$(\mathbb{A}^1, g)$$

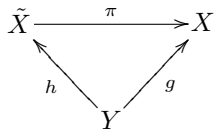
mit $g : \mathbb{A}^1 \longrightarrow D, t \to (t^2 - 1, t(t^2 - 1))$ die Normalisierung der Schleife

$$D = V(Y^2 - X^3 - X^2) \subseteq \mathbb{A}^2.$$

Satz 1.6. *Für jede Varietät X und jede endliche algebraische Erweiterung $L \supseteq \mathbb{K}(X)$ existiert genau eine Normalisierung von X in L.*
Genauer: Seien $\pi_i : \tilde{X}_i \to X$ zwei Normalisierungen von X in L. Dann existiert ein eindeutiger Isomorphismus $t : \tilde{X}_1 \to \tilde{X}_2$, sodass $\pi_1 = \pi_2 \circ t$ gilt und sodass t^* die identische Abbildung von L nach L ist.

Beweis. Siehe etwa [Mum99]. □

Satz 1.7. (Universelle Eigenschaft der Normalisierung) *Seien X und Y Varietäten. Weiters seien $g : Y \to X$ eine reguläre Abbildung, $g(Y)$ dicht in X und Y normal. Dann existiert eine reguläre Abbildung $h : Y \to \tilde{X}$, sodass das Diagramm*



kommutiert.

Beweis. Siehe etwa [Sha94]. □

Satz 1.8. *Die Normalisierung einer affinen irreduziblen Varietät ist wieder affin.*

Beweis. Siehe etwa [Sha94]. □

Satz 1.9. *Die Normalisierung einer projektiven Varietät X in einer endlichen algebraischen Erweiterung $L \supseteq \mathbb{K}(X)$ ist wieder eine projektive Varietät.*

Beweis. Siehe etwa [Mum99]. □

1.2.3 Zariski's Main Theorem

In der bisherigen Diskussion der Normalisierung sind wir auch im geometrischen Teil immer wieder auf Ideale von Polynomen und algebraischen Konstruktionen übergegangen. Trotzdem besitzt die Normalisierung auch einen geometrischen Inhalt. Dieser hat mit den "Zweigen" einer Varietät zu tun. Um diese Idee zu verstehen, werde ich zuerst den Fall $\mathbb{K} = \mathbb{C}$ betrachten und eine naive topolgische Beschreibung eines *Zweiges* angeben:

Seien X eine Varietät über $\mathbb{C}$, $x \in X$ ein abgeschlossener Punkt und $S = \text{Sing}(X) \subseteq$

X der singuläre Ort von X. Weiters sei $U \subseteq X$ eine genügend reguläre und genügend kleine Umgebung von x in der komplexen (oder starken) Topologie (bestehend nur aus abgeschlossenen Punkten).
Zerlege nun $U \setminus S$ in der komplexen Topologie in Komponenten:

$$U \setminus S = V_1 \cup \ldots \cup V_n.$$

Dann heißen die Abschlüsse $\overline{V_1}, \ldots, \overline{V_n}$ die *Zweige von X in x*.

Beispiel 1.12. Sei X die ebene Kurve

$$X = \mathrm{V}(x^2 - y^2 + x^3) \subseteq \mathbb{C}^2.$$

Weiters sei U folgende Umgebung des Nullpunktes (dem einzigen singulären Punkt der Varietät):

$$U = \{(x, y); |x| < \varepsilon, |y| < \varepsilon\}$$

für ein kleines ε. Dann "zerfällt"

$$U \cap (X \backslash \{(0, 0\})$$

immer in 2 Teile. Denn in $U \cap X$ gilt:

$$|x - y| \cdot |x + y| = |x|^3 < \varepsilon \cdot |x|^2.$$

Daher ist entweder $|x - y| < \sqrt{\varepsilon}|x|$ oder $|x + y| < \sqrt{\varepsilon}|x|$. Klarerweise können (falls $\varepsilon < 1$ ist) nicht beide Fälle gleichzeitig auftreten. Jeder der beiden Zweige ist zusammenhängend. Daher erhalten wir in $(0, 0)$ *zwei Zweige* von X, die durch $|x - y| \ll |x|$ und $|x + y| \ll |x|$ beschrieben werden können.

Beispiel 1.13. Sei X der Kegel $xy = z^2$ in $\mathbb{C}^3$ und sei

$$U = \{(x, y, z); |x| < \varepsilon, |y| < \varepsilon, |z| < \varepsilon\}.$$

Nun definieren wir eine stetige surjektive Abbildung:

$$\begin{array}{rcl} \{(s, t); |s| < \sqrt{\varepsilon}, |t| < \sqrt{\varepsilon}\} & \longrightarrow & X \cap (U \backslash \{(0, 0, 0)\}) \\ (s, t) & \longrightarrow & (s^2, t^2, st). \end{array}$$

Daher ist $X \cap (U \backslash \{(0, 0, 0)\})$ das stetige Bild einer zusammenhängenden Menge und somit selbst zusammenhängend. Folglich hat X im Ursprung nur *einen Zweig*.

Nun stellt sich die Frage, ob es einen rein algebraischen Weg gibt, mit diesen Zweigen umzugehen. Ein Weg, um die Existenz mehrerer Zweige in einem Punkt $x \in X$ festzustellen, ist, dass man *Überlagerungsräume* vom folgenden Typ sucht:

$$f : Y \to X,$$

sodass

- $f^{-1}(a)$ für alle $a \in X$ eine endliche Menge ist und
- f birational ist.

Damit wissen wir, dass für $f^{-1}(x) = \{x_1, \ldots, x_n\}$ und eine kleine komplexe Umgebung $U \subset X$ von x das Urbild $f^{-1}(U)$ in n Komponenten zerfällt, d.h.:

$$f^{-1}(U) = U_1 \cup \ldots \cup U_n,$$

wobei die U_i kleine Umgebungen der x_i sind. Dann ist jedes $\overline{f(U_i)}$ die Vereinigung einiger Teilmengen von Zweigen durch x. In anderen Worten: Wir erhalten n disjunkte Teilmengen der Menge der Zweige von X in x, wobei jede Teilmenge $\overline{f(U_i)}$ von den Zweigen von Y in x_i herrührt.

Es gibt einen kanonischen Weg, um derartige Überlagerungen zu finden: Seien $(Y, f) = (\tilde{X}, \pi)$ die Normalisierung von X, $S = \text{Sing}(X) \subset X$ der singuläre Ort von X und $S' := f^{-1}(S)$. In diesem Fall definiert f einen Isomorphismus von $Y \backslash S'$ nach $X \backslash S$. Daher ist $U \setminus S$ homeomorph zur disjunkten Vereinigung der Mengen $U_i \setminus S'$. Wir erhalten damit eine kanonische Zerlegung der Menge der Zweige von X in x. Der Hauptbestandteil von *Zariski's Main Theorem* besagt nun, dass eine normale Varietät in jedem ihrer Punkte nur aus einem Zweig besteht!
Der Vollständigkeit halber gebe ich verschiedene Versionen von Zariski's Main Theorem an:

Satz 1.10. (Zariski's Main Theorem) *Sei $\mathbb{K}$ ein algebraisch abgeschlossener Körper. Dann gilt:*

1. **Orginalform:** *Sei X eine normale Varietät über $\mathbb{K}$. Weiters sei $f : Y \to X$ ein birationaler Morphismus mit endlichen Fasern von einer Varietät Y nach X. Dann ist f ein Isomorphismus von Y auf eine offene Teilmenge $U \subseteq X$.*

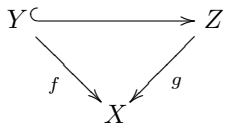
2. **Topologische Form:** *Seien X eine normale Varietät über $\mathbb{C}$ und $x \in X$ ein abgeschlossener Punkt. Weiters sei $S = \text{Sing}(X)$ der singuläre Ort von X. Dann existiert eine Basis $\{U_i\}$ von Umgebungen von x, sodass*

   $$U_i \setminus S$$

   für alle i zusammenhängend ist.

3. **Potenzreihen-Form:** *Seien X eine normale Varietät über $\mathbb{K}$ und $x \in X$ ein normaler (nicht notwendigerweise abgeschlossener) Punkt. Dann ist die Komplettierung $\widehat{\mathcal{O}_x}$ ein Integritätsbereich, der in seinem Quotientenkörper ganz abgeschlossen ist.*
   (Vergleiche Satz 1.2.)

4. **Grothendieck'sche Form:** *Sei $f : Y \to X$ ein Morphismus von Varietäten über $\mathbb{K}$ mit endlichen Fasern. Dann existiert ein Diagramm,*

   wobei Z eine Varietät, Y eine offene Teilmenge von Z und g ein endlicher Morphismus ist.

5. **Zusammenhangssatz:** *Sei X eine Varietät über $\mathbb{K}$, die in einem abgeschlossenen Punkt x normal ist. Weiters sei $f : Y \to X$ ein birationaler Morphismus. Dann ist $f^{-1}(x)$ (in der Zariski-Topolgie) eine zusammenhängende Menge.*

Beweis. Siehe etwa [Mum99]. □

1.3 Einführung in Standardbasen und Mora's Tangentialkegel Algorithmus

Eine *Monomordnung* auf der Menge $\mathbb{N}^n \times \{1, \ldots, s\}$ ist eine totale Ordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$, die mit der Addition in $\mathbb{N}^n$ verträglich ist und die keine unendlich absteigenden Folgen zulässt. Man nennt eine derartige Ordnung *graduiert*, wenn für alle $(\alpha, l), (\beta, m) \in \mathbb{N}^n \times \{1, \ldots, s\}$ gilt: $|\alpha| < |\beta|$ impliziert $(\alpha, l) < (\beta, m)$. Eine *Erweiterung* $<_\varepsilon$ von $<_\eta$ ist eine Monomordnung auf $\mathbb{N}^{n+p} \times \{1, \ldots, s\}$, deren Einschränkung auf $\mathbb{N}^n \times \{\gamma\} \times \{1, \ldots, s\}$ für alle $\gamma \in \mathbb{N}^p$ mit der von $<_\eta$ auf $\mathbb{N}^n \times \{\gamma\} \times \{1, \ldots, s\}$ induzierten Ordnung übereinstimmt.
Wir identifizieren Monomordnungen auf $\mathbb{N}^n \times \{1, \ldots, s\}$ immer mit der zugehörigen Ordnung der Monomvektoren in $K[\![x]\!]^s$.

Der *Initialmonomvektor* $\text{in}(g)$ eines Potenzreihenvektors $g = \sum_{\alpha,l} c_{\alpha l} x^\alpha e_l \in K[\![x]\!]^s$ bzgl. $<_\eta$ ist jener Vektor $c_{\alpha l} x^\alpha e_l$ der Entwicklung von g, der bzgl. $<_\eta$ minimal ist, d.h., der den in $\mathbb{N}^n \times \{1, \ldots, s\}$ kleinsten Exponenten (α, l) von g besitzt. Im Folgenden nehmen wir an, dass $x^\alpha e_l$ in der Entwicklung von g Koeffizient 1 hat. Dann schreiben wir g als $g = x^\alpha e_l - \overline{g}$ und nennen $\overline{g}$ den *Rest* von g.

Für einen Untermodul $I \subset K[\![x]\!]^s$ definieren wir den *Initialmodul* bzgl. $<_\eta$ als jenen Untermodul $\text{in}(I)$ von $K[\![x]\!]^s$, der von den Initialmonomvektoren aller Elemente von I erzeugt wird.

Für eine K-Algebra R mit $K[x] \subseteq R \subseteq K[\![x]\!]$ definieren wir

$$R_{loc} := R_{1+\mathfrak{m}} = \left\{ \frac{a}{1+b}; a, b \in R, b \in \mathfrak{m} \right\},$$

wobei $\mathfrak{m} :=_{K[\![x]\!]} \langle x_1, \ldots, x_n \rangle \cap R$.

Definition 1.7. Sei R^s das s-fache kartesische Produkt des Ringes R mit $K[x] \subseteq R \subseteq K[x]$. Weiters seien I ein Untermodul von R^s und $\{g_1, \ldots, g_r\} \subset I$. Wir sagen:

- $g \in R^s \setminus \{0\}$ hat eine *R-Standarddarstellung* durch $\{g_1, \ldots, g_r\}$, falls g eine Darstellung der Form
$$g = \sum h_i g_i$$
mit $h_i \in R^s$ und $\text{in}(h_i) \cdot \text{in}(g_i) \geq \text{in}(g)$ für alle i besitzt.
- Ein Element $h \in R^s$ ist eine *R^s-Normalform* von g bzgl. $\{g_1, \ldots, g_r\}$, falls $g - h$ eine R-Standarddarstellung durch $\{g_1, \ldots, g_r\}$ besitzt und entweder $h = 0$ oder $\text{in}(h) \notin \langle \text{in}(g_1), \ldots, \text{in}(g_r) \rangle$ gilt. Dann schreiben wir: $h \in \text{NF}(g, \{g_1, \ldots, g_r\}, R^s)$.
- $\{g_1, \ldots, g_r\}$ ist eine *R^s-Standardbasis* von I, falls die Menge $\{in(g_1), \ldots, in(g_r)\}$ den Initialmodul $\text{in}(I)$ erzeugt.

Bemerkung. Der folgende wichtige Satz aus der Theorie der Gröbnerbasen für Polynomringe liefert einen effektiven Test auf Idealzugehörigkeit:

Satz 1.11. *Sei $g \in K[x]$ ein Polynom, $I \subseteq K[x]$ ein Ideal und $\{g_1, \ldots, g_r\}$ eine Gröbnerbasis von I. Dann gilt:*

$$0 \textit{ ist eine Normalform von } g \textit{ bzgl. } \{g_1, \ldots, g_r\} \iff g \in I,$$
$$g \textit{ besitzt eine von } 0 \textit{ verschiedene Normalform bzgl. } \{g_1, \ldots, g_r\} \iff g \notin I.$$

Ein ähnliches Resultat gibt es auch im Falle von Standardbasen. Jedoch tritt dort neben den beiden obigen Fällen noch ein dritter Fall auf, nämlich jener, dass keine Normalform von g bzgl. der Standardbasis $\{g_1, \ldots, g_r\}$ existiert.

Beispiel 1.14. Seien $n = 1$, $g_1 := x - x^2$, $g := x$ und $I := \langle g_1 \rangle \subset K[x]$. Dann ist $\{g_1\}$ eine Standardbasis des Ideals I. Klarerweise gilt $x \notin \langle x - x^2 \rangle$. Daher existiert keine $K[x]$-Standarddarstellung von g durch $\{g_1\}$ und 0 ist keine Normalform von g bzgl. $\{g_1\}$. Darüber hinaus ergibt sich für eine Normalform $h \in K[x] \setminus \{0\}$ aus $x - h \in \langle g_1 \rangle$ durch Auswerten in 0: $h(0) = 0$, also $\text{in}(h) \in \langle \text{in}(g_1) \rangle$. Daraus folgt aber, dass g keine $K[x]$-Normalform bzgl. $\{g_1\}$ besitzt.

Definition 1.8. Wir sagen, dass der Modul R^s die Eigenschaft *(NF)* besitzt, falls für alle $\{g_1, \ldots, g_r\} \subseteq R^s$ und $g \in R^s$ eine R^s-Normalform von g bzgl. $\{g_1, \ldots, g_r\}$ existiert.

Satz 1.12. *Sei R^s ein Modul, der die Eigenschaft (NF) hat. Weiters seien $I \subseteq R^s$ ein Untermodul und $G \subseteq I$ eine Standardbasis von I. Dann gilt:*

1. *Für jedes $f \in R^s$ gilt: $f \in I \iff NF(f, G, R^s) = 0$.*
2. *Ist $J \subseteq R^s$ ein Untermodul mit $J \subseteq I$, dann folgt aus $in(I) = in(J)$ bereits $I = J$.*

Beweis. Vergleiche [GP02]. □

Satz 1.13. *Sei R^s ein Modul, der die Bedingung (NF) erfüllt. Weiters seien $g_1, \ldots, g_r \in R^s$ und $I = \langle g_1, \ldots, g_r \rangle \subseteq R^s$. Dann sind folgende Bedingungen äquivalent:*

1. *$\{g_1, \ldots, g_r\}$ ist eine R^s-Standardbasis von I.*
2. *Jedes $g \in I$ besitzt eine R-Standarddarstellung durch $\{g_1, \ldots, g_r\}$.*
3. *Für alle $g \in I$ gilt: $NF(g, \{g_1, \ldots, g_r\}, R^s) = 0$.*

Beweis. Vergleiche [GP02]. □

Aus den letzten beiden Sätzen erhält man, falls man Standandardbasen von Untermoduln und Normalformen von Elementen effektiv berechnen kann, einen Test auf Zugehörigkeit zu einem Untermodul.

Fortsetzung von Beispiel 1.14. Wir haben gesehen, dass $\text{NF}(g, \{g_1\}, K[x]) = \emptyset$ ist. Daher erfüllt der Ring $K[x]$ die Bedingung (NF) nicht! Darüber hinaus gilt in $K[x]$: $\{g_1\}$ ist eine Standardbasis des Ideals $J = \langle g \rangle = \langle g, g_1 \rangle$, ohne überhaupt eine Basis davon zu sein und $g \in J$, obwohl g keine $K[x]$-Standarddarstellung durch $\{g_1\}$ besitzt. Im Potenzreihenring $K[\![x]\!]$ gilt $\langle g \rangle = \langle g, g_1 \rangle = \langle g_1 \rangle$ und somit ist g_1 eine Standardbasis von I. Weiters ist $x = (\sum_{i=0}^{\infty} x^i) g_1$ eine $K[\![x]\!]$-Standarddarstellung von g durch $\{g_1\}$. Damit hat g eine $K[\![x]\!]$-Standarddarstellung durch $\{g_1\}$ und es gilt $0 \in \text{NF}(g, \{g_1\}, K[\![x]\!])$. Außerdem würde aus $h \in \text{NF}(g, \{g_1\}, K[\![x]\!]) \setminus \{0\}$ wieder $h(0) = 0$ folgen, also $\text{in}(h) \in \text{in}(I)$, was ein Widerspruch wäre. Daraus folgt: $\text{NF}(g, \{g_1\}, K[\![x]\!]) = \{0\}$.
Außerdem, da $\sum_{i=0}^{\infty} x^i = \frac{1}{1-x} \in K[x]_{loc}$ gilt, folgt mit demselben Argument: $\text{NF}(g, \{g_1\}, K[x]_{loc}) = \{0\}$ und $g = \frac{1}{1-x} \cdot g_1$ ist eine $K[x]_{loc}$-Standarddarstellung durch $\{g_1\}$.

Der folgende Satz zeigt, dass das obige Beispiel verallgemeinert werden kann. Er wird in Kapitel 6 ein wichtiger algorithmischer Bestandteil sein.

Satz 1.14. (Tangentialkegel-Satz und -Algorithmus)

1. *$K[x]^s_{loc}$ erfüllt die Bedingung (NF).*
2. *In $K[x]^s_{loc}$ sind die Bedingungen 1.,2. und 3. des letzten Satzes äquivalent.*
3. *Seien $G, F_1, \ldots, F_t \in K[x]^s_{loc}$ gegeben. Dann existiert ein endlicher Algorithmus ("Tangentialkegel-Algorithmus"), der*
   (a) *Polynome U und H berechnet, sodass U eine Einheit in $K[x]^s_{loc}$ und $U^{-1}H$ eine $K[x]^s_{loc}$-Normalform von G durch $\{F_1, \ldots, F_t\}$ sind.*
   (b) *Polynome $G_1, \ldots, G_u$ berechnet, sodass $\{G_1, \ldots, G_u\}$ eine $K[x]^s_{loc}$-Standardbasis von $\langle F_1, \ldots, F_t\rangle$ ist.*
   (c) *entscheidet, ob $G \in \langle F_1, \ldots, F_t\rangle$ gilt.*

Beweis. Vergleiche [MPT92]. □

1.4 Babylonische Division

Die Babylonische Division ist eine Variation der euklidischen Division für Polynome, die im Artikel [ACJHb] entwickelt wurde. Der Unterschied zur euklidischen Division besteht darin, dass man allgemeinere Leitmonome zulässt: Im Falle der Babylonischen Division müssen diese nicht maximal bzgl. einer Monomordnung in $\mathbb{N}^n$ sein.

Ich werde in diesem Abschnitt kurz die Schreibweisen und Ergebnisse von [ACJHb] zusammenfassen.

Definition 1.9. Der Untermodul I von $K[\![x]\!]^s$ erfüllt *Hironaka's Box-Bedingung* bzgl. $<_\eta$, wenn $\mathrm{co}(I)$ ein kartesisches Produkt von direkten Summen von endlichen freien monomialen $K[\![x_1,\ldots,x_j]\!]$-Moduln ist, d.h.

$$\mathrm{co}(I) = \prod_{l=1}^{s} \oplus_{j=0}^{n} \oplus_{\gamma\in Z_{lj}} K[\![x_1,\ldots,x_j]\!]\cdot x^\gamma$$

mit endlichen Mengen $Z_{lj} \subseteq \mathbb{N}^n$.

Definition 1.10. Polynomvektoren $P_1,\ldots,P_r \in K[x]^s$ bilden eine *Janet-Basis mit Reichweiten* $n_1,\ldots,n_r \le n$, wenn der durch $P_1,\ldots,P_r$ erzeugte Untermodul I von $K[x]^s$ gleich der direkten Summe $\oplus_{k=1}^{r} K[x_1,\ldots,x_{n_k}]\cdot P_k$ ist.

Bemerkung. Im Potenzreihenfall gilt die analoge Definition.

Janet-Basen verfeinern die Definition von Gröbner- bzw. Standardbasen. Theorem 2 in [ACJHb] besagt, dass sie durch Hinzunahme (zur Gröbner- bzw. Standardbasis) von geeigneten monomialen Vielfachen konstruiert werden kann.

Definition 1.11. Man nennt Monomvektoren $x^{\alpha_1}e_{l_1},\cdots,x^{\alpha_r}e_{l_r}$ mit (α_k,l_k) im Träger von P_k *Leuchttürme* für $P_1,\ldots,P_r$ bzgl. der Reichweiten $n_1,\ldots,n_r$, wenn die $x^{\alpha_1}e_{l_1},\ldots,x^{\alpha_r}e_{l_r}$ eine Janet-Basis mit Reichweiten $n_1,\ldots,n_r$ des von ihnen erzeugten monomialen Untermoduls M von $K[x]^s$ bilden und wenn die Reste $\overline{P_k} = x^{\alpha_k}e_{l_k} - P_k$ für alle k im kanonischen direkten monomialen Komplement $\mathrm{co}(M)$ von M in $K[x]^s$ liegen.

Seien Polynomvektoren $P_{\alpha l} \in K[x]^s$ der Form

$$P_{\alpha l} = x^\alpha e_l - \sum_{m=1}^{s}\sum_{\gamma\in\mathbb{N}^n} c_{\alpha l,\gamma m}x^\gamma e_m = x^\alpha e_l - \overline{P_{\alpha l}}$$

mit Leuchttürmen $x^\alpha e_l$, Reichweiten $n_{\alpha l}$ und Koeffizienten $c_{\alpha l,\gamma m}\in K$ gegeben, wobei (α,l) in einer endlichen Teilmenge V von $\mathbb{N}^n\times\{1,\ldots,s\}$ variiert.

Weiters seien $E = \cup_{(\alpha,l)\in V}(\alpha+\mathbb{N}^{n_{\alpha l}})\times\{l\}$ und $F = (\mathbb{N}^n\times\{1,\ldots,s\})\setminus E$, sodass $M = \oplus_{(\alpha,l)\in V} K[x_1,\ldots,x_{n_{\alpha l}}]\cdot x^\alpha e_l$ und $N = \mathrm{co}(M)$ aus Polynomvektoren in E bzw. F bestehen.

Definition 1.12. Die *Babylonische Division* eines Vektors $P\in K[x]^s$ durch die $P_{\alpha l}$'s bzgl. der Leuchttürme $x^\alpha e_l$ und der Reichweiten $n_{\alpha l}$ besteht darin, dass man jeden Monomvektor $x^\rho e_l$ in der Entwicklung von P durch ein monomiales Vielfaches des Restes $\overline{P_{\alpha l}}$ ersetzt.
Genauer: Sei (ρ,l) im Träger von P, dann liegt (ρ,l) entweder in F (wobei $x^\rho e_l$ dann

nicht ersetzt wird) oder in E. Liegt der zweite Fall vor, so existiert ein eindeutiges $(\alpha, l) \in V$, sodass (ρ, l) der Menge $(\alpha + \mathbb{N}^{n_{\alpha l}}) \times \{l\}$ angehört. Dann schreiben wir $\rho = \alpha + \nu$ mit $\nu \in \mathbb{N}^{n_{\alpha l}}$. Nun ersetzen wir in P jedes $x^\rho e_l$, für das $(\rho, l) \in E$ gilt, durch den Polynomvektor $x^\nu \cdot (P_{\alpha l} + \overline{P_{\alpha l}}) = x^\nu \cdot P_{\alpha l} + \sum_{m=1}^{s} \sum_\gamma c_{\alpha l, \gamma m} x^{\gamma+\nu} e_m$. Dies liefert uns ein neues Polynom $P' = P - x^\nu \cdot P_{\alpha l} \in K[x]^s$.
Dann wenden wir den Substitutionsprozess auf P' an und erhalten sukzessive Polynomvektoren P'', P''', usw.

Der Algorithmus terminiert für $k \in \mathbb{N}$, falls der Träger jenes Polynomvektors $P^{(k)}$, den man nach dem k-ten Substitutionsschritt erhält, ganz in F liegt. (In diesem Fall kann keine weitere Substitution mehr durchgeführt werden.) Man kann zeigen, dass dies der Fall ist, wenn der Modul $M = \oplus_{(\alpha,l)\in V} K[x_1, \ldots, x_{n_{\alpha l}}] \cdot x^\alpha e_l$ Hironaka's Box-Bedingung erfüllt.

Satz 1.15. *Seien $P_{\alpha l}$ mit $(\alpha, l) \in V \subsetneq \mathbb{N}^n \times \{1, \ldots, s\}$ eine endliche Menge von Polynomvektoren in $K[x]^s$ mit Leuchttürmen $x^\alpha e_l$ und Reichweiten $n_{\alpha l}$. Wir nehmen an, dass der monomiale Modul $M = \oplus_{(\alpha,l)\in V} K[x_1, \ldots, x_{n_{\alpha l}}] \cdot x^\alpha e_l$ Hironaka's Box-Bedingung erfüllt. Dann terminiert die Babylonische Division jedes Polynomvektors $P \in K[x]^s$ durch die $P_{\alpha l}$'s bzgl. der Leuchttürme $x^\alpha e_l$ und der Reichweiten $n_{\alpha l}$ in endlich vielen Schritten und liefert uns eine Zerlegung $P = \sum A_{\alpha l} P_{\alpha l} + R$ mit eindeutigen $A_{\alpha l} \in K[x_1, \ldots, x_{n_{\alpha l}}]$ und $R \in co(M)$. Speziell gilt: Die $P_{\alpha l}$'s bilden eine Janet-Basis mit Reichweiten $n_{\alpha l}$.*

Beweis. Siehe [ACJHb]. □

Beispiel 1.15. Wir werden die Babylonische Division anhand eines einfachen Beispieles demonstrieren: Betrachte jenes Ideal in $K[\![x, y]\!]$, das von den folgenden Polynomen erzeugt wird:

$$\begin{aligned} P_1 &= y^3 - x^4, \\ P_2 &= x^2y^2 - x, \\ P_3 &= x^2y - xy^2 - x^5. \end{aligned}$$

Wir verwenden eine Monomordnung $<_\eta$ auf $\mathbb{N}^2$, die durch eine Linearform $\lambda : \mathbb{N}^2 \to \mathbb{R}$ mit Komponenten $\lambda = (1, 1+\delta)$, wobei $\delta > 0$ genügend klein gewählt wird, gegeben ist. Auf jener Region von $\mathbb{N}^2$, die wir betrachten werden, stimmt diese Monomordnung mit der graduierten lexikographischen Ordnung mit $x < y$ überein. Die Initialmonome sind dann

$$\begin{aligned} M_1 &= y^3, \\ M_2 &= x^2y^2, \\ M_3 &= x^2y. \end{aligned}$$

Die zugehörigen Reichweiten sind 2, 1 und 1. Daraus ergibt sich

$$\text{in}(I) = K[\![x, y]\!]y^3 \oplus K[\![x]\!]x^2y^3 \oplus K[\![x]\!]x^2y$$

mit direktem kanonischen monomialen Komplement

$$\text{co}(I) = K[\![x]\!] \oplus Ky \oplus Kxy \oplus Ky^2 \oplus Kxy^2.$$

P_1, P_2 und P_3 sind Polynome mit Leuchttürmen M_1, M_2, M_3 und Reichweiten 2, 1, 1. Weiters erfüllt I Hironaka's Box-Bedingung. Damit sind alle Voraussetzungen des

letzten Satzes erfüllt.
Wir wollen nun

$$P := y^4$$

durch P_1, P_2 und P_3 bzgl. der Leuchttürme M_1, M_2, M_3 und der Reichweiten 2, 1, 1 babylonisch dividieren. Dabei erhalten wir

$$\begin{aligned} y^4 &= y \cdot y^3 \\ &= y \cdot P_1 + x^4 y \\ &= y \cdot P_1 + x^2 \cdot x^2 y \\ &= y \cdot P_1 + x^2 \cdot P_3 + x^3 y^2 + x^7 \\ &= y \cdot P_1 + x^2 \cdot P_3 + x \cdot x^2 y^2 + x^7 \\ &= y \cdot P_1 + x^2 \cdot P_3 + x \cdot P_2 + x^7 + x^2 \end{aligned}$$

mit Rest $R = x^7 + x^2 \in \mathrm{co}(I)$.

2 Der Ring der algebraischen Potenzreihen

In diesem Abschnitt sei stets $K = \mathbb{R}$ oder $\mathbb{C}$. Weiters seien $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_p)$.

2.1 Algebraische Potenzreihen

Zur Erinnerung:

Definition 2.1. Eine formale Potenzreihe $f \in K[\![x]\!]$ heißt *algebraisch*, wenn es ein Polynom

$$P(x,t) = a_0(x)t^p + a_1(x)t^{p-1} + \ldots + a_{p-1}(x)t + a_p(x) \in K[x,t],$$

$P \neq 0$ gibt, sodass $P(x, f(x)) = 0$.

In anderen Worten: Algebraische Potenzreihen sind gerade jene Elemente von $K[\![x]\!]$, die algebraisch über $K[x]$ sind. Damit bilden sie (nach den Eigenschaften von algebraischen Erweiterungen) einen Ring - den *Ring der algebraischen Potenzreihen*. Wir werden ihn im Folgenden mit $\mathcal{N}_n$, $K\langle x\rangle$ oder $K\langle x_1, \ldots, x_n\rangle$ bezeichnen.

Es gilt: Ist f eine algebraische Potenzreihe mit $f(0) \neq 0$, dann ist auch $g := \frac{1}{f}$ eine algebraische Potenzreihe.
Denn: Da f eine algebraische Potenzreihe ist, existiert ein von 0 verschiedenes Polynom $P(x,t) = a_0(x)t^p + \ldots + a_p(x) \in K[x,t]$ mit $P(x, f(x)) = 0$. Dann gilt für $Q(x,u) := a_p(x)u^p + a_{p-1}(x)u^{p-1} + \ldots + a_1(x)u + a_0(x) \in K[x,u]$ jedoch: $Q(x, g(x)) = 0$. Und damit ist g eine algebraische Potenzreihe.
Daraus folgt, dass alle $f \in K\langle x\rangle$ mit $f(0) \neq 0$ in $K\langle x\rangle$ Einheiten sind. Somit ist der Ring der formalen Potenzreihen ein lokaler Ring mit maximalem Ideal

$$\{f \in K\langle x\rangle; f(0) = 0\}.$$

Satz 2.1. (M. Artin's Approximations-Satz) *Sei $\mathfrak{m}$ das maximale Ideal eines Ringes von konvergenten Potenzreihen und $\hat{\mathfrak{m}}$ das maximale Ideal des zugehörigen Ringes von formalen Potenzreihen. Weiters sei $f = (f_1, \ldots, f_q) \in K\{x,y\}^q$ mit $f(0,0) = 0$.*
Dann gilt: Ist $\hat{g}(x) = (\hat{g_1}(x), \ldots, \hat{g_q}(x)) \in K[\![x]\!]^p$ eine Lösung des Systems $f(x,y) = 0$, dann existiert für jedes $\alpha \in \mathbb{N}$, $\alpha \geq 1$, eine Lösung $g(x) = (g_1(x), \ldots, g_q(x)) \in K\{x\}^q$ von $f(x,y) = 0$ mit

$$g(x) = \hat{g}(x) \bmod \hat{\mathfrak{m}}^\alpha.$$

Beweis. Siehe etwa [Rui93]. □

Folgerung 2.1. *Jede algebraische Potenzreihe ist konvergent.*

Beweis. Für jede algebraische Potenzreihe f existiert ein von 0 verschiedenes Polynom $P \in K[x,t]$ mit $P(x, f(x)) = 0$. (Ist $P(0,0) \neq 0$, so setze $\tilde{P} := P \cdot t$. Für $\tilde{P}$ gilt klarerweise $\tilde{P}(0,0) = 0$, $\tilde{P} \neq 0$ und $\tilde{P}(x, f(x)) = 0$.) Nach Artin's Approximations-Satz (vgl. Satz 2.1) existiert dann für jedes $\alpha \in \mathbb{N}$, $\alpha \geq 1$, eine konvergente Potenzreihe $f_\alpha(x) \in K\{x\}$, deren Taylorentwicklung bis zum Grad α mit jener von $f(x)$ übereinstimmt und die $P(x, f_\alpha(x)) = 0$ erfüllt. Wären nun alle f_α verschieden von f, so hätte die polynomiale Gleichung $P(x,t) = 0$ unendlich viele verschiedene Lösungen in $K[\![x]\!]$, was unmöglich ist. □

Beispiel 2.1. Es ist klar, dass die Potenzreihe

$$f := \sum_{k \geq 0} x^{2^k}$$

(als Teilreihe der geometrischen Reihe) für $-1 < x < 1$ konvergiert. Weiters kann man zeigen, dass f keine algebraische Potenzreihe ist.

Damit gilt:

$$K\langle x \rangle \subsetneq K\{x\} \subsetneq K[\![x]\!].$$

2.2 Substitution

Seien $y = (y_1, \ldots, y_p)$ und t eine weitere Variable. Weiters sei $P \in K[\![x]\!][t]$ ein t-reguläres Polynom vom Grad p. Mit F bezeichnen wir im Folgenden den algebraischen Abschluss des Quotientenkörpers von $K[\![y]\!]$. Sei $\xi \in F$ eine Nullstelle von P.
Für $f(y,t) \in K[\![y,t]\!]$ sei $R(y,t) \in K[\![y]\!][t]$ der Rest der formalen Division von f durch P bzgl. dem Initialmonom t^p. Wir setzen

$$f(y,\xi) = R(y,\xi) \in F.$$

Lemma 2.2. *Es gilt:*

1. *Die Abbildung $f(y,t) \to f(y,\xi)$ ist ein K-Algebrenhomomorphismus.*
2. *Ist $f \in K\langle y,t \rangle$ und $f(y,\xi) = 0$, dann ist ξ algebraisch über $K[y]$.*
3. *Ist $f \in K\langle y,t \rangle$ und ξ algebraisch über $K[y]$, dann ist $f(y,\xi)$ auch algebraisch über $K[y]$ (d.h. $f(y,\xi) \in K\langle y \rangle$).*

Beweis. Vergleiche [Rui93]. □

Satz 2.2. *Seien $f, g_1, \ldots, g_n \in \mathcal{N}$ mit $g_1(0) = \ldots = g_n(0) = 0$. Dann liefert die Substitution $f(g_1, \ldots, g_n)$ wieder eine algebraische Potenzreihe.*

Beweis. Zuerst nennen wir einige Variablen um, indem wir $g_1(z), \ldots, g_n(z)$ schreiben. Dann betrachten wir die Division

$$f(x) = Q(z,x)(x_n - g_n(z)) + R(z, x_1, \ldots, x_{n-1}),$$

wobei $R(z, x_1, \ldots, x_{n-1}) \in K[\![x_1, \ldots, x_{n-1}]\!]$. Damit gilt:

$$f(x_1, \ldots, x_{n-1}, g_n(z)) = R(z, x_1, \ldots, x_{n-1}).$$

Nun liegt mit

$$y = (z, x_1, \ldots, x_{n-1}), t = x_n, P = x_n - g_n(z), \xi = g_n(z)$$

dieselbe Situation wie in Lemma 2.2 vor. Damit gilt:

$$f(x_1, \ldots, x_{n-1}, g_n(z)) \in K\langle z, x_1, \ldots, x_{n-1} \rangle.$$

Wiederholt man dasselbe Argument weitere $n-1$ mal, so ist die Aussage des Satzes bewiesen. □

2.3 Ableitung

Satz 2.3. *Die partiellen Ableitungen einer algebraischen Potenzreihe sind wieder algebraische Potenzreihen.*

Beweis. Sei $f \in \mathcal{N}_n$ und

$$P(x, f(x)) = a_0(x)f(x)^p + \ldots + a_p(x) = 0.$$

Leiten wir diese Gleichung partiell nach x_i ab, so ergibt sich

$$0 = \frac{\partial}{\partial x_i}(P(x, f(x))) = \sum_{j=0}^{p} \frac{\partial a_j}{\partial x_i} f^{p-j} + \underbrace{\frac{\partial f}{\partial x_i} \sum_{j=0}^{p-1} (p-j) a_j f^{p-j-1}}_{(*)}.$$

Wählen wir P mit minimalem Grad, so ist die Summe $(*)$ ungleich null. (Denn wäre sie null, so würde für $\tilde{P}(x,t) = \partial_{x_i} f \cdot \sum_{j=0}^{p-1}(p-j)a_j(x,t)t^{p-j-1}$ gelten: $\tilde{P}(x, f(x)) = 0$ und $\deg(\tilde{P}) < \deg(P)$, was ein Widerspruch zu unserer Wahl von P ist.) Da die Ableitungen $\partial_{x_i} a_j$ der a_j's wieder Polynome sind, ist die Potenzreihe $\partial_{x_i} f$ algebraisch über $K(x)[f]$ und folglich auch über $K(x)$. □

2.4 Divisionssatz für algebraische Potenzreihenvektoren (Existenz)

Dazu wiederholen wir zuerst den Divisionsatz für formale Potenzreihen von Grauert-Hironaka-Galligo (vergleiche etwa [Hir77]).

Satz 2.4. *Sei I ein Untermodul von $K[\![x]\!]^s$ mit Initialmodul in(I) bzgl. einer Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$. Weiters sei co$(I)$ das kanonische direkte monomiale Komplement von in(I) in $K[\![x]\!]^s$. Dann gilt:*

$$I \oplus co(I) = K[\![x]\!]^s.$$

Wird der Untermodul I von $g_1, \ldots, g_r \in K[\![x]\!]^s$ erzeugt, so folgt aus dem letzten Satz, dass jeder Vektor $f \in K[\![x]\!]^s$ eine Zerlegung der Form

$$f = \sum_k a_k g_k + c$$

mit einem eindeutigen $c \in \text{co}(I)$ besitzt. Die Potenzreihenentwicklungen der Quotienten a_k und des Restes c können bis zu einem beliebigen Grad durch einen endlichen Algorithmus berechnet werden. Der Rest c ist unabhängig von der Wahl von $g_1, \ldots, g_r$ (aber abhängig von der Monomordnung $<_\eta$).

Aus dem letzten Satz folgt weiters:

Korollar 2.3. *Seien I, J Untermoduln von $K[\![x]\!]^s$ mit $J \subseteq I$ und* $\text{in}(J) = \text{in}(I)$ *bzgl. einer Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$. Dann gilt bereits $J = I$.*

Die Existenz des Divisionssatzes für algebraische Potenzreihen wurde ursprünglich von Hironaka für Ideale, die die Box-Bedingung erfüllen, bewiesen. Vergleiche [Hir77]. Wir formulieren den Satz hier für Moduln:

Satz 2.5. *Sei I ein Untermodul von $K[\![x]\!]^s$, der von algebraischen Potenzreihenvektoren erzeugt wird. Angenommen, I erfüllt Hironaka's Box-Bedingung bzgl. einer Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$. Dann ist für alle algebraischen Potenzreihenvektoren $f \in K[\![x]\!]^s$ der Rest c der formalen Potenzreihendivision von f durch I ein algebraischer Potenzreihenvektor.*

Der letzte Satz impliziert, dass I eine reduzierte Standardbasis, bestehend aus algebraischen Potenzreihenvektoren, besitzt.
Lässt man Hirnoka's Box-Bedingung weg, so ist der Rest c der Division im Allgemeinen nicht mehr algebraisch. (Dividiere zum Beispiel xy durch $(x - y^2)(y - x^2) = xy - x^3 - y^3 + x^2y^2$ mit Initialmonom xy.)

In Kapitel 7 werden wir eine konstruktive Version von Satz 2.5 beweisen.

3 Codes von algebraischen Potenzreihen

Im Folgenden sei K stets ein Körper der Charakteristik 0. Weiters seien die Variablen $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_p)$ fixiert.

3.1 Definition eines Codes

Definition 3.1. Ein *Muttercode (in x und y)* ist ein polynomialer Zeilenvektor $H = (H_1, \ldots, H_p) \in K[x, y]^p$ mit $H(0, 0) = 0$, dessen Jacobi-Matrix $D_y H$ bzgl. y in 0 invertierbar ist, d.h.

$$D_y H(0, 0) \in \mathrm{Gl}_p(K).$$

Die Invertierbarkeit von $D_y H(0, 0)$ kann auch folgendermaßen umformuliert werden: Für jede gradkompatible Monomordnung auf $\mathbb{N}^p$ wird das Initialideal des Ideals $\langle H_1(0, y), \ldots, H_p(0, y)\rangle \subseteq K[\![y]\!]$ von $y_1, \ldots, y_p$ erzeugt. Daher existiert ein linearer Koordinatenwechsel in den y_i's, sodass das Initialmonom $\mathrm{in}(H_i(0, y))$ von $H_i(0, y)$ für alle $1 \leq i \leq p$ gleich y_i ist.
Der *Babyreihenvektor* eines Muttercodes $H \in K[x, y]^p$ ist gerade jener Vektor $h = (h_1, \ldots, h_p) \in K[\![x]\!]$ mit $h(0) = 0$, der die eindeutige Lösung von

$$H(x, h(x)) = 0$$

ist. Also ist h durch H bestimmt. Existenz und Eindeutigkeit von h sind auf Grund des Satzes über implizite Funktionen für formale Potenzreihen gesichert. Es gilt sogar, dass die einzelnen Komponenten h_i des Babyreihenvektors auf Grund des Satzes über implizite Funktionen für algebraische Potenzreihen (vgl. [Art69]) wieder algebraische Potenzreihen sind.
Ein Vektor von algebraischen Potenzreihen $h = (h_1, \ldots, h_p) \in K[\![x]\!]^p$ heißt ein *Babyreihenvektor*, wenn es einen Muttercode $H \in K[x, y]^p$ gibt, der h definiert.
Ein *Vatercode* ist ein Vektor $G = (G_1, \ldots, G_r)$ von Polynomen $G_i \in K[x, y]^s$. Er unterliegt keinen weiteren Bedingungen.
Ein *Familiencode* ist ein Paar (H, G), wobei $H \in K[x, y]^p$ ein Muttercode und $G \in K[x, y]^{s\times r}$ ein Vatercode in denselben Variablen sind.
Man sagt, dass die algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ den *Familiencode* $(H, G) \in K[x, y]^p \times K[x, y]^{s\times r}$ haben, wenn für alle $1 \leq k \leq r$ gilt:

$$g_k = G_k(x, h(x)) \in K[\![x]\!]^s,$$

wobei $h \in K[\![x]\!]^p$ der durch H definierte Babyreihenvektor ist.

3.2 Existenz und Konstruktion eines Codes einer algebraischen Potenzreihe

Satz 3.1. *Für jede algebraische Potenzreihe $g \in K[\![x]\!]$ kann man aus einer algebraischen Relation $P(x, t) = 0$ für g (d.h. $P(x, g(x)) = 0$) und der Taylorentwicklung von g bis zu einem genügend hohen Grad einen Familiencode $(H, G) \in K[x, y]^p \times K[x, y]$ von g konstruieren.*

Beweis. Vergleiche auch Appendix in [AMR92].
Betrachte die algebraische Menge

$$V := \{(x, t); P(x, t) = 0\} \subseteq \mathbb{A}_K^n \times \mathbb{A}_K = \mathbb{A}_K^{n+1}.$$

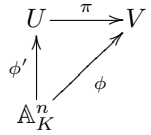
Ohne Beschränkung der Allgemeinheit können wir voraussetzen, dass P irreduzibel ist. Ist dies nicht der Fall, so faktorisieren wir P, und da wir die Taylorentwicklung von g bis zu einem genügend hohen Grad kennen, können wir leicht feststellen, welcher der Faktoren von P die algebraische Potenzreihe g als Nullstelle hat. Weiters können wir ohne Beschränkung der Allgemeinheit annehmen, dass die algebraische Potenzreihe g keinen konstanten Term hat, d.h., $g(0) = 0$ ist, und dass $a = (0, 0)$ ein Element von V ist, d.h., dass auch P keinen konstanten Term hat.
Auf Grund von Satz 1.6 existiert die Normalisierung von V in $K(V)$ (und diese ist bis auf Isomorphie eindeutig), d.h. es existiert eine algebraische normale Menge $U \subseteq \mathbb{A}_K^{n+p}$ mit $K(U) = K(V)$ und ein endlicher birationaler Morphismus $\pi : U \to V$. Auf Grund von Satz 1.8 wissen wir, dass U wieder eine affine algebraische Varietät ist. Daher können wir eine Einbettung $U \subseteq \mathbb{A}_K^{n+p}$ wählen, sodass $\pi : U \subseteq \mathbb{A}_K^{n+p} \to V \subseteq \mathbb{A}_K^{n+1}$ durch die Projektion $\tau : \mathbb{A}_K^{n+p} \longrightarrow \mathbb{A}_K^{n+1}, (x, y_1, \ldots, y_p) \longrightarrow (x, y_1)$ induziert wird.
Seien $F_1, \ldots, F_m \in K[x, y_1, \ldots, y_p]$ definierende Gleichungen für U, d.h.

$$K[U] = K[x, y_1, \ldots, y_p]/\langle F_1, \ldots, F_m \rangle.$$

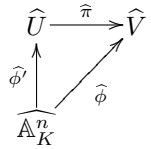
Wir betrachten nun die folgende Auswertungsabbildung:

$$\phi : \mathbb{A}_K^n \longrightarrow V \subseteq \mathbb{A}_K^{n+1}; x \to (x, g(x)).$$

Auf Grund der universellen Eigenschaft der Normalisierung (vgl. Satz 1.7) existiert eine reguläre Abbildung $\phi' : \mathbb{A}_K^n \longrightarrow U$, sodass das folgende Diagramm kommutiert:



Nun lokalisieren wir V und U in den Punkten $a = \phi(0) = (0, 0) \in V \subseteq \mathbb{A}_K^{n+1}$ bzw. $b = \phi'(0) \in U \subseteq \mathbb{A}_K^{n+p}$. Bezeichnen wir jetzt die Komplettierungen von $V \subseteq \mathbb{A}_K^{n+1}$ in a und $U \subseteq \mathbb{A}_K^{n+p}$ in b mit $\widehat{V}$ bzw. $\widehat{U}$, so ergibt sich (vgl. Satz 1.2) das folgende kommutative Diagramm:



Auf Grund von Zariski's Main Theorem (Satz 1.10) ist $\widehat{U}$ eine irreduzible n-dimensionale Varietät. Diese enthält den Graph von ϕ', der aber eine n-dimensionale Mannigfaltigkeit ist. Somit ist $\widehat{U}$ selbst glatt.
Daher hat die Jacobi-Matrix der F_i's ($1 \leq i \leq m$) bzgl. $y_1, \ldots, y_p$ im Punkt b Rang p. Folglich existieren p Linearkombinationen $H_1, \ldots, H_p$ der $F_1, \ldots, F_m$, sodass $(H_1, \ldots, H_p)$ ein Muttercode der algebraischen Potenzreihe g im Punkt b ist. Nach Konstruktion gilt $h_1 = g$. Somit kann $G = y_1$ als Vatercode der algebraischen Potenzreihe g gewählt werden. Damit haben wir die Existenz eines Familiencodes für g bewiesen.

□

Bemerkung. Wie man an Hand des Beweises des letzten Satzes sieht, ist es möglich, den Vatercode G immer gleich y_1 zu wählen. Dann ist g gerade die erste Komponente des Babyreihenvektors h von H.

3.3 Beispiele

Beispiel 3.1. In diesem Beispiel sei die Potenzreihe

$$g(x) := \sqrt[3]{1+x} - 1 = \frac{1}{3}x - \frac{1}{9}x^2 + \frac{5}{81}x^3 - \frac{10}{243}x^4 + \frac{22}{729}x^5 + - \ldots \in \mathbb{R}[\![x]\!]$$

gegeben. Diese ist eine algebraische Potenzreihe, denn für

$$P(x,t) = (t+1)^3 - x - 1 = t^3 + 3t^2 + 3t - x$$

gilt $P(x, g(x)) = 0$. Weiters ist g eine um 0 zentrierte Potenzreihe, denn $g(0) = 0$. Um einen Code für g zu finden, betrachten wir den Ring

$$R := K[x,t]/\langle t^3 + 3t^2 + 3t - x\rangle.$$

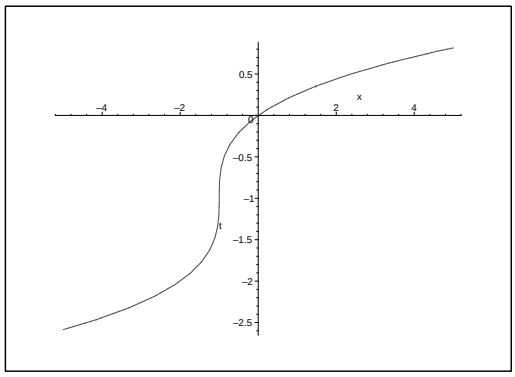


Abbildung 1: $\mathcal{C} = \mathrm{V}(P(x,t))$.

Der Ring R ist normal, denn die ebene Kurve

$$\mathcal{C} := \mathrm{V}(P) \subseteq \mathbb{R}^2$$

(siehe Abbildung 1) ist auf Grund von

$$\mathrm{grad}(P(x,t)) = (-1, 3t^2 + 6t + 3) \neq (0,0) \ \ \forall (x,t) \in \mathbb{R}^2$$

nichtsingulär und damit nach Korollar 1.8 normal. Also gilt $\tilde{R} = R$.
Nach dem Beweis des letzten Satzes ist daher

$$\begin{aligned} H &= y^3 + 3y^2 + 3y - x, \\ G &= y \end{aligned}$$

ein Code für die algebraische Potenzreihe g.

Probe: $H = y^3 + 3y^2 + 3y - x$ erfüllt alle Voraussetzungen für einen Muttercode, denn $H(0,0) = 0$ und

$$D_y H(0,0) = (3y^2 + 6y + 3)(0,0) = 3 \in \mathrm{Gl}_1(\mathbb{R}).$$

Weiters definiert H auf Grund der Bedingung $h(0) = 0$ eindeutig den Babyreihenvektor $h(x) = \sqrt[3]{1+x} - 1$. Außerdem gilt:

$$G(x, h(x)) = h(x) = g.$$

Damit ist $(H, G) = (y^3 + 3y^2 + 3y - x, y)$ ein Familiencode für $g = \sqrt[3]{x+1} - 1$.

Beispiel 3.2. In diesem Beispiel wollen wir einen Familiencode für die algebraische Potenzreihe

$$g(x) := \frac{1}{1+x+x^2} - 1 = -x + x^3 - x^4 + - \ldots \in \mathbb{R}[\![x]\!]$$

finden. Offensichtlich ist g ist eine algebraische Potenzreihe, denn g erfüllt $P(x, g(x)) = 0$ mit

$$P(x,t) := (t+1)(1+x+x^2) - 1 = tx^2 + tx + t + x + x^2.$$

Weiters gilt $g(0) = 0$. Auch der Ring

$$R := \mathbb{R}[x,t]/\langle tx^2 + tx + t + x + x^2 \rangle$$

ist bereits normal, denn die ebene Kurve $\mathcal{D} = \mathrm{V}(P)$ (siehe Abbildung 2) hat keinen singulären Punkt (grad$(P(x,t)) = (2tx+t+1+2x, x^2+x+1) \neq (0,0)\ \forall (x,t) \in \mathbb{R}^2$) und ist damit nach Korollar 1.8 normal.

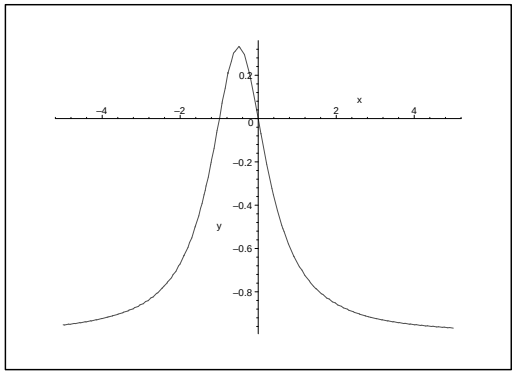


Abbildung 2: $\mathcal{D} = \mathrm{V}(P(x,t))$.

Damit ist wiederum $\tilde{R} = R$ und

$$\begin{aligned} H &= yx^2 + yx + y + x + x^2, \\ G &= y \end{aligned}$$

ein Code für die gesuchte algebraische Potenzreihe.

Probe: H erfüllt alle Anforderungen an einen Muttercode: $H(0,0) = 0$ und

$$D_y H(0,0) = (x^2 + x + 1)(0,0) = 1 \neq 0.$$

Weiters definiert H eindeutig die Babyreihe $h(x) = \frac{1}{1+x+x^2} - 1 \in \mathbb{R}[\![x]\!]$. Auch die Bedingung $G(x, h(x)) = g(x)$ ist erfüllt.

Beispiel 3.3. In den letzten beiden Beispielen haben wir gesehen, dass es leicht ist, einen Code für einen normalen Ring zu konstruieren. Daher betrachten wir nun einen nichtnormalen Ring:
Sei

$$P(x,t) = t^2 - x^3 - x^2.$$

Dann hat die ebene Kurve

$$\mathcal{E} = \mathrm{V}(P) \subseteq \mathbb{R}^2$$

(siehe Abbildung 3) im Punkt $(0,0)$ einen singulären Punkt (grad$(P(x,t)) = (-3x^2 - 2x, 2t)$) und damit ist $(0,0)$ nach Korollar 1.8 kein normaler Punkt von $\mathcal{E}$. (Andere Argumentation: Die Kurve $\mathcal{E}$ besteht im Punkt $(0,0)$ aus zwei verschiedenen Ästen (vergleiche Beispiel 1.12) und ist daher nach Zariski's Hauptsatz nicht normal.)

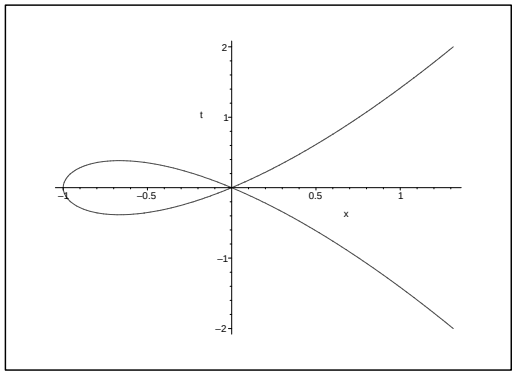


Abbildung 3: $\mathcal{E} = \mathrm{V}(P(x,t))$.

Wir wollen nun einen Code für die Potenzreihe

$$g(x) := x\sqrt{1+x} = x + \frac{1}{2}x^2 - \frac{1}{8}x^3 + \frac{1}{16}x^4 - \frac{5}{128}x^5 + - \ldots \in \mathbb{R}[\![x]\!]$$

finden. Klarerweise ist g eine algebraische Potenzreihe, denn g erfüllt $P(x, g(x)) = 0$. Weiters gilt $g(0) = 0$. Die algebraische Potenzreihe g ist gerade jener Zweig von $\mathcal{E}$, der in $(0,0)$ die Steigung $+1$ hat (siehe Abbildung 4).

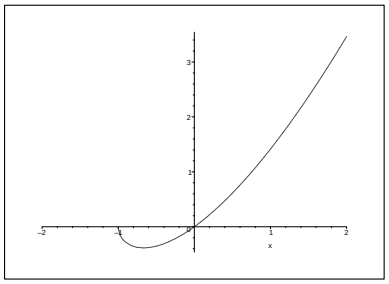


Abbildung 4: $g(x) = x\sqrt{1+x}$, $x \geq -1$.

Wie wir schon festgestellt haben, ist

$$R := \mathbb{R}[x,t]/\langle t^2 - x^3 - x^2 \rangle$$

kein normaler Ring. In Beispiel 1.2 haben wir gesehen, dass $y_2 := \frac{t}{x}$ ganz über R ist und dass

$$\tilde{R} = \mathbb{R}[x, y_1, y_2]/\langle x + 1 - y_2^2, y_1 + y_2 - y_2^3\rangle \cong \mathbb{R}[y_2]$$

die Normalisierung von R ist. Für den von uns gesuchten Zweig g von $\mathcal{E}$ ist $y_2 = \frac{t}{x}$ in einer kleinen Umgebung vom Ursprung gleich 1. Damit erhalten wir im Punkt $(x, y_1 = t, y_2) = (0, 0, 1)$ folgenden Code für die algebraische Potenzreihe g:

$$\begin{aligned} H_1' &= x + 1 - y_2^2, \\ H_2' &= y_1 + y_2 - y_2^3, \\ G &= y_1. \end{aligned}$$

Probe: $H' = (H_1', H_2') = (x + 1 - y_2^2, y_1 + y_2 - y_2^3)$ erfüllt alle Bedingungen für einen Muttercode, denn $H'(0, 0, 1) = (0, 0)$ und

$$D_y H'(0, 0, 1) = \begin{pmatrix} 0 & 1 \\ -2y_2 & 1 - 3y_2^2 \end{pmatrix} (0, 0, 1) = \begin{pmatrix} 0 & 1 \\ -2 & -2 \end{pmatrix} \in \mathrm{Gl}_2(\mathbb{R}).$$

Weiters ist der Babyreihenvektor $h' = (h_1', h_2')$ durch $H'(x, h(x)) = 0$ eindeutig bestimmt: das Gleichungssystem

$$\begin{aligned} x + 1 - h_2'^2 &= 0, \\ h_1' + h_2' - h_2'^3 &= 0 \end{aligned}$$

besitzt die eindeutige Lösung

$$h' = (h_1', h_2') = (x\sqrt{1 + x}, \sqrt{1 + x})$$

mit $h(0) = (0, 1)$. Auch die Bedingung $G(x, h'(x)) = g(x)$ ist erfüllt.

Suchen wir nun einen Code für g im Punkt $(0, 0, 0)$, so betrachten wir die Taylorentwicklung von H' im Punkt $(0, 0, 0)$. Es ergibt sich:

$$\begin{aligned} H_1 &= x + 1 - (y_2 + 1)^2 = x - 2y_2 - y_2^2, \\ H_2 &= y_1 + (y_2 + 1) - (y_2 + 1)^3 = y_1 - y_2^3 - 3y_2^2 - 2y_2. \end{aligned}$$

Man kann leicht nachprüfen, dass $(H, G) = ((x - y_2 + y_2^2, y_1 - y_2^3 - 3y_2^2 - 2y_2), y_1)$ ein Code (im Punkt $(0, 0, 0)$) für die algebraische Potenzreihe $g = x\sqrt{1 + x}$ ist.

Analog ergibt sich für den zweiten Zweig von $\mathcal{E}$, also für die algebraische Potenzreihe

$$g'' := -x\sqrt{1 + x},$$

folgender Code (im Punkt $(0, 0, 0)$):

$$(H'', G'') = ((x + 2y_2 - y_2^2, y_1 - y_2^3 + 3y_2^2 - 2y_2), y_1).$$

Bemerkung: Wie schon im letzten Abschnitt erwähnt wurde, kann das Computeralgebrasystem SINGULAR die Normalisierung eines Ringes berechnen:
(Vergleiche [GP02].)

```
>LIB "normal.lib"; LIB "surf.lib";
>ring A=0,(x,t),dp;
>ideal I=t2-x3-x2;
>list nor=normal(I);
     'normal' created a list of 1 ring(s)
>def R=nor[1]; setring R;
>norid;
     norid[1]=0
>normap;
     normap[1]=T(1)2-1, normap[2]=T(1)3-T(1)
```

Dies liefert für die Normalisierung von $R := K[x,t]/\langle t^2 - x^3 - x^2\rangle$:

$$\pi : \tilde{\mathcal{E}} = \mathbb{A}^1 \longrightarrow \mathcal{E}, T(1) \to (T(1)^2 - 1, T(1)^3 - T(1)).$$

Daher gilt

$$\tilde{R} = K[x,t,T(1)]/\langle x - T(1)^2 + 1, t - T(1)^3 + T(1)\rangle \cong K[T(1)].$$

Man sieht also, dass auch SINGULAR dasselbe Ergebnis liefert!

Beispiel 3.4. Sei

$$g(x) := x^3\sqrt{1+x+x^2} = x^3 + \frac{1}{2}x^4 + \frac{3}{8}x^5 + \ldots \in \mathbb{R}[\![x]\!].$$

Die Potenzreihe g ist eine algebraische Potenzreihe, denn für

$$P(x,t) := t^2 - x^6(1+x+x^2) = t^2 - x^8 - x^7 - x^6$$

gilt $P(x, g(x)) = 0$.

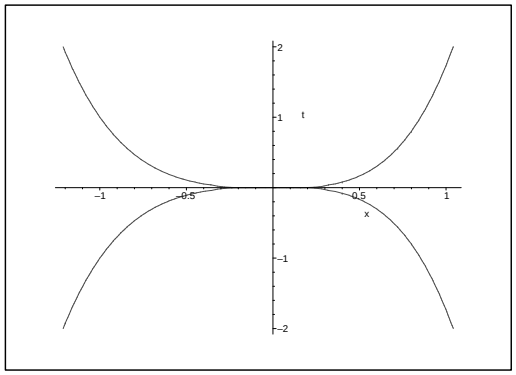


Abbildung 5: $\mathcal{F} = \mathrm{V}(P(x,t))$.

Weiters gilt $P(0,0) = 0$. Der Ursprung ist der einzige singuläre Punkt der ebenen Kurve

$$\mathcal{F} = \mathrm{V}(P) \subseteq \mathbb{R}^2$$

(siehe Abbildung 5). Damit ist $(0,0)$ kein normaler Punkt von $\mathcal{F}$. Tatsächlich besitzt $\mathcal{F}$ in $(0,0)$ zwei verschiedene Zweige. Einer der beiden Zweige ist gegeben durch die algebraische Potenzreihe g (siehe Abbildung 6).

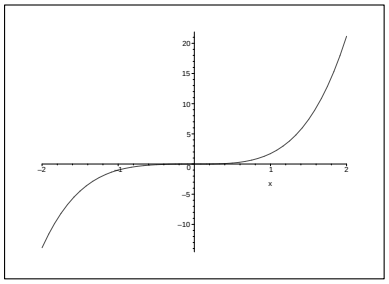


Abbildung 6: $g(x) = x^3\sqrt{1+x+x^2}, x \in \mathbb{R}$.

Wir wissen nun, dass der Ring

$$R := \mathbb{R}[x,t]/\langle P\rangle$$

kein normaler Ring ist (wohl aber reduziert). Das Element $y_2 := \frac{t}{x^3} \in \text{Quot}(R)$ ist ganz über R, denn y_2 erfüllt die Ganzheitsgleichung $u^2-(1+x+x^2) = 0$. Tatsächlich ergibt sich für die Normalisierung von R:

$$\begin{aligned}\tilde{R} &= \mathbb{R}[x,y_1,y_2]/\langle y_1^2 - x^6(1+x+x^2), y_2^2-1-x-x^2, y_1-x^3y_2\rangle \\ &\cong \mathbb{R}[x,y_1,y_2]/\langle y_2^2-1-x-x^2, y_1-x^3y_2\rangle \\ &\cong \mathbb{R}[x,y_2]/\langle y_2^2-1-x-x^2\rangle\end{aligned}$$

Bemerkung: SINGULAR liefert für die Normalisierung dasselbe Resultat:

$$\begin{aligned}\pi : \mathrm{V}(T(1)^2 - T(2)^2 + T(1) + 1) \subseteq \mathbb{R}^2 &\longrightarrow \mathcal{F}, \\ (T(1),T(2)) &\longrightarrow (T(1), T(1)^3T(2)).\end{aligned}$$

Damit ist

$$\begin{aligned}H &= (y_2^2-1-x-x^2, y_1-x^3y_2), \\ G &= y_1\end{aligned}$$

ein Code für unsere algebraische Potenzreihe g. Dabei muss man jedoch beachten, dass dieser Code noch nicht zentriert ist, genauer: Da wir nach dem Beweis des letzten Satzes wissen, dass nach unserer Konstruktion des Codes stets $y_1 = g$ gelten soll, hat das algebraische Gleichungssystem $H(x,h(x)) = 0$, d.h.

$$\begin{aligned}y_2^2-1-x-x^2 &= 0, \\ y_1-x^3y_2 &= 0,\end{aligned}$$

nur dann eine eindeutige Lösung mit $h_1(x) = g(x)$, wenn $h_2(x)$ gleich $\sqrt{1+x+x^2}$ ist, d.h., wenn wir den Code im Punkt $(0,0,+1)$ betrachten! Man kann leicht nachprüfen, dass $(H,G) = ((y_2^2-1-x-x^2, y_1-x^3y_2), y_1)$ im Punkt $(0,0,1)$ dann tatsächlich einen Familiencode für $g(x) = x^3\sqrt{1+x+x^2}$ darstellt.

Man erhält einen Code für g im Punkt $(0,0,0)$, indem man die Taylorentwicklung von H im Punkt $(0,0,0)$ betrachtet. Es ergibt sich:

$$\begin{aligned}H &= ((y_2+1)^2-1-x-x^2, y_1-x^3(y_2+1)) \\ &= (y_2^2+2y_2-x-x^2, y_1-x^3y_2-x^3), \\ G &= y_1.\end{aligned}$$

Beispiel 3.5. In diesem Beispiel wollen wir einen zentrierten Code für die Potenzreihe

$$g := (x^2 + x)\sqrt{1 + x^2} = x + x^2 + \frac{1}{2}x^3 + \ldots \in \mathbb{R}[\![x]\!]$$

finden. Klarerweise ist g eine algebraische Potenzreihe. Weiters ist g gerade einer der beiden Zweige der nichtnormalen ebenen Kurve

$$\mathcal{G} = \mathrm{V}(t^2 - (x^2 + x)^2(1 + x^2))$$

durch den Ursprung (siehe Abbildungen 7 und 8).

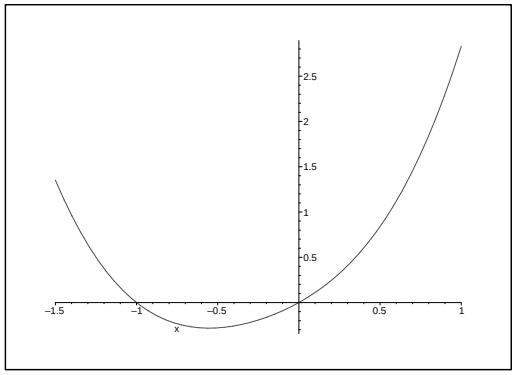


Abbildung 7: $g(x) = (x^2 + x)\sqrt{1 + x^2}, x \in \mathbb{R}$.

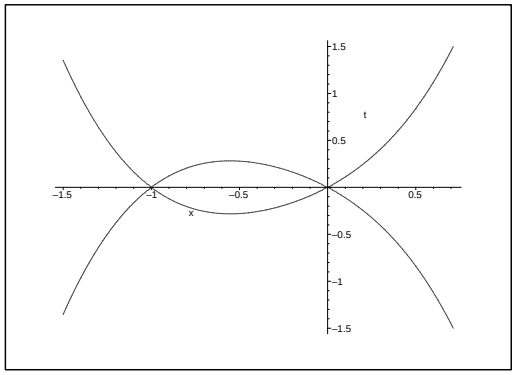


Abbildung 8: $\mathcal{G} = \mathrm{V}(t^2 - (x^2 + x)^2(1 + x^2))$.

Wir betrachten dazu den Ring

$$R := \mathbb{R}[x, t]/\langle t^2 - (x^2 + x)^2(1 + x^2)\rangle.$$

Dieser ist reduziert, jedoch nicht normal. Das Computeralgebrasystem SINGULAR liefert für die Normalisierung von R:

$$\pi : \tilde{\mathcal{G}} = \mathrm{V}(x^2 - y_2^2 + 1) \longrightarrow \mathcal{G}, (x, y_2) \to (x, y_2^3 + xy_2 - y_2).$$

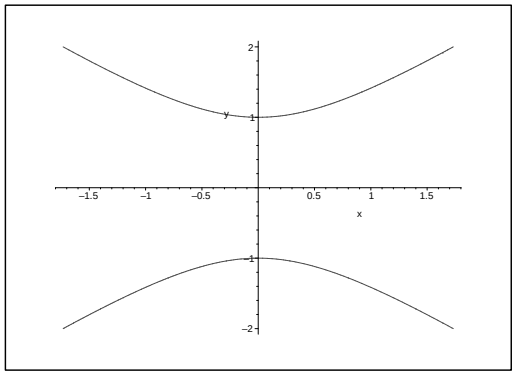


Abbildung 9: $\tilde{\mathcal{G}} = \mathrm{V}(x^2 - y_2^2 + 1)$.

Bemerkung: Die Normalisierung $\tilde{\mathcal{G}} = \mathrm{V}(x^2 - y_2^2 + 1)$ von $\mathcal{G}$ ist tatsächlich eine normale ebene Kurve (siehe Abbildung 9). Man kann leicht nachprüfen, dass

$$\begin{aligned} H &= (x^2 - y_2^2 + 1, y_1 - y_2^3 - xy_2 + y_2), \\ G &= y_1 \end{aligned}$$

ein Familiencode von g im Punkt $(0, 0, 1)$ und

$$\begin{aligned} H &= (x^2 - y_2^2 - 2y_2, y_1 - y_2^3 - y_2^2 - xy_2 - x), \\ G &= y_1 \end{aligned}$$

ein Familiencode von g im Ursprung ist.

Beispiel 3.6. Natürlich können wir mit demselben Verfahren auch Codes für algebraische Potenzreihen in mehreren Variablen konstruieren:
Sei etwa

$$g(x_1, x_2, x_3) = x_1 x_3 \sqrt{1 + x_1^2} - x_2^2 \in K[\![x_1, x_2, x_3]\!].$$

Dann ergibt sich für die Normalisierung des Ringes

$$R := K[x_1, x_2, x_3, t]/\langle (t + x_2^2)^2 - x_1^2 x_3^2 (1 + x_1^2) \rangle$$

mit Hilfe von SINGULAR:

$$\begin{aligned} \tilde{X} = \mathrm{V}(x_1^2 - y_2^2 + 1) \subseteq K^4 \quad &\longrightarrow \quad X = \mathrm{V}((t + x_2^2)^2 - x_1^2 x_3^2 (1 + x_1^2)) \subseteq K^4, \\ (x_1, x_2, x_3, y_2) \quad &\longrightarrow \quad (x_1, x_2, x_3, x_1 x_3 y_2 - x_2^2). \end{aligned}$$

Wie man leicht nachprüfen kann, ist also

$$\begin{aligned} H &= (x_1^2 - y_2^2 + 1, y_1 - x_1 x_3 y_2 + x_2^2), \\ G &= y_1 \end{aligned}$$

ein Familiencode von g im Punkt $(0, 0, 0, 0, 1) \in K^5$. Folglich ist

$$\begin{aligned} H &= (x_1^2 - y_2^2 - 2y_2, y_1 - x_1 x_3 y_2 - x_1 x_3 + x_2^2), \\ G &= y_1 \end{aligned}$$

ein Code von g im Ursprung.

4 Rechnen mit Codes algebraischer Potenzreihen

Wie wir in Kapitel 2 gesehen haben, bilden die algebraischen Potenzreihen einen Ring. Weiters ist auch die Komposition von algebraischen Potenzreihen wieder algebraisch. In diesem Abschnitt wollen wir untersuchen, wie man diese Verknüpfungen mit Hilfe von Codes durchführt.

Betrachtet man mehrere algebraische Potenzreihen $g_1, \ldots, g_r$ gleichzeitig, so ist es vorteilhaft, mit nur einem gemeinsamen Muttercode (und mehreren Vatercodes) für alle Reihen zu arbeiten. Wie erhält man aber einen derartigen Muttercode?
Seien $H^j \in K[x, y^j]^{p_j}$ für $j = 1, \ldots, r$ die r verschiedenen Muttercodes der algebraischen Potenzreihen $g_1, \ldots, g_r$. Dabei seien $y^j = (y_1^j, \ldots, y_{p_j}^j)$ für $j = 1, \ldots, r$ disjunkte Mengen von Variablen. Das *direkte Produkt* H der H^j's ist durch den Zeilenvektor $H = (H^1, \ldots, H^r) \in \prod_{j=1}^r K[x, y^j]^{p_j} \cong K[x, y]^p$ gegeben, wobei y aus der Menge aller y^j besteht und $p = \sum_{j=1}^r p_j$ ist.

Lemma 4.1. *Der oben konstruierte Zeilenvektor $H \in K[x, y]^p$ ist wieder ein Muttercode.*

Beweis. Die erste Bedingung $H(0, 0) = (H^1, \ldots, H^r)(0, 0) = 0$ ist klarerweise erfüllt, da die einzelnen H^i's diese Bedingung erfüllen. Auch die zweite Bedingung $D_y H(0, 0) \in \mathrm{Gl}_p(K)$ ist erfüllt, denn die Jacobi-Matrix $D_y H$ ist eine Blockdiagonalmatrix, wobei die einzelnen Blöcke gerade die Jacobi-Matrizen $D_{y^j} H^j(0, 0)$ der einzelnen Muttercodes sind. Diese sind jedoch nach Voraussetzung im Ursprung invertierbar, und damit ist auch $D_y H(0, 0)$ invertierbar. □

Weiters gilt: Der durch den Muttercode $H(x, y)$ eindeutig bestimmte Babyreihenvektor $h = (h^1, \ldots, h^r)$ ist gerade die Ansammlung aller Babyreihenvektoren $h^j = (h_1^j, \ldots, h_{p_j}^j) \in K[\![x]\!]^{p_j}$ der Muttercodes H^j.

Der Übergang zum direkten Produkt von Muttercodes ermöglicht uns also, dass die von uns betrachteten algebraischen Potenzreihen $g_1, \ldots, g_r$ alle den gleichen Muttercode $H(x, y)$ und Babyreihenvektor $h(x)$ haben.

4.1 Addition, Subtraktion und Multiplikation von algebraischen Potenzreihen

Gegeben seien zwei algebraische Potenzreihen g_1 und g_2 in $K[\![x]\!]$ mit Familiencodes $(H^1, G^1) \in K[x, y^1]^{p_1} \times K[x, y^1]$ bzw. $(H^2, G^2) \in K[x, y^2]^{p_2} \times K[x, y^2]$ und ein Polynom $a \in K[x]$. Weiters sei $H = (H^1, H^2)$ der gemeinsame Muttercode der Reihen g_1 und g_2 (vgl. Konstruktion oben). Dann sind

$$(H, G^1 \pm G^2), \quad (H, a \cdot G^1) \quad \text{bzw.} \quad (H, G^1 \cdot G^2)$$

klarerweise Familiencodes der algebraischen Potenzreihen

$$g_1 \pm g_2, \quad a \cdot g_1 \quad \text{und} \quad g_1 \cdot g_2.$$

Beispiel 4.1. In diesem Beispiel suchen wir einen Code für die algebraische Potenzreihe

$$g := 2x\sqrt{1+x} + 5x^3\sqrt{1+x}(\sqrt[3]{1+x} - 1).$$

Dazu zerlegen wir g in uns bereits bekannte algebraische Potenzreihen, d.h. $g = a \cdot g_1 + b \cdot g_1 \cdot g_2$ mit

$$a := 2,\ b := 5x^2,\ g_1 := x\sqrt{1+x},\ g_2 := \sqrt[3]{1+x} - 1.$$

Wie wir bereits aus Beispiel 3.3 wissen, ist

$$(H^1, G^1) = ((-y_2^3 - 3y_2^2 - 2y_2 + y_1, -y_2^2 - 2y_2 + x), y_1)$$

ein Code für die algebraische Potenzreihe g_1. Weiters ist nach Beispiel 3.1

$$(H^2, G^2) = (x - y_3^3 - 3y_3^2 - 3y_3, y_3)$$

ein Code für die algebraische Potenzreihe g_2. Nach der Konstruktion am Beginn dieses Kapitels ist

$$(H, G) = ((-y_2^3 - 3y_2^2 - 2y_2 + y_1, -y_2^2 - 2y_2 + x, x - y_3^3 - 3y_3^2 - 3y_3), (y_1, y_3))$$

daher ein Familiencode für $(g_1, g_2) \in K[\![x]\!]^2$. Folglich ist nach obigen Überlegungen

$$\begin{aligned}(H_g, G_g) \quad = \quad & ((-y_2^3 - 3y_2^2 - 2y_2 + y_1, -y_2^2 - 2y_2 + x, x - y_3^3 - 3y_3^2 - 3y_3), \\ & 2y_1 + 5x^2 y_1 y_3)\end{aligned}$$

ein Code für die algebraische Potenzreihe g.

4.2 Komposition von algebraischen Potenzreihen

Gegeben seien algebraische Potenzreihen $g_1, \ldots, g_n, f$ mit $g_1(0) = 0, \ldots, g_n(0) = 0$ und zugehörige Codes $(H_{g_1}, G_{g_1}) \in K[x, y^1]^{p_1} \times K[x, y^1], \ldots, (H_{g_n}, G_{g_n}) \in K[x, y^n]^{p_n} \times K[x, y^n], (H_f, G_f) \in K[x, z]^r \times K[x, z]$.
Gesucht sei ein Code der algebraischen Potenzreihe

$$f(g_1, \ldots, g_n) \in K\langle x_1, \ldots, x_n \rangle.$$

Lemma 4.2. *Sei $H_g = (H^1, \ldots, H^n) \in \prod_{j=1}^n K[x, y^j]^{p_j} \cong K[x, y]^p$ der gemeinsame Muttercode der Reihen $g_1, \ldots, g_n$ (vgl. Konstruktion am Beginn des Kapitels), dann ist*

$$\begin{aligned} H \quad &= \quad (H_f(G_{g_1}, \ldots, G_{g_n}, z), H_g(x, y)) \in K[x, z]^r \times K[x, y]^p, \\ G \quad &= \quad G_f(x, z) \in K[x, z] \end{aligned}$$

ein Code für die algebraische Potenzreihe $f(g_1, \ldots, g_n)$.

Beweis. Dazu zuerst eine kleine Vorüberlegung: Da die $(H_{g_1}, G_{g_1}), \ldots, (H_{g_n}, G_{g_n})$ Familiencode der algebraischen Potenzreihen $g_1, \ldots, g_n$ sind, müssen sie die Bedingung

$$G_{g_j}(x, h^j(x)) = g_j,\ j = 1, \ldots, n,$$

erfüllen. Wertet man diese Bedingung in $x = 0$ aus, so ergibt sich:

$$G_{g_j}(0, h^j(0)) = g_j(0),\ j = 1, \ldots, n.$$

Aber es gilt $h^j(0) = 0$ und $g_j(0) = 0$ (vgl. Voraussetzungen). Daraus folgt

$$G_{g_j}(0, 0) = 0,\ j = 1, \ldots, n.$$

Somit ergibt sich für $H = (H_f(G_1, \ldots, G_n, z), H_g(x, y))$ sofort

$$\begin{aligned} H(0,0,0) &= (H_f(G_1(0,0), \ldots, G_n(0,0), 0), H_{g_1}(0,0), \ldots, H_{g_n}(0,0)) \\ &= (H_f(0, \ldots, 0, 0), 0, \ldots, 0) = 0. \end{aligned}$$

Der Polynomvektor H erfüllt auch die zweite Bedingung $D_{(z,y)}H(0,0,0) \in \mathrm{Gl}_{n+r}(K)$ für einen Muttercode, denn die Matrix $D_{(z,y)}H$ hat folgende Gestalt:

$$D_{(z,y)}H = \begin{pmatrix} \frac{\partial H_f(G_{g_1}(x,y),\ldots,G_{g_n}(x,y),z)}{\partial z} & \frac{\partial H_f(G_{g_1}(x,y),\ldots,G_{g_n}(x,y),z)}{\partial z} \\ \frac{\partial H_g(x,y)}{\partial z} & \frac{\partial H_g(x,y)}{\partial y} \end{pmatrix}.$$

Der gemeinsame Muttercode H_g der H_{g_j}'s hängt nicht von z ab und damit ist $\frac{\partial H_g(x,y)}{\partial z} = 0$. Nach Voraussetzung ist die Untermatrix $\frac{\partial H_g(x,y)}{\partial y}$ im Punkt $(x, y) = (0, 0)$ invertierbar. Damit bleibt noch zu zeigen:

$$\frac{\partial H_f(G_{g_1}(x,y), \ldots, G_{g_n}(x,y), z)}{\partial z} \in \mathrm{Gl}_r(K).$$

Wie wir aber in unserer Vorüberlegung gesehen haben, gilt $G_{g_j}(0,0) = 0,\ j = 1, \ldots, n$, und daraus folgt:

$$\frac{\partial H_f(G_{g_1}(x,y), \ldots, G_{g_n}(x,y), z)}{\partial z}(0,0,0) = \frac{\partial H_f(0, \ldots, 0, 0)}{\partial z}.$$

Diese Matrix ist aber invertierbar, da H_f ein Muttercode von f ist. Die Bedingung

$$G(x, h(x)) = f(g_1(x), \ldots, g_n(x))$$

für einen Familiencode ist klarerweise erfüllt. □

Beispiel 4.2. Seien $x = (x_1, x_2, x_3)$ und

$$\begin{aligned} f &:= x_1 x_3 \sqrt{1 + x_1^2} - x_2^2, \\ g_1 &:= x_1^2 + x_2^2 + x_3^2, \\ g_2 &:= x_3 \sqrt{1 + x_1 + x_2^2}, \\ g_3 &:= \frac{x_2^2}{x_1 x_3 + 1}. \end{aligned}$$

Dann sind

$$\begin{aligned} (H_f, G_f) &= ((x_1^2 - z_2^2 - 2z_2, z_1 - x_1 x_3 z_2 - x_1 x_3 + x_2^2), z_1), \\ (H_{g_1}, G_{g_1}) &= (y_1 - x_1^2 - x_2^2 - x_3^2, y_1), \\ (H_{g_2}, G_{g_2}) &= ((x_1 - y_3^2 - 2y_3 + x_2^2, y_2 - x_3 - y_3 x_3), y_2), \\ (H_{g_3}, G_{g_3}) &= (y_4 x_1 x_3 + y_4 - x_2^2, y_4) \end{aligned}$$

Codes von f, g_1, g_2 und g_3. Aus Lemma 4.2 folgt, dass

$$\begin{aligned} (H, G) = ((&y_1^2 - z_2^2 - 2z_2, z_1 - y_1 y_4 z_2 - y_1 y_4 + y_2^2, y_1 - x_1^2 - x_2^2 - x_3^2, \\ &x_1 - y_3^2 - 2y_3 + x_2^2, y_2 - x_3 - y_3 x_3, y_4 x_1 x_3 + y_4 - x_2^2), z_1) \end{aligned}$$

ein Code für die algebraische Potenzreihe

$$f(g_1, g_2, g_3) = (x_1^2 + x_2^2 + x_3^2)\frac{x_2^2}{x_1 x_3 + 1}\sqrt{1 + (x_1^2 + x_2^2 + x_3^2)^2} - x_3^2(1 + x_1 + x_2^2)$$

ist.

Im Appendix sind für einige weitere algebraische Potenzreihen Codes angegeben.

5 Codes für Moduln von algebraischen Potenzreihen

In diesem Kapitel seien algebraische Potenzreihen $g_1, \ldots, g_r \in K[\![x]\!]^s$ mit zugehörigem Muttercode $H \in K[x,y]^p$, Vatercode $G \in K[x,y]^{s\times r}$ und Babyreihenvektor $h \in K[\![x]\!]^p$ gegeben. (Vergleiche die Konstruktion am Beginn von Kapitel 4 und Lemma 4.1.)

Lemma 5.1. *Seien $\langle (y_i - h_i)\cdot e_l, g_k\rangle$ und $\langle H_i \cdot e_l, G_k\rangle$ jene Untermoduln von $K[\![x,y]\!]^s$, die von $(y_i - h_i)\cdot e_l$ und g_k bzw. $H_i \cdot e_l$ und G_k für $1 \le i \le p$, $1 \le l \le s$, $1 \le k \le r$ erzeugt werden. Dann gilt:*

$$\langle (y_i - h_i)\cdot e_l, g_k\rangle = \langle H_i \cdot e_l, G_k\rangle.$$

Beweis. Sei $<_\eta$ eine beliebige Monomordnung auf $\mathbb{N}^n \times \{1,\ldots,s\}$. Dazu wählen wir eine Erweiterung $<_\varepsilon$ von $<_\eta$ auf $\mathbb{N}^{n+p} \times \{1,\ldots,s\}$, die bzgl. $\mathbb{N}^p$ gradkompatibel ist und die $y_i < x_j$ für alle $1 \le i \le p$ und $1 \le j \le n$ erfüllt. Da $h_i \in K[\![x]\!]$ und $h_i(0) = 0$, folgt daraus, dass für die von uns gewählte Termordnung ε für alle $1 \le i \le p$ und $1 \le l \le s$ gilt: $y_i \cdot e_l <_\varepsilon \text{in}(h_i)\cdot e_l$. Ohne Beschränkung der Allgemeinheit nehmen wir noch an (vgl. Definition 3.1), dass das Initialmonom von H_i bzgl. der Monomordnung $<_\varepsilon$ für alle $1 \le i \le p$ gerade y_i ist.
Aus $H_i(x, h_i(x)) = 0$ ergibt sich, dass h_i eine Nullstelle von H_i ist, also ist $y_i - h_i$ ein Faktor von H_i. Daraus folgt $\langle H_i\rangle \subset \langle y_i - h_i\rangle \subseteq K[\![x,y]\!]$.
Weiters gilt: Die Initialmodulen von $\langle H_i\rangle$ und $\langle y_i - h_i\rangle$ stimmen überein, denn sie werden auf Grund unserer Wahl von $< \varepsilon$ beide von $y_1, \ldots, y_p$ erzeugt. Nach Korollar 2.3 folgt daher $\langle H_i\rangle = \langle y_i - h_i\rangle$.
Man erhält die algebraische Potenzreihe g_k, indem man im Vatercode G_k an Stelle von y_i die Babyreihe h_i einsetzt. Daher sind die Untermodulen $\langle g_1, \ldots, g_r\rangle$ und $\langle G_1, \ldots, G_r\rangle$ modulo $\langle y_i - h_i\rangle = \langle H_i\rangle$ kongruent. □

Im Folgenden werden wir $J = \langle H_i \cdot e_l, G_k\rangle$, oder auch seine polynomialen Erzeuger $H_i \cdot e_l$ und G_k, als *Code des Untermoduls $I = \langle g_k\rangle \subseteq K[\![x]\!]^s$ in $K[\![x,y]\!]^s$* bezeichnen.

Bemerkung. Auf Grund des letzten Lemmas gilt $J = \langle (y_i - h_i)\cdot e_l, g_k\rangle$. Daraus folgt

$$J \cap K[\![x]\!]^s = I.$$

Lemma 5.2. *Sei $<_\eta$ eine Monomordnung auf $\mathbb{N}^n \times \{1,\ldots,s\}$ und $<_\varepsilon$ eine Erweiterung auf $\mathbb{N}^{n+p}\times\{1,\ldots,s\}$, die bzgl. $\mathbb{N}^p$ gradkompatibel ist und die $y_i\cdot e_l <_\varepsilon \text{in}(h_i)\cdot e_l$ und $y_i < x_j$ für alle $1 \le i \le p$, $1 \le l \le s$, $1 \le j \le n$ erfüllt. Weiters seien $J = \langle H_i \cdot e_l, G_k\rangle$ und $I = \langle g_k\rangle$ Untermoduln von $K[\![x,y]\!]^s$ bzw. $K[\![x]\!]^s$. Dann gilt:*

$$\text{in}(J) \cap K[\![x]\!]^s = \text{in}(I).$$

Beweis. Wähle eine minimale Standardbasis von J, die die Vektoren $H_i \cdot e_l$ enthält. (Dies ist möglich, da nach Voraussetzung $y_i \cdot e_l <_\varepsilon \text{in}(h_i)\cdot e_l$ für alle i und alle l gilt, und wir o.B.d.A. $\text{in}(H_i) = y_i$ annehmen können.)
Mit $\tilde{G}_{k'}$, $1 \le k' \le r'$, bezeichnen wir die restlichen Vektoren dieser minimalen Standardbasis von J. Aus der Minimalität folgt, dass deren Initialmonomvektoren in $K[\![x]\!]^s$ liegen. Setze nun für $1 \le k' \le r'$: $\tilde{g}_{k'} = \tilde{G}_{k'}(x, h(x))$.
Auf Grund der Wahl von $<_\varepsilon$ und der Tatsache, dass $\text{in}(\tilde{G}_{k'})$ ein Element von $K[\![x]\!]^s$ ist (und die Elemente $H_i \cdot e_l$ und $\tilde{G}_{k'}$ eine Standardbasis von J bilden), ergibt sich, dass die Initialmonomvektoren von $\tilde{G}_{k'}$ und $\tilde{g}_{k'}$ übereinstimmen.
Nach Konstruktion gilt $\tilde{g}_{k'} \in J \cap K[\![x]\!]^s = I$. Folglich ist $\tilde{g}_{k'}$ eine Standardbasis von I und es gilt $\text{in}(J) \cap K[\![x]\!]^s = \text{in}(I)$. □

6 Konstruktion einer Standardbasis

Das folgende Resultat ist eine direkte Folge aus Mora's Tangentialkegel Algorithmus. Es liefert uns ein Verfahren zur Konstruktion des Codes einer Standardbasis eines Moduls, der von algebraischen Potenzreihenvektoren erzeugt wird.

6.1 Konstruktion einer Standardbasis

Satz 6.1. *Sei I der von den algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ (die durch ihren Familiencode gegeben sind) erzeugte Untermodul von $K[\![x]\!]^s$. Weiters sei eine Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$ gegeben. Dann existiert ein endlicher Algorithmus, der aus den Familiencodes der $g_1, \ldots, g_r$ einen Familiencode einer Standardbasis von I bzgl. $<_\eta$ berechnet. Speziell ist es also möglich, den Initialmodul* $\mathrm{in}(I)$ *von I zu berechnen.*

Beweis. Die algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ seien durch Muttercode $H \in K[x,y]^p$, Vatercode $G \in K[x,y]^{s \times r}$ und Babyreihenvektor $h \in K[\![x]\!]^p$ gegeben. Wir erweitern nun die Monomordnung $<_\eta$ auf eine Monomordnung $<_\varepsilon$ auf $\mathbb{N}^{n+p} \times \{1, \ldots, s\}$, die auf $\mathbb{N}^p$ gradkompatibel ist und die für alle i, p und j, $y_i \cdot e_l <_\varepsilon \mathrm{in}(h_i) \cdot e_l$ und $y_i < x_j$, erfüllt.
Da $J = \langle H_i \cdot e_l, G_k \rangle$ von Polynomen erzeugt wird, können wir Mora's Tangentialkegel Algorithmus verwenden, um eine polynomiale Standardbasis von J zu konstruieren. Wie in Lemma 5.2 können wir eine minimale Standardbasis wählen, die aus den Vektoren $H_i \cdot e_l$, mit $\mathrm{in}(H_i \cdot e_l) = y_i \cdot e_l$, und weiteren polynomialen Vektoren $\tilde{G}_1, \ldots, \tilde{G}_{r'} \in K[x,y]^s$, mit Initialmonomvektoren in $K[\![x]\!]^s$, besteht. Wir setzen nun für $1 \leq k' \leq r'$: $\tilde{g}_{k'} = \tilde{G}_{k'}(x,h)$. Dann bilden die $\tilde{G}_1, \ldots, \tilde{G}_{r'}$ gerade den Vatercode der algebraischen Potenzreihenvektoren $\tilde{g}_1, \ldots, \tilde{g}_{r'}$. Auf Grund von Lemma 5.2 bilden die $\tilde{g}_{k'}$'s eine Standardbasis des Moduls I. □

6.2 Beispiele

Beispiel 6.1. In diesem Beispiel wollen wir zeigen, dass

$$g_1 := x_1 x_3 \sqrt{1 + x_1^2} - x_2^2,\ g_2 := \frac{x_3}{\sqrt{1 + x_1 x_2}},$$

bereits eine Standardbasis bzgl. der graduiert lexikographischen Ordnung $<_\eta$ auf $\mathbb{N}^3$ mit $x_1 <_\eta x_2 <_\eta x_3$ des von ihnen erzeugten Ideals

$$I = \langle g_1, g_2 \rangle = \langle x_1 x_3 \sqrt{1 + x_1^2} - x_2^2, \frac{x_3}{\sqrt{1 + x_1 x_2}} \rangle \subseteq K[\![x_1, x_2, x_3]\!]$$

bilden. Man kann leicht nachprüfen, dass

$$\begin{aligned} ((H_1^1, H_2^1), G^1) &= ((y_1 - x_1 x_3 y_2 - x_1 x_3 + x_2^2, y_2 - \frac{1}{2} x_1^2 + \frac{1}{2} y_2^2), y_1), \\ ((H_1^2, H_2^2), G^2) &= ((y_3 + y_3 y_4 - x_3, y_4 + \frac{1}{2} y_4^2 - \frac{1}{2} x_1 x_2), y_3) \end{aligned}$$

Codes der algebraischen Potenzreihen $g_1, g_2 \in K[\![x_1, x_2, x_3]\!]$ sind. Wir erweitern die Monomordnung $<_\eta$ auf die graduiert lexikographische Ordnung $<_\varepsilon$ auf $\mathbb{N}^{3+4}$ mit

$y_1 <_\varepsilon y_2 <_\varepsilon y_3 <_\varepsilon y_4 <_\varepsilon x_1 <_\varepsilon x_2 <_\varepsilon x_3$. Die Ordnung $<_\varepsilon$ erfüllt die Voraussetzungen von Lemma 5.2. Daher betrachten wir nun das folgende Ideal

$$J = \langle H_1^1, H_2^1, H_1^2, H_2^2, G^1, G^2 \rangle \subseteq K[\![x_1, x_2, x_3, y_1, y_2, y_3, y_4]\!].$$

Dieses Ideal wird von Polynomen erzeugt und somit können wir Mora's Tangentialkegel Algorithmus zur Berechnung einer Standardbasis von J verwenden. Da Mora's Tangentkegel rechnerisch recht aufwendig ist, er aber in SINGULAR implementiert ist, werde ich dies für die Berechnung einer Standardbasis von J nützen:

```
>ring R=0,(y(1..4),x(1..3)),ds;
>poly H11=y(1)-x(1)*x(3)*y(2)-x(1)*x(3)+x(2)*x(2);
>poly H12=y(2)-1/2*x(1)*x(1)+1/2*y(2)*y(2);
>poly H21=y(3)+y(3)*y(4)-x(3);
>poly H22=y(4)+1/2*y(4)*y(4)-1/2*x(1)*x(2);
>poly G1=y(1); poly G2=y(3);
>ideal J=H11,H12,H21,H22,G1,G2;
>ideal Jstd=std(J); Jstd;
   Jstd[1]=y(1)
   Jstd[2]=y(2)-1/2*x(1)*x(1)+1/2*y(2)*y(2)
   Jstd[3]=y(3)
   Jstd[4]=y(4)+1/2*y(4)*y(4)-1/2*x(1)*x(2)
   Jstd[5]=x(3)-y(3)*y(4)
   Jstd[6]=x(2)*x(2)-x(1)*x(3)-y(2)*x(1)*x(3)
```

Dieser liefert uns folgende Standardbasis von J bzgl. $<_\varepsilon$:

$$y_1,\ H_2^1,\ y_3,\ H_2^2,\ x_3 - y_3y_4,\ x_2^2 - x_1x_3 - y_2x_1x_3.$$

Man kann leicht nachprüfen, dass auch

$$H_1^1,\ H_2^1,\ H_1^2,\ H_2^2,\ x_3 - y_3y_4,\ x_2^2 - x_1x_3 - y_2x_1x_3$$

eine Standardbasis von J bzgl. $<_\varepsilon$ ist ($H_1^1 = 1 \cdot y_1 + 1 \cdot (x_2^2 - x_1x_3 - y_2x_1x_3)$, $H_1^2 = 1 \cdot y_3 + (-1) \cdot (x_3 - y_3y_4)$). Diese Standardbasis hat nun die im Beweis von Satz 6.1 gewünschte Form. Daher setzen wir wie in den Beweisen von Lemma 5.2 und Satz 6.1

$$\tilde{G} = (\tilde{G}_1, \tilde{G}_2) := (x_3 - y_3y_4, x_2^2 - x_1x_3 - y_2x_1x_3).$$

Dieses $\tilde{G}$ formt den Vatercode der algebraischen Potenzreihen

$$\tilde{g} := \tilde{G}(x, h) = (\tilde{g}_1, \tilde{g}_2) = (x_3 - h_3h_4, x_2^2 - x_1x_3 - h_2x_1x_3),$$

die eine Standardbasis von I bilden. Setzt man nun noch $h_1 = g_1$, $h_2 = -1+\sqrt{1+x_1^2}$, $h_3 = g_2$ und $h_4 = -1 + \sqrt{1 + x_1x_2}$ ein, so ergibt sich

$$\tilde{g} = (g_2, -g_1).$$

Damit ist gezeigt, dass g_1 und g_2 bereits eine Standardbasis von $I = \langle g_1, g_2 \rangle$ sind.

Beispiel 6.2. Wir betrachten die algebraischen Potenzreihen $g_1 := x_1x_3\sqrt{1+x_1^2} - x_2^2$ und $g_1 := x_1x_3\sqrt{1+x_1^2} + x_2^2$. Klarerweise bilden diese bzgl. der lexikographischen

Ordnung $<_\eta$ auf $\mathbb{N}^3$ mit $x_3 < x_2 < x_1$ keine Standardbasis des von ihnen erzeugten Ideals

$$I = \langle g_1, g_2 \rangle \subseteq K[\![x_1, x_2, x_3]\!].$$

Daher wollen wir in diesem Beispiel den Code einer Standardbasis von I berechnen. Als Erweiterung von $<_\eta$ wählen wir die Blockordnung $<_\varepsilon = (<_\eta, <_{deglex})$ auf $\mathbb{N}^{3+4}$, die durch

$$\begin{aligned} x^\alpha y^\beta <_\varepsilon x^{\alpha'} y^{\beta'} \quad :\Longleftrightarrow \quad & x^\alpha <_\eta x^{\alpha'}, \\ & \text{oder } (x^\alpha = x^{\alpha'} \text{ und } y^\beta <_{deglex} y^{\beta'}) \end{aligned}$$

definiert ist, wobei $y_1 <_{deglex} y_2 <_{deglex} y_3$, d.h.

$$y_1 <_\varepsilon y_2 <_\varepsilon y_3 <_\varepsilon y_4 <_\varepsilon y_1^2 <_\varepsilon y_1 y_2 <_\varepsilon y_2^2 <_\varepsilon \ldots <_\varepsilon y_1^3 <_\varepsilon \ldots <_\varepsilon x_3 <_\varepsilon \ldots$$

$$\ldots <_\varepsilon x_2 <_\varepsilon \ldots <_\varepsilon x_2^2 <_\varepsilon \ldots <_\varepsilon x_1 <_\varepsilon \ldots.$$

Man kann leicht überprüfen, dass

$$\begin{aligned} ((H_1^1, H_2^1), G^1) &= ((y_1 + x_2^2 - x_1x_3 - x_1x_3y_2, y_2 + \frac{1}{2}y_2^2 - \frac{1}{2}x_1^2), y_1), \\ ((H_1^2, H_2^2), G^2) &= ((y_3 - x_2^2 - x_1x_3 + x_1x_3y_4, y_4 - \frac{1}{2}y_4^2 + \frac{1}{2}x_1^2), y_3) \end{aligned}$$

Familiencodes von g_1 und g_2 sind und dass die Monomordnung $<_\varepsilon$ die Voraussetzungen von Lemma 5.2 erfüllt. Daher betrachten wir das Ideal

$$J = \langle H_1^1, H_2^1, H_1^2, H_2^2, G^1, G^2 \rangle.$$

Wir erhalten mit Hilfe von Mora's Tangentialkegel Algorithmus folgende Standardbasis von J bzgl. $<_\varepsilon$:

$$H_1^1, H_2^1, H_1^2, H_2^2, x_1x_3, x_2^2 - x_1x_3 - x_1x_3y_2.$$

Dem Beweis von Satz 6.1 folgend setzen wir

$$\tilde{G} = (\tilde{G}_1, \tilde{G}_2) := (x_1x_3, x_2^2 - x_1x_3 - x_1x_3y_2)$$

und

$$\tilde{g} := \tilde{G}(x, h) = (x_1x_3, x_2^2 - x_1x_3 - x_1x_3h_2) = \left(x_1x_3, x_2^2 - x_1x_3\sqrt{1 + x_1^2}\right).$$

Nach Satz 6.1 ist $\tilde{g}$ eine Standardbasis des Ideals $I = \langle x_1x_3\sqrt{1 + x_1^2} - x_2^2, x_1x_3\sqrt{1 + x_1^2} + x_2^2 \rangle$ bzgl. $<_\varepsilon$ und

$$(H, \tilde{G}) = (y_2 + \frac{1}{2}y_2^2 - \frac{1}{2}x_1^2, (x_1x_3, x_2^2 - x_1x_3 - x_1x_3y_2))$$

ein Code der Standardbasis $\tilde{g}$ von I.

Bemerkung. Die Standardbasis $\tilde{g}$ von I ist noch nicht reduziert. Die reduzierte Standardbasis von I ist $g' = \langle x_2^2, x_1x_3 \rangle$.

Beispiel 6.3. In diesem Beispiel wollen wir eine Standardbasis des von den algebraischen Potenzreihenvektoren

$$g_1 := x^3\sqrt{1+x+x^2}\cdot e_1 + x^2\cdot e_2,\ g_2 := (x+x^2)\cdot e_1 + x\sqrt{1+x}\cdot e_2$$

erzeugten Moduls $I := \langle g_1, g_2\rangle \subseteq K[\![x]\!]^2$ konstruieren. Dabei sei $K[\![x]\!]^2$ mit jener lexikographischen Ordnung $<_\eta = (<_{lex}, C)$ versehen, die durch

$$x^\alpha e_i <_\eta x^\beta e_j \ :\Longleftrightarrow\ (x^\alpha <_{lex} x^\beta \text{ oder } i > j)$$

definiert ist. (Dabei bedeutet $(<_{lex}, C)$, dass zuerst die Initialmonome der einzelnen Komponenten lexikographisch verglichen werden. Nur im Falle, dass diese übereinstimmen, wird dann der Initialmonomvektor durch die Nummerierung der Komponenten bestimmt. Für unsere Monomordnung $<_\eta$ bedeutet dies zum Beispiel, dass $\text{in}(x\cdot e_1 + x\cdot e_2) = x\cdot e_2$ ist.)
Man kann leicht nachprüfen, dass

$$\begin{aligned}(H^1, G^1) &= ((y_1 - x^3y_2 - x^3, y_2 - \frac{1}{2}x - \frac{1}{2}x^2 + \frac{1}{2}y_2^2, y_3 - x^2),\\ &\quad\ y_1\cdot e_1 + y_3\cdot e_2),\\ (H^2, G^2) &= ((y_4 - x - x^2, y_5 + \frac{1}{2}y_5^2 - \frac{1}{2}x, y_6 - y_5^3 - 3y_5^2 - 2y_5),\\ &\quad\ y_4\cdot e_1 + y_6\cdot e_2),\end{aligned}$$

Codes der algebraischen Potenzreihen g_1 und g_2 sind. Wir erweitern die Monomordnung $<_\eta$ auf die graduiert lexikographische Ordnung $<_\varepsilon = (<_{deglex}, C)$ auf $\mathbb{N}^{1+6}\times\{1,2\}$ mit $y_6 < y_5 < y_4 < y_3 < y_2 < y_1 < x$ (wobei wir die Priorität wiederum auf die Koeffizienten aller Komponenten richten). Diese Erweiterung erfüllt alle Voraussetzungen von Lemma 5.2. Daher betrachten wir das Ideal

$$J = \langle H_1^1 e_l, H_2^1 e_l, H_3^1 e_l, H_1^2 e_l, H_2^2 e_l, H_3^2 e_l, G^1, G^2\rangle \subseteq K[\![x,y]\!],$$

wobei $1 \le l \le 2$. Mit Hilfe des in SINGULAR implementierten Tangentialkegel Algorithmus' von Mora berechnen wir folgendermaßen eine Standardbasis von J bzgl. $<_\varepsilon$:

```
>ring R=0,(y(6..1),x),ds;
>poly H11=y(1)-x*x*x*y(2)-x*x*x;
>poly H12=y(2)-1/2*x-1/2*x*x+1/2*y(2)*y(2);
>poly H13=y(3)-x*x;
>poly H21=y(4)-x-x*x;
>poly H22=y(5)+1/2*y(5)*y(5)-1/2*x;
>poly H23=y(6)-y(5)*y(5)*y(5)-3*y(5)*y(5)-2*y(5);
>vector G1=[y(1),y(3)]; vector G2=[y(4),y(6)];
>vector s(1)=[H11,0]; vector s(2)=[0,H11];
>vector s(3)=[H12,0]; vector s(4)=[0,H12];
>vector s(5)=[H13,0]; vector s(6)=[0,H13];
>vector s(7)=[H21,0]; vector s(8)=[0,H21];
>vector s(9)=[H22,0]; vector s(10)=[0,H22];
>vector s(11)=[H23,0]; vector s(12)=[0,H23];
>module J=s(1..12),G1,G2;
>module Jstd=std(J);
```

Damit ergibt sich folgende Standardbasis von J bzgl. $<_\varepsilon$:

$$y_4 \cdot e_1 + y_6 \cdot e_2, y_1 \cdot e_1 + y_3 \cdot e_2,$$
$$H_3^2 \cdot e_1, 2H_2^2 \cdot e_1, 2H_2^2 \cdot e_2, H_1^2 \cdot e_1, H_1^2 \cdot e_2, H_3^1 \cdot e_1, 2H_2^1 \cdot e_1, 2H_2^1 \cdot e_2, H_1^1 \cdot e_2,$$
$$y_1 \cdot e_1 + x^2 \cdot e_2, (x + x^2) \cdot e_1 + (x + 2y_5^2 + y_5^3) \cdot e_2,$$
$$(x^2 - y_2 x^3) \cdot e_1 + (2y_5^2 x + y_5^3 x) \cdot e_2.$$

Man kann leicht nachprüfen, dass auch

$$H_1^1 \cdot e_1, H_1^1 \cdot e_2, H_2^1 \cdot e_1, H_2^1 \cdot e_2, H_3^1 \cdot e_1, H_3^1 \cdot e_2,$$
$$H_1^2 \cdot e_1, H_1^2 \cdot e_2, H_2^2 \cdot e_1, H_2^2 \cdot e_2, H_3^2 \cdot e_1, H_3^2 \cdot e_2$$
$$(x + x^2) \cdot e_1 + (x + 2y_5^2 + y_5^3) \cdot e_2, (x^2 - y_2 x^3) \cdot e_1 + (2y_5^2 x + y_5^3 x) \cdot e_2$$

eine Standardbasis von J ist. Diese Standardbasis hat die im Beweis von Satz 6.1 gewünschte Form. Daher setzen wir

$$\tilde{G} := ((x^2 - y_2 x^3) \cdot e_1 + (2y_5^2 x + y_5^3 x) \cdot e_2, (x + x^2) \cdot e_1 + (x + 2y_5^2 + y_5^3) \cdot e_2).$$

Nach Satz 6.1 ist

$$((H_2^1, H_2^2), \tilde{G})$$

ein Familiencode einer Standardbasis von I. Will man die algebraischen Potenzreihenvektoren der Standardbasis von I noch explizit berechnen, so setzt man

$$\begin{aligned} \tilde{g} &:= \tilde{G}(x, h) \\ &= ((x + x^2)e_1 + (x + 2h_5^2 + h_5^3)e_2, (x^2 - h_2 x^3)e_1 + (2h_5^2 x + h_5^3 x)e_2), \end{aligned}$$

wobei $h_2 = -1 + \sqrt{1 + x + x^2}$ und $h_5 = -1 + \sqrt{1 + x}$, und erhält nach einer kürzeren Rechnung

$$\begin{aligned} \tilde{g} = (\tilde{g}_1, \tilde{g}_2) &= ((x^2 + x^3 - x^3\sqrt{1 + x + x^2})e_1 + (x^2\sqrt{1 + x} - x^2)e_2, g_2) \\ &= (x \cdot g_2 - g_1, g_2). \end{aligned}$$

Bemerkung. Diese Standardbasis von I ist noch nicht reduziert.

7 Konstruktion einer reduzierten Standardbasis und Effektive Division mit Hilfe von Codes

7.1 Der Fall eines x_n-regulären Moduls

Zur Erinnerung: Für einen Untermodul $I \subseteq K[\![x]\!]^s$ ist der *Initialmodul* von I bzgl. einer Monomordnung $<_\eta$ jener Untermodul $\text{in}(I)$ von $K[\![x]\!]^s$, der von den Initialmonomvektoren aller Elemente von I erzeugt wird. Elemente $g_1, \ldots, g_r \in K[\![x]\!]^s$ bilden genau dann eine *Standardbasis* bzgl. $<_\eta$ von $I = \langle g_1, \ldots, g_r \rangle$, wenn deren Initialmonomvektoren den Initialmodul $\text{in}(I)$ erzeugen.
Mit $\text{co}(I)$ bezeichnen wir das kanonische direkte monomiale Komplement von $\text{in}(I)$ in $K[\![x]\!]^s$.

Definition 7.1. Man nennt eine Standardbasis $g_1, \ldots, g_r$ eines Moduls I eine *reduzierte Standardbasis*, wenn die Reste $\overline{g_k} = g_k - \text{in}(g_k)$ in $\text{co}(I) \subseteq K[\![x]\!]^s$ liegen.

Definition 7.2. Wir nennen einen Modul $I \subseteq K[\![x]\!]^s$ x_n*-regulär* bzgl. $<_\eta$, wenn der Initialmodul $\text{in}(I)$ von I bzgl. $<_\eta$ von Monomvektoren in $K[\![x_n]\!]^s$ erzeugt wird.

Wir werden für derartige Moduln dann ohne Beschränkung der Allgemeinheit annehmen, dass $\text{in}(I)$ von Vektoren der Form $x_n^{d_k} \cdot e_k$ mit $d_k \geq 0$ und $1 \leq k \leq t$ für ein $t \leq s$ erzeugt wird. (Dies kann man durch geeignete Permutation der Komponenten von $K[\![x]\!]^s$ erreichen.) Somit ist $\text{co}(I)$ das folgende kartesische Produkt eines endlichen freien $K[\![x']\!]$-Moduls und eines endlichen freien $K[\![x]\!]$-Moduls:

$$\text{co}(I) = \prod_{k=1}^{t} (\oplus_{j=0}^{d_k - 1} K[\![x']\!] \cdot x_n^j) \times K[\![x]\!]^{s-t}.$$

Zur Erinnerung:

Definition 7.3. Wir sagen, der Untermodul I erfüllt *Hironaka's Box-Bedingung* bzgl. $<_\eta$, wenn $\text{co}(I)$ ein kartesisches Produkt von direkten Summen von endlichen freien monomialen $K[\![x_1, \ldots, x_j]\!]$-Moduln ist, d.h.

$$\text{co}(I) = \prod_{l=1}^{s} \oplus_{j=0}^{n} \oplus_{\gamma \in Z_{lj}} K[\![x_1, \ldots, x_j]\!] \cdot x^\gamma$$

mit endlichen Mengen $Z_{lj} \subseteq \mathbb{N}^n$.

Bemerkung. Klarerweise erfüllen x_n-reguläre Moduln die obige Box-Bedingung.

Im Folgenden werden wir einen endlichen Algorithmus zur Berechnung einer reduzierten Standardbasis eines von algebraischen Potenzreihen erzeugten x_n-regulären Moduls angeben. Später werden wir den allgemeinen Fall (eines von algebraischen Potenzreihen erzeugten Moduls) mittels des folgendes Satzes, Satz 7.2 und Induktion über n beweisen. Somit stellt Satz 7.1 einen wichtigen Spezialfall des allgemeinen Falls dar.

Satz 7.1. *Wir nehmen an, der von den algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ erzeugte und mit der Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$ versehene Modul $I \subseteq K[\![x]\!]^s$ ist bzgl. $<_\eta$ ein x_n-regulärer Modul. Dann kann man aus den Familiencodes der $g_1, \ldots, g_r$ mittels eines endlichen Algorithmus den Familiencode einer reduzierten Standardbasis von I bzgl. $<_\eta$ berechnen.*

Beweis. Der Beweis erfolgt in mehreren Schritten:
(1) Wir haben in Lemma 5.1 und Lemma 5.2 gesehen, dass es ausreicht, eine reduzierte Standardbasis des Untermoduls $J = \langle H_i \cdot e_l, G_k \rangle = \langle (y_i - h_i) \cdot e_l, g_k \rangle \subseteq K[\![x,y]\!]^s$ bzgl. der gewählten Erweiterung $<_\varepsilon$ von $<_\eta$ zu konstruieren. Auf Grund von Satz 6.1 können wir ohne Beschränkung der Allgemeinheit annehmen, dass die Polynomvektoren $H_i \cdot e_l$ und G_k bereits eine minimale Standardbasis von J bilden.
Da I ein x_n-regulärer Modul ist und wir o.B.d.A. $\mathrm{in}(H_i \cdot e_l) = y_i \cdot e_l$ annehmen dürfen (vgl. Definition 3.1), wird der Initialmodul $\mathrm{in}(J)$ von $y_i \cdot e_l$ und Monomvektoren der Form $x_n^{d_k} \cdot e_{m_k}$ erzeugt, wobei $d_k \geq 0$ und $1 \leq m_k \leq s$. Nach einer geeigneten Permutation der Komponenten von $K[\![x]\!]^s$ und Umnummerierung der Vatercodes $G_1, \ldots, G_r$ dürfen wir $\mathrm{in}(G_k) = x_n^{d_k} \cdot e_k$ annehmen.
Somit hat das kanonische direkte monomiale Komplement $\mathrm{co}(J)$ von $\mathrm{in}(J)$ in $K[\![x,y]\!]^s$ die Form

$$\mathrm{co}(J) = \oplus_{m=1}^{r} \oplus_{j=0}^{d_m-1} K[\![x']\!] \cdot x_n^j \cdot e_m \oplus \oplus_{m=r+1}^{s} K[\![x]\!] \cdot e_m.$$

Wie wir in Punkt (9) sehen werden, ist es für die Berechnung einer reduzierten Standardbasis von I sogar ausreichend (und viel einfacher), wenn wir nur eine *partiell reduzierte Standardbasis* von J konstruieren. Damit ist gemeint, dass die Standardbasis von J in den letzten $s - r$ Komponenten nicht reduziert sein muss (dort dürfen also y_i's auftreten). Eine derartige partiell reduzierte Standardbasis von J hat also folgende Gestalt:

$$\begin{aligned} b_{il} &= y_i \cdot e_l - b_{il}^\circ - \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} u_{il,mj}(x') \cdot x_n^j \cdot e_m - \sum_{m=r+1}^{s} v_{il,m}(x,y) \cdot e_m, \\ b_k &= x_n^{d_k} \cdot e_k - b_k^\circ - \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} u_{k,mj}(x') \cdot x_n^j \cdot e_m - \sum_{m=r+1}^{s} v_{k,m}(x,y) \cdot e_m. \end{aligned}$$

Dabei sind $u_{il,mj}(x')$, $v_{il,m}(x',y)$, $u_{k,mj}(x)$ und $v_{k,m}(x,y)$ in 0 verschwindende algebraische Potenzreihen in den Variablen $x' = (x_1, \ldots, x_{n-1})$ bzw. (x,y) sowie b_{il}° und b_k° Polynomvektoren in

$$\oplus_{m=1}^{r} \oplus_{j=0}^{d_m-1} K \cdot x_n^j \cdot e_m \oplus \oplus_{m=r+1}^{s} K \cdot e_m$$

Beachte, dass $u_{il,mj}(x')$ und $u_{k,mj}(x')$ nicht von x_n abhängen!

Bemerkung. Es ist notwendig, b_{il}° und b_k° abzutrennen, da der Muttercode nur für in 0 verschwindende algebraische Potenzreihen definiert ist.

Die Elemente $H_i \cdot e_{l''}$, $r+1 \leq l'' \leq s$, von J besitzen bereits die obige Form (mit $u_{il'',mj}(x) = 0$, $b_{il''}^\circ = 0$ und $v_{il'',m}(x,y) = \overline{H_i} \cdot e_{l''}$) und sind folglich Bestandteile der partiell reduzierten Standardbasis von J. Damit müssen wir noch eine partiell reduzierte Standardbasis $b_{il'}$, b_k ($1 \leq l', k \leq r$, $1 \leq i \leq p$) von

$$J' = \langle H_i \cdot e_{l'}, G_k \rangle \subseteq K[\![x,y]\!]^s$$

konstruieren. Dazu werden wir zuerst die Polynomvektoren $b_{il'}^\circ$ und b_k° bestimmen. Danach werden wir Codes der Koeffizientenreihen $u_{il',mj}(x')$, $u_{k,mj}(x')$, $v_{il',m}(x,y)$ und $v_{k,m}(x,y)$ konstruieren. Dies wird insbesondere zeigen, dass diese algebraisch sind.

(2) Um die Polynomvektoren $b_{il'}^\circ$ und b_k° zu bestimmen, kann man zum Beispiel mittels Babylonischer Division die partiell reduzierte Standardbasis von J' bis zu einem genügend hohen Grad berechnen. (Ein derartiger Grad ist etwa $d = \max_k d_k$.)

(3) Um die Potenzreihen $u_{il',mj}(x')$, $v_{il',m}(x',y)$, $u_{k,mj}(x)$ und $v_{k,m}(x,y)$ zu bestimmen, verwenden wir den folgenden Trick: Wir definieren die *virtuelle partiell reduzierte Standardbasis* von J' als die polynomialen Vektoren

$$\begin{aligned} B_{il'} &= y_i \cdot e'_l - b^{\circ}_{il'} - \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} u_{il',mj} \cdot x_n^j \cdot e_m - \sum_{m=r+1}^{s} v_{il',m} \cdot e_m, \\ B_k &= x_n^{d_k} \cdot e_k - b^{\circ}_k - \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} u_{k,mj} \cdot x_n^j \cdot e_m - \sum_{m=r+1}^{s} v_{k,m} \cdot e_m, \end{aligned}$$

wobei $u_{il',mj}$, $u_{k,mj}$, $v_{il',m}$ und $v_{k,m}$ nun neue Variablen sind, die wir im Folgenden mit u und v abkürzen werden. Im übernächsten Schritt werden wir Polynome $U_{il',mj}$, $U_{k,mj}$, $V_{il',m}$ und $V_{k,m}$ in $K[x,u,v,y]$ konstruieren. Diese werden dann den Muttercode (U,V) der Babyreihenvektoren

$$(u(x'),v(x,y)) = (u_{il',mj}(x'), u_{k,mj}(x'), v_{il',m}(x,y), v_{k,m}(x,y))$$

bilden. Folglich werden $B_{il'}$ und B_k die Vatercodes der Reihen $b_{il'}$ und b_k sein, die aber gerade die von uns gewünschte partiell reduzierte Standardbasis von J' bilden.

(4) Die Konstruktion des Muttercodes (U,V) der partiell reduzierten Standardbasis von J' erfolgt mit Hilfe der Babylonischen Division. Dazu müssen wir aber zuerst überprüfen, ob wir diese in der uns vorliegenden Situation auch anwenden dürfen: Dabei stellen wir als Erstes fest, dass kein Monomvektor der Reste von $B_{il'}$ und B_k durch $y_i \cdot e_{l'}$ oder $x_n^{d_k} \cdot e_k$ teilbar ist. Darüber hinaus bilden $y_i \cdot e_{l'}$ und $x_n^{d_k} \cdot e_k$ eine Janet-Basis mit Reichweiten $n_{il'} = n+q+i$ und $n_k = n+q$ des Untermoduls $\mathrm{in}(J') \otimes K[u,v] = \langle y_i \cdot e'_l, x_n^{d_k} \cdot e_k \rangle$ von $K[x,u,v,y]^r \times \{0\}^{s-r} \subseteq K[x,u,v,y]^s$. Dabei seien die Variablen als (x,u,v,y) geordnet und q die Anzahl der u- und v-Variablen. Daher sind $y_i \cdot e'_l$ und $x_n^{d_k} \cdot e_k$ Leuchttürme von $B_{il'}$ bzw. B_k bzgl. der Reichweiten $n_{il'}$ und n_k. Weiters ist klar, dass $\mathrm{in}(J') \otimes K[u,v]$ (als Untermodul von $K[x,u,v,y]^r$ betrachtet) Hironaka's Box-Bedingung erfüllt. Damit sind alle Voraussetzungen für die Babylonische Division gegeben.

(5) Um den Muttercode (U,V) zu berechnen, dividieren wir die polynomialen Erzeuger $H_i \cdot e_{l'}$ und G_k von J' mit Hilfe der Babylonischen Division durch die virtuelle partiell reduzierte Standardbasis $B_{il'}$ und B_k von J' bzgl. der Leuchttürme $y_i \cdot e_{l'}$, $x_n^{d_k} \cdot e_k$ und der Reichweiten $n_{il'}$, n_k. Diese Division liefert in endlich vielen Schritten Reste $R_{il'}$ und R_k im kanonischen direkten monomialen Komplement

$$\mathrm{co}(J') \otimes K[u,v] = \prod_{m=1}^{r} (\oplus_{j=0}^{d_m-1} K[x',u,v] \cdot x_n^j) \times K[x,u,v,y]^{s-r}$$

von $\mathrm{in}(J') \otimes K[u,v]$ in $K[x,u,v,y]^s$. Drücken wir die Reste als Polynomvektoren in x_n aus, so sind sie von der Form

$$\begin{aligned} R_{il'} &= \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} U_{il',mj} \cdot x_n^j \cdot e_m + \sum_{m=r+1}^{s} V_{il',m} \cdot e_m, \\ R_k &= \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} U_{k,mj} \cdot x_n^j \cdot e_m + \sum_{m=r+1}^{s} V_{k,m} \cdot e_m, \end{aligned}$$

wobei $U_{il',mj}$, $U_{k,mj}$ Polynome in (x', u) und $V_{il',m}$, $V_{k,m}$ Polynome in (x, u, v, y) sind.
Beachte: $U_{il',mj}$ und $U_{k,mj}$ hängen nicht von v ab!

(6) In diesem Schritt werden wir zeigen, dass U und V keinen konstanten Term haben: Ersetzt man in $R_{il'}$ und R_k die Variablen u und v durch die Potenzreihen $u(x')$ und $v(x, y)$, so erhält man auf Grund der Tatsache, dass $u(x')$ nicht von x_n und U nicht v abhängt, Potenzreihen $r_{il'}$ und r_k in co(J'). Nach Konstruktion liegen $r_{il'}$ und r_k aber in J'. Damit folgt aus dem Divisionssatz für formale Potenzreihen (vgl. Satz 2.4), dass $r_{il'}$ und r_k beide identisch null sind. Dies impliziert wegen der direkten Summenzerlegung von co(J'), dass das Ersetzen der Variablen u und v durch $u(x')$ und $v(x, y)$ in U und V null ergibt. Da aber $u(x')$ und $v(x, y)$ nach Konstruktion keinen konstanten Term besitzen, haben auch U und V keinen konstanten Term.

(7) Man kann zeigen, dass U und V tatsächlich alle Eigenschaften für einen Muttercode erfüllen. Dazu muss man noch nachprüfen, dass die Initialmonomvektoren der linearen Terme von $U_{il',mj}(0, u, v, 0)$, $U_{k,mj}(0, u, v, 0)$, $V_{il',mj}(0, u, v, 0)$ und $V_{k,m}(0, u, v, 0)$ bzgl. einer (bzgl. u und v graduierten) Erweiterung $<_\xi$ von $<_\varepsilon$ auf $\mathbb{N}^{n+p+q} \times \{1, \ldots, s\}$ gerade $u_{il',mj}$, $u_{k,mj}$, $v_{il',m}$ und $v_{k,m}$ sind. Da dies eine längere Rechnung ist, wird sie hier weggelassen. Für Details vergleiche Schritt (f) im Beweis von Theorem 2 in [ACJHa].

(8) In diesem Schritt zeigen werden wir zeigen, dass $u(x')$ und $v(x, y)$ tatsächlich die Babyreihen von U und V sind:
Nach Definition verschwinden $u(x')$ und $v(x, y)$ in null. Wir haben in Punkt (6) bereits gesehen, dass $r_{il'} = R_{il'}(x, u(x'), v(x, y))$ und $r_k = R_k(x, u(x'), v(x, y))$ null sind. Da aber $u(x')$ nicht von x_n und U nicht von v abhängt, folgt aus der Zerlegung von in(J'), dass $U(x, u(x'))$ und $V(x, u(x'), v(x, y), y)$ null sind.

(9) Wie wir soeben gezeigt haben, bilden die

$$b_{il'},\ b_k,\ H_i \cdot e_{l''},$$

wobei $1 \leq l', k \leq r$ und $r + 1 \leq l'' \leq s$, eine partiell reduzierte Standardbasis von J. Dabei sind die Initialmonomvektoren von $b_{il'}$ und $H_i \cdot e_{l''}$ gerade $y_i \cdot e_{l'}$ bzw. $y_i \cdot e_{l''}$. Ersetzt man nun in b_k die Variablen y_i durch h_i, so erhält man Vektoren $\tilde{g}_k$, die eine reduzierte Standardbasis von I bilden. Denn das Ersetzen von y_i durch h_i tritt nur in den letzten $s - r$ Komponenten von b_k auf und unsere Erweiterung $<_\varepsilon$ von $<_\eta$ erfüllt nach Voraussetzung $y_i <_\varepsilon$ in(h_i) für alle i, woraus folgt, dass durch diese Substitution die Reduziertheit von $\tilde{g}_k$ nicht zerstört wird. □

Bemerkung. (1) Würden wir im Beweis des letzten Satzes eine reduzierte Standardbasis von J konstruieren, so würde (im Fall $r < s$) U von v abhängen, woraufhin der restliche Teil des Beweises schwerer zu zeigen wäre.
(2) Im Falle $s = r$ ist die im Beweis des letzten Satzes konstruierte partiell reduzierte Standardbasis von J eine reduzierte Standardbasis von J.

Beispiel 7.1. In diesem Beispiel wollen wir eine reduzierte Standardbasis des folgenden x_2-regulären Ideals bzgl. der graduiert lexikographischen Ordnung $<_\eta$ auf $\mathbb{N}^2$ mit $x_2 < x_1$ berechnen:

$$I = \langle x_2^2 \sqrt{1 + x_1 x_2} \rangle \subseteq K[\![x_1, x_2]\!].$$

Man kann leicht nachprüfen, dass

$$(H, G) = ((y_1 - x_2^2 - x_2^2 y_2, y_2 + \frac{1}{2} y_2^2 - \frac{1}{2} x_1 x_2), y_1)$$

ein Code der algebraische Potenzreihe $g := x_2^2 \sqrt{1 + x_1 x_2}$ ist. Dem Beweis von Satz 7.1 folgend betrachten wir das Ideal $J = \langle H_1, H_2, G \rangle \subseteq K[\![x_1, x_2, y_1, y_2]\!]$ und als Erweiterung $<_\varepsilon$ von $<_\eta$ auf $\mathbb{N}^{2+2}$ die graduiert lexikographische Ordnung mit $y_2 < y_1 < x_2 < x_1$. Dann berechnen wir mit Hilfe von Satz 6.1 folgende Standardbasis von J bzgl. $<_\varepsilon$:

$$H_1, H_2, x_2^2.$$

Damit hätten wir die reduzierte Standardbasis von I bzgl. $<_\eta$ bereits gefunden:

$$b = x_2^2.$$

Der Beweis von Satz 7.1 liefert uns jedoch mehr - nämlich die Konstruktion einer reduzierten Standardbasis von J - und dies wollen wir nun durchführen:
Dazu betrachten wir - Schritt (1) des Beweises von Satz 7.1 folgend - das Ideal

$$J = \langle H_1, H_2, x_2^2 \rangle = \langle y_1 - x_2^2 - x_2^2 y_2, y_2 + \frac{1}{2} y_2^2 - \frac{1}{2} x_1 x_2, x_2^2 \rangle.$$

(Diese Erzeuger von J bilden nach unserer obigen Berechnung eine minimale Standardbasis.) Daraus ergibt sich

$$\text{in}(J) = \langle y_1, y_2, x_2^2 \rangle$$

und folglich

$$\text{co}(J) = K[\![x_1]\!] \oplus K[\![x_1]\!] \cdot x_2.$$

Somit wissen wir, dass eine reduzierte Standardbasis von J folgende Gestalt hat:

$$\begin{array}{lcl} b_i & = & y_i - b_i^\circ - u_{i,0}(x_1) - u_{i,1}(x_1) \cdot x_2, \\ b & = & x_2^2 - b^\circ - u_0(x_1) - u_1(x_1) \cdot x_2. \end{array}$$

Dabei sind $u_{i,0}(x_1)$, $u_0(x_1)$, $u_{i,1}$ und $u_1(x_1)$ in 0 verschwindende algebraische Potenzreihen in x_1, sowie b_i° und b° Polynome in $K \oplus K \cdot x_2$ und $1 \leq i \leq 2$.
Um den Rechenaufwand zu verkleinern, erinnern wir uns daran, dass der Erzeuger x_2^2 von J bereits reduziert ist. Damit ergibt sich sofort:

$$b^\circ = 0, \;\; u_0(x_1) = u_1(x_1) \equiv 0.$$

Im nächsten Schritt wollen wir b_1° und b_2° bestimmen. Dazu setzen wir b_1 und b_2 bis zum Grad $d = 2$ unbestimmt an und erhalten (mit $a, b, c, d, a', b', c', d' \in K$):

$$\begin{array}{lcl} B_1' & = & y_1 - ax_1 - bx_2 - cx_1^2 - dx_1 x_2, \\ B_2' & = & y_2 - a'x_1 - b'x_2 - c'x_1^2 - d'x_1 x_2, \\ B & = & x_2^2. \end{array}$$

Jetzt dividieren wir die Erzeuger H_1, H_2 und x_2^2 von J babylonisch durch B_1', B_2' und B bzgl. y_1, y_2, x_2^2 und der Reichweiten 4, 3, 2. Es ergeben sich folgende Reste

$$\begin{array}{lcl} R_1' & = & ax_1 + bx_2 + cx_1^2 + dx_1 x_2, \\ R_2' & = & a'x_1 + b'x_2 + (c' + \frac{1}{2} a'^2) x_1^2 + (d' - \frac{1}{2} + a'b') x_1 x_2 \\ & & + \text{Terme höherer Ordnung.} \end{array}$$

Daraus erhalten wir $a = b = c = d = a' = b' = c' = 0,\ \ d' = \frac{1}{2}$ und folglich ($b_i^\circ \in K \oplus K \cdot x_2$)

$$b_1^\circ = b_2^\circ = 0.$$

Nun können wir - Schritt (5) des Beweises von Satz 7.1 folgend - die Standardbasis H_1, H_2, x_2^2 von J durch die virtuelle reduzierte Standardbasis

$$\begin{array}{lcl} B_1 & = & y_1 - u_{1,0} - u_{1,1} \cdot x_2, \\ B_2 & = & y_2 - u_{2,0} - u_{2,1} \cdot x_2, \\ B & = & x_2^2, \end{array}$$

von J bzgl. der Leuchttürme y_1, y_2, x_2^2 und der Reichweiten 8, 7, 6 babylonisch dividieren. Wir erhalten folgende Reste

$$\begin{array}{lcl} R_1 & = & [u_{1,0} - u_0 - u_0u_{2,0} - u_1u_{2,1}u_0] + \\ & & [u_{1,1} - u_1 - u_0u_{2,1} - u_1u_{2,0} - u_1u_{2,1}u_1] \cdot x_2, \\ R_2 & = & [u_{2,0} + \frac{1}{2}u_{2,0}^2] + [u_{2,1} + u_{2,0}u_{2,1} - \frac{1}{2}x_1 + \frac{1}{2}u_{2,1}^2u_1] \cdot x_2. \end{array}$$

Damit ist

$$\begin{array}{lcl} U & = & (u_{1,0} - u_0 - u_0u_{2,0} - u_1u_{2,1}u_0, \\ & & u_{1,1} - u_1 - u_0u_{2,1} - u_1u_{2,0} - u_1u_{2,1}u_1, \\ & & u_{2,0} + \frac{1}{2}u_{2,0}^2, u_{2,1} + u_{2,0}u_{2,1} - \frac{1}{2}x_1 + \frac{1}{2}u_{2,1}^2u_1) \end{array}$$

ein Muttercode und (B_1, B_2, B) ein Vatercode der reduzierten Standardbasis b_1, b_2, b von J. Berechnet man mittels des Satzes über implizite Funktionen für algebraische Potenzreihen die Babyreihen $u_{i,0}(x_1)$, $u_{i,1}(x_1)$, $u_0(x_1)$ und $u_1(x_1)$, so ergibt sich

$$u_0(x_1) = u_1(x_1) = u_{1,0}(x_1) = u_{1,1}(x_1) = u_{2,0}(x_1) \equiv 0,\ \ u_{2,1}(x_1) = \frac{1}{2}x_1.$$

Daher ist

$$(u_{2,1} - \frac{1}{2}x_1, (y_1, y_2 - u_{2,1}x_2, x_2^2))$$

ein weiterer (und viel einfacherer) Familiencode der reduzierten Standardbasis b_1, b_2, b von J.

Beispiel 7.2. Seien

$$g_1 := x^3\sqrt{1 + x + x^2} \cdot e_1 + x^2 \cdot e_2,\ g_2 := (x + x^2) \cdot e_1 + x\sqrt{1 + x} \cdot e_2$$

und I der von den algebraischen Potenzreihenvektoren g_1 und g_2 erzeugte Modul. (Dieser ist klarerweise x-regulär.)
Man kann leicht überprüfen, dass

$$\begin{array}{lcl} (H, G) & = & ((y_1 - x^3y_2 - x^3, y_2 - \frac{1}{2}x - \frac{1}{2}x^2 + \frac{1}{2}y_2^2, y_3 - x^2, \\ & & y_4 - x - x^2, y_5 + \frac{1}{2}y_5^2 - \frac{1}{2}x, y_6 - y_5^3 - 3y_5^2 - 2y_5), \\ & & (y_1 \cdot e_1 + y_3 \cdot e_2, y_4 \cdot e_1 + y_6 \cdot e_2)) \end{array}$$

ein Code von I ist.
Unser Ziel ist es nun, eine reduzierte Standardbasis von I bzgl. der Monomordnung

$<_\eta = (<_{lex}, C)$ (vgl. Beispiel 6.3) zu konstruieren.
Wie im Beweis von Satz 7.1 betrachten wir dazu den Modul $J = \langle H_i \cdot e_l, G_k \rangle$, wobei $1 \leq i \leq 4$, $1 \leq l \leq 2$ und $1 \leq k \leq 2$. Weiters wählen wir als Erweiterung $<_\varepsilon$ von $<_\eta$ auf $\mathbb{N}^{1+4} \times \{1,2\}$ die graduiert lexikographische Ordnung $(<_{deglex}, C)$ mit $y_6 < y_5 < y_4 < y_3 < y_2 < y_1 < x$ (wobei die Priorität auf den Koeffizienten liegt).
Mit Hilfe von Satz 6.1 ergibt sich folgende Standardbasis von J

$$\begin{gathered} H_i \cdot e_l, \\ (x + x^2) \cdot e_1 + (x + 2y_5^2 + y_5^3) \cdot e_2, \\ (x^2 - y_2 x^3) \cdot e_1 + (2y_5^2 x + y_5^3 x) \cdot e_2, \end{gathered}$$

wobei $1 \leq i \leq 4$ und $1 \leq l \leq 2$. Nach Lemma 5.2 ist

$$\begin{aligned} (\tilde{H}, \tilde{G}) &= ((y_2 - \frac{1}{2}x - \frac{1}{2}x^2 + \frac{1}{2}y_2^2, y_5 + \frac{1}{2}y_5^2 - \frac{1}{2}x), \\ &\quad ((x^2 - y_2 x^3) \cdot e_1 + (2y_5^2 x + y_5^3 x) \cdot e_2, \\ &\quad (x + x^2) \cdot e_1 + (x + 2y_5^2 + y_5^3) \cdot e_2)) \end{aligned}$$

ein Code einer Standardbasis von I und

$$\begin{aligned} \tilde{g} &= \tilde{G}(x, H(x)) \\ &= ((x^2 - h_2 x^3)e_1 + (2h_5^2 x + h_5^3 x)e_2, (x + x^2)e_1 + (x + 2h_5^2 + h_5^3)e_2) \\ &= (g_2, (x^2 + x^3 - x^3\sqrt{1 + x + x^2})e_1 + (x^2\sqrt{1+x} - x^2)e_2) \end{aligned}$$

eine Standardbasis von I.
Somit gilt für $J = \langle H_i \cdot e_l, \tilde{G}_1, \tilde{G}_2 \rangle$

$$\text{in}(J) = \langle y_i \cdot e_l, x^2 \cdot e_1, x \cdot e_2 \rangle$$

und folglich $\text{co}(J) = K \cdot e_1 \oplus K \cdot x \cdot e_1 \oplus K \cdot e_2$. Die reduzierte Standardbasis von J bzgl. $<_\varepsilon$ ist von der Form

$$\begin{aligned} b_{il} &= y_i \cdot e_l - b_{il}^\circ - u_{il,10} \cdot e_1 - u_{il,11} \cdot x \cdot e_1 - u_{il,20} \cdot e_2, \\ b_1 &= x^2 \cdot e_1 - b_1^\circ - u_{1,10} \cdot e_1 - u_{1,11} \cdot x \cdot e_1 - u_{1,20} \cdot e_2, \\ b_2 &= x \cdot e_2 - b_2^\circ - u_{2,10} \cdot e_1 - u_{2,11} \cdot x \cdot e_1 - u_{2,20} \cdot e_2, \end{aligned}$$

wobei $1 \leq i \leq 4$, $1 \leq l \leq 2$ und $u_{il,10}$, $u_{il,11}$, $u_{il,20}$, $u_{1,10}$, $u_{1,11}$, $u_{1,20}$, $u_{2,10}$, $u_{2,11}$, $u_{2,20} \in K$ in 0 verschwinden, also 0 sein müssen. Weiters liegen die Polynomvektoren b_{il}°, b_1° und b_2° in $K \cdot e_1 \oplus K \cdot x \cdot e_1 \oplus K \cdot e_2$. Da jedoch $\text{in}(b_1) = x^2 \cdot e_1$ gelten soll, folgt daraus unmittelbar

$$b_1^\circ = 0.$$

Wir müssen nun also noch b_2° und b_{il}° für $1 \leq i \leq 4$, $1 \leq l \leq 2$ bestimmen. Dazu schreiben wir die virtuelle reduzierte Standardbasis von J (unter Beachtung von $\text{in}(B_{il}) = y_i \cdot e_l$) als

$$\begin{aligned} B_{il} &= y_i \cdot e_l - a_{il}^\circ \cdot c \cdot e_1, \\ B_1 &= x^2 \cdot e_1, \\ B_2 &= x \cdot e_2 - c \cdot x \cdot e_1, \end{aligned}$$

wobei $a_{il}, c \in K$. Babylonische Division der Standardbasis $H_i \cdot e_l, \tilde{G}_1, \tilde{G}_2$ von J durch B_{il}, B_1, B_2 bzgl. der Leuchttürme $y_i \cdot e_l$, $x^2 \cdot e_1$, $x \cdot e_2$ und der Reichweiten 7,6, 5 liefert folgende Reste:

$$\begin{array}{lcllcl}
R_1 & = & 0, & R_2 & = & (1+c)\cdot x\cdot e_1,\\
R_{11} & = & a_{11}\cdot x\cdot e_1, & R_{12} & = & a_{12}\cdot x\cdot e_1,\\
R_{21} & = & (a_{21}-\frac{1}{2})\cdot x\cdot e_1, & R_{22} & = & (a_{22}+\frac{1}{2})\cdot x\cdot e_1,\\
R_{31} & = & a_{31}\cdot x\cdot e_1, & R_{32} & = & a_{32}\cdot x\cdot e_1,\\
R_{41} & = & (a_{41}-1)\cdot x\cdot e_1, & R_{42} & = & (a_{42}+1)\cdot x\cdot e_1,\\
R_{51} & = & (a_{51}-\frac{1}{2})\cdot x\cdot e_1, & R_{52} & = & (a_{52}+\frac{1}{2})\cdot x\cdot e_1,\\
R_{61} & = & (a_{61}-2a_{51})\cdot x\cdot e_1, & R_{62} & = & (a_{62}-2a_{52})\cdot x\cdot e_1.
\end{array}$$

Daraus folgt

$$a_{11}=a_{12}=a_{31}=a_{32}=0,\ a_{21}=a_{51}=\tfrac{1}{2},$$
$$a_{22}=a_{52}=-\tfrac{1}{2},\ a_{41}=a_{61}=1,\ a_{42}=a_{62}=-1.$$

Somit ist

$$\begin{array}{lcl}
b_1 & = & x^2\cdot e_1,\\
b_2 & = & x\cdot e_2+x\cdot e_1
\end{array}$$

eine reduzierte Standardbasis des Moduls I.

Beispiel 7.3. In diesem Beispiel betrachten wir die algebraischen Potenzreihenvektoren

$$g_1:=\frac{x_2}{1+x_1}\cdot e_1+x_1x_2\cdot e_2,\ g_2:=x_1^2x_2^2\cdot e_1+x_2\cdot e_2$$

und den davon erzeugten x_2-regulären Modul $I=\langle g_1,g_2\rangle\subseteq K[\![x_1,x_2]\!]^2$. Dabei sei $K[\![x_1,x_2]\!]^2$ mit der graduiert lexikographischen Ordnung $<_\eta=(<_{deglex},C)$ auf $\mathbb{N}^n\times\{1,2\}$ mit $x_1<x_2$ versehen (vgl. Beispiel 6.3). Wie man leicht nachrechnen kann, ist

$$(H,G) \quad = \quad ((y_1+y_1x_1-x_2,y_2-x_1x_2),(y_1\cdot e_1+y_2\cdot e_2,y_2^2\cdot e_1+x_2\cdot e_2))$$

ein Familiencode des Moduls I.
Wir wollen nun eine reduzierte Standardbasis von I konstruieren. Dem Beweis von Satz 7.1 folgend berechnen wir dazu zuerst eine Standardbasis von $J=\langle H_i\cdot e_l,G_k\rangle\subseteq K[\![x,y]\!]^2$, wobei $1\leq i,l,k\leq 2$, bzgl. einer Erweiterung $<_\varepsilon$ der Monomordnung $<_\eta$ auf $\mathbb{N}^{2+2}\times\{1,2\}$. Dabei wählen wir $<_\varepsilon$ als die graduiert lexikographische Ordung $<_\varepsilon=(<_{deglex},C)$ mit $y_1<y_2<x_1<x_2$. Dann ergibt sich folgende minimale Standardbasis von J:

$$H_1\cdot e_1,\ H_1\cdot e_2,\ H_2\cdot e_1,\ H_2\cdot e_2,\ (x_2-y_1x_1)\cdot e_1+x_1x_2\cdot e_2,\ G_2.$$

Setzt man nun

$$\tilde{G}:=((x_2-y_1x_1)\cdot e_1+x_1x_2\cdot e_2,G_2),$$

so ist nach Satz 6.1

$$\tilde{g}:=\tilde{G}(x,h(x))=\left(\left(x_2-\frac{x_2x_1}{1+x_1}\right)\cdot e_1+x_1x_2\cdot e_2,g\right)=(g_1,g_2)$$

eine Standardbasis des Moduls I bzgl. der Monomordnung $<_\eta$. Diese ist jedoch noch nicht reduziert. Daher folgen wir weiter dem Beweis von Satz 7.1. Es gilt

$$\text{in}(J)=\langle H_i\cdot e_l,x_2\cdot e_1,x_2\cdot e_2\rangle$$

und folglich $\text{co}(J)=K[\![x_1]\!]\cdot e_1+K[\![x_1]\!]\cdot e_2$. Somit ist die reduzierte Standardbasis von J von der Gestalt

$$\begin{aligned} b_{il} &= y_i \cdot e_l - b_{il}^\circ - u_{il,1}(x_1) \cdot e_1 - u_{il,2}(x_2) \cdot e_2, \\ b_1 &= x_2 \cdot e_1 - b_1^\circ - u_{1,1}(x_1) \cdot e_1 - u_{1,2}(x_1) \cdot e_2, \\ b_2 &= x_2 \cdot e_2 - b_2^\circ - u_{2,1}(x_1) \cdot e_1 - u_{2,2}(x_1) \cdot e_2, \end{aligned}$$

wobei $u_{il,1}$, $u_{il,2}$, $u_{1,1}$, $u_{1,2}$, $u_{2,1}$ und $u_{2,2}$ in 0 verschwindende Potenzreihen in x_1 und b_{il}°, b_1° und b_2° Polynomvektoren in $K \cdot e_1 \oplus K \cdot e_2$ sind. Da aber in$(b_{il}) = y_i \cdot e_l$, in$(b_1) = x_2 \cdot e_1$ und in$(b_2) = x_2 \cdot e_2$ gelten soll, folgt daraus sofort

$$b_{il}^\circ = b_1^\circ = b_2^\circ = 0.$$

Wir definieren die virtuelle reduzierte Standardbasis von J als

$$\begin{aligned} B_{il} &= y_i \cdot e_l - u_{il,1} \cdot e_1 - u_{il,2} \cdot e_2, \\ B_1 &= x_2 \cdot e_1 - u_{1,1} \cdot e_1 - u_{1,2} \cdot e_2, \\ B_2 &= x_2 \cdot e_2 - u_{2,1} \cdot e_1 - u_{2,2} \cdot e_2. \end{aligned}$$

Babylonische Division von $H_i \cdot e_l$ und $\tilde{G}$ durch B_{il}, B_1 und B_2 bzgl. der Leuchttürme $y_i \cdot e_l$, $x_2 \cdot e_1$, $x_2 \cdot e_2$ und der Reichweiten $n_{il} = 2 + 12 + i$, $n_1 = n_2 = 2 + 12$ liefert folgende Reste:

$$\begin{aligned} R_{11} &= (u_{11,1} - u_{1,1} + u_{11,1}x_1) \cdot e_1 + (u_{11,2} - u_{1,2} + u_{11,2}x_1) \cdot e_2, \\ R_{12} &= (u_{12,1} + u_{12,1}x_1 - u_{2,1}) \cdot e_1 + (u_{12,2} + u_{12,2}x_1 - u_{2,2}) \cdot e_2, \\ R_{21} &= (u_{21,1} - u_{1,1}x_1) \cdot e_1 + (u_{21,2} - u_{1,2}x_1) \cdot e_2, \\ R_{22} &= (u_{22,1} - u_{2,1}x_1) \cdot e_1 + (u_{22,2} - u_{2,2}x_1) \cdot e_2, \\ R_1 &= (u_{1,1} - u_{11,1}x_1 + u_{2,1}x_1) \cdot e_1 + (u_{1,2} - u_{11,2}x_1 + u_{2,2}x_1) \cdot e_2, \\ R_2 &= (u_{2,1} + u_{21,1}^2 + u_{21,2}u_{22,1}) \cdot e_1 + (u_{2,2} + u_{21,1}u_{21,2} + u_{21,2}u_{22,2}) \cdot e_2. \end{aligned}$$

Berechnet man daraus die Babyreihen $u_{il,1}(x_1)$, $u_{il,2}(x_1)$, $u_{1,1}(x_1)$, $u_{1,2}(x_1)$, $u_{2,1}(x_1)$ und $u_{2,2}(x_1)$, so erhält man

$$u_{il,1}(x_1) = u_{il,2}(x_1) = u_{1,1}(x_1) = u_{1,2}(x_1) = u_{2,1}(x_1) = u_{2,2}(x_1) \equiv 0.$$

Folglich ist

$$b_{il} = y_i \cdot e_l,\ b_1 = x_2 \cdot e_1,\ b_2 = x_2 \cdot e_2$$

eine reduzierte Standardbasis von J und $b_1 = x_2 \cdot e_1$, $b_2 = x_2 \cdot e_2$ die von uns gesuchte reduzierte Standardbasis von I.

Beispiel 7.4. In diesem Beispiel seien $h := x^2 + x^3$,

$$g := (x + h^2x^2) \cdot e_1 + h \cdot e_2$$

und $I = \langle g \rangle \subseteq K[\![x]\!]^2$ der von g erzeugte Modul. Klarerweise ist I bzgl. jeder Monomordnung x-regulär.
Man kann leicht überprüfen, dass

$$(H, G) \quad = \quad (y - x^2 - x^3, (x + x^2y^2) \cdot e_1 + y \cdot e_2)$$

ein Code von g ist.
Wir wollen nun eine reduzierte Standardbasis des Moduls I bzgl. der Monomordnung $<_\eta = (<_{deglex}, C)$ auf $\mathbb{N}^1 \times \{1, 2\}$ berechnen. Dazu betrachten wir den Modul

$$J = \langle H \cdot e_1, H \cdot e_2, G \rangle \subseteq K[\![x, y]\!]^2.$$

Weiters wählen wir als Erweiterung $<_\varepsilon$ von $<_\eta$ auf $\mathbb{N}^{1+1} \times \{1,2\}$ die graduiert lexikographische Ordnung mit $y < x$.
Mit Hilfe von Satz 6.1 berechnen wir zuerst folgende minimale Standardbasis von J bzgl. $<_\varepsilon$:

$$H \cdot e_1,\ H \cdot e_2,\ (x + y^2x^2) \cdot e_1 + (x^2 + x^3) \cdot e_2.$$

Dann setzen wir $\tilde{G} := (x + y^2x^2) \cdot e_1 + (x^2 + x^3) \cdot e_2$ und

$$\tilde{g} := \tilde{G}(x, h) = (x + h^2x^2) \cdot e_1 + (x^2 + x^3) \cdot e_2 = g.$$

Nach dem Beweis von Satz 6.1 ist $(H, \tilde{G})$ ein Code der minimalen (noch nicht reduzierten) Standardbasis $\tilde{g} = g$ von I. Der Vorteil dieses Codes von g liegt darin, dass seine Elemente $H \cdot e_1$, $H \cdot e_2$ und $\tilde{G}$ eine minimale Standardbasis von J bilden, was im Beweis von Satz 7.1 vorausgesetzt wird. Damit ergibt sich

$$\text{in}(J) = \langle y \cdot e_1, y \cdot e_2, x \cdot e_1 \rangle$$

und folglich $\text{co}(J) = K \cdot e_1 \oplus K[\![x]\!] \cdot e_2$. Wie wir im Beweis von Satz 7.1 gesehen haben, ist es ausreichend, eine partiell reduzierte Standardbasis von J zu konstruieren. Diese ist von der Gestalt

$$\begin{array}{lcl} b_1 & = & y \cdot e_1 - b_1^\circ - u_1 \cdot e_1 - v_1(x, y) \cdot e_2, \\ b_2 & = & H \cdot e_2, \\ b & = & x \cdot e_1 - b^\circ - u \cdot e_1 - v(x, y) \cdot e_2, \end{array}$$

wobei $u_1, u \in K$ und $v_1, v \in K[\![x, y]\!]$ in 0 verschwinden sollen. Daraus folgt sofort

$$u_1 = u = 0.$$

Weiters sind b_1° und b° Polynomvektoren in $K \cdot e_1 \oplus K \cdot e_2$. Da jedoch $\text{in}(b_1) = y \cdot e_1$ und $\text{in}(b) = x \cdot e_1$ gelten soll, ergibt sich

$$b_1^\circ = b^\circ = 0.$$

Um die partiell reduzierte Standardbasis b_1, b des Moduls

$$J' = \langle H \cdot e_1, G \rangle$$

zu konstruieren, betrachten wir dessen virtuelle partiell reduzierte Standardbasis

$$\begin{array}{lcl} B_1 & = & y \cdot e_1 - v_1 \cdot e_2, \\ B & = & x \cdot e_1 - v \cdot e_2. \end{array}$$

Nun dividieren wir $H \cdot e_1$ und $\tilde{G}$ babylonisch durch B_1 und B bzgl. der Leuchttürme $y \cdot e_1$, $x \cdot e_1$ und der Reichweiten 4, 3. Dabei ergeben sich folgende Reste

$$\begin{array}{lcl} R_1 & = & v_1 - xv - x^2v, \\ R & = & v + x^2yv_1 + x^2 + x^3. \end{array}$$

Damit ist

$$\begin{array}{rcl} (V, (B_1, B)) & = & ((v_1 - xv - x^2v, v + x^2yv_1 + x^2 + x^3), \\ & & (y \cdot e_1 - v_1 \cdot e_2, x \cdot e_1 - v \cdot e_2)) \end{array}$$

ein Familiencode der partiell reduzierten Standardbasis b_1, b von J' und $(V, (B_1, H \cdot e_2, B))$ ein Familiencode der partiell reduzierten Standardbasis b_1, $H \cdot e_2$, b von J. Berechnet man die Babyreihen v_1 und v von V, so erhält man

$$v_1(x,y) = -\frac{x(x+x^2)^2}{1+y(x^3+x^4)},\ v(x,y) = -\frac{x^2+x^3}{1+y(x^3+x^4)}.$$

Setzt man nun noch in $b = x \cdot e_1 - v(x,y) \cdot e_2$ für y die Babyreihe $h(x) = x^2 + x^3$ ein, so ergibt sich folgende reduzierte Standardbasis von I:

$$x \cdot e_1 + \frac{x^2+x^3}{1+x(x^2+x^3)^2} \cdot e_2.$$

Beispiel 7.5. Wir betrachten den algebraischen Potenzreihenvektor

$$g = \frac{x_3}{\sqrt{1+x_1x_2}} \cdot e_1 + \left(x_3^2 + x_1x_2\sqrt{1+x_1^2}\right) \cdot e_2$$

und den davon erzeugten Untermodul $I = \langle g \rangle$ von $K[\![x_1, x_2, x_3]\!]^2$. Dabei sei der Potenzreihenmodul $K[\![x_1, x_2, x_3]\!]^s$ mit der graduiert lexikographischen Ordnung $<_\eta = (<_{deglex}, C)$ auf $\mathbb{N}^3 \times \{1,2\}$ mit $x_3 < x_2 < x_1$ versehen. Der Modul I ist x_3-regulär.

Bemerkung. Betrachtet man die algebraische Potenzreihe g genauer, so erkennt man, dass $x_3 \cdot e_1 + \left(x_3^2\sqrt{1+x_1x_2} + x_1x_2\sqrt{1+x_1x_2}\sqrt{1+x_1^2}\right) \cdot e_2$ eine reduzierte Standardbasis des Moduls I bzgl. der Monomordnung $<_\eta$ ist. Im Folgenden werden wir zeigen, dass auch der Algorithmus von Satz 7.1 dasselbe Resulat liefert.

Wie man leicht nachrechnen kann, ist

$$\begin{aligned}(H,G) \quad = \quad & ((y_1 + y_1y_2 - x_3, y_2 + \frac{1}{2}y_2^2 - \frac{1}{2}x_1x_2, \\ & y_3 + x_1x_2(y_4-1) - x_3^2, y_4 - \frac{1}{2}y_4^2 + \frac{1}{2}x_1^2), y_1e_1 + y_3e_2)\end{aligned}$$

ein Code der algebraischen Potenzreihe g. Dem Beweis von Satz 7.1 folgend betrachten wir den Modul $J = \langle H_i \cdot e_l, G \rangle \subseteq K[\![x,y]\!]^2$, wobei $1 \le i \le 4$, $1 \le l \le 2$, und wählen als Erweiterung $<_\varepsilon$ von $<_\eta$ die graduiert lexikographische Monomordnung $<_\varepsilon = (<_{deglex}, C)$ auf $\mathbb{N}^{3+4} \times \{1,2\}$ mit $y_1 < y_2 < y_3 < y_4 < x_3 < x_2 < x_1$. Mittels Satz 6.1 ergibt sich folgende minimale Standardbasis von J bzgl. $<_\varepsilon$:

$$H_i \cdot e_l, (x_3 - y_1y_2) \cdot e_1 + (x_1x_2 + x_3^2 - y_4x_1x_2) \cdot e_2.$$

Daraus folgt $\mathrm{in}(J) = \langle y_i \cdot e_l, x_3 \cdot e_1 \rangle$ und $\mathrm{co}(J) = K[\![x_1, x_2]\!] \cdot e_1 + K[\![x_1, x_2, x_3]\!] \cdot e_2$. Damit hat die partiell reduzierte Standardbasis von J die Form

$$\begin{aligned} b_{i1} \quad &= \quad y_i \cdot e_1 - b_{i1}^\circ - u_{i1}(x_1,x_2) \cdot e_1 - v_{i1}(x,y) \cdot e_2, \\ b_{i2} \quad &= \quad H_i \cdot e_2, \\ b \quad &= \quad x_3 \cdot e_1 - b^\circ - u(x_1,x_2) \cdot e_1 - v(x,y) \cdot e_2, \end{aligned}$$

wobei u_{i1}, u, v_{i1} und v in 0 verschwindende Potenzreihen und b_{i1}° und b° Polynomvektoren in $K \cdot e_1 \oplus K \cdot e_2$ sind. Daraus ergibt sich wegen $\mathrm{in}(b_{i1}) = y_i \cdot e_1$ und $\mathrm{in}(b) = x_3 \cdot e_1$ sofort

$$b_{i1}^\circ = b^\circ = 0.$$

Wir definieren nun die virtuelle partiell reduzierte Standardbasis von $J' = \langle H_i \cdot e_1, G \rangle$:

$$\begin{aligned} B_{i1} &= y_i \cdot e_1 - u_{i1} \cdot e_1 - v_{i1} \cdot e_2, \\ B &= x_3 \cdot e_1 - u \cdot e_1 - v \cdot e_2. \end{aligned}$$

Babylonische Division von $H_i \cdot e_1$ und $\tilde{G} := (x_3 - y_1 y_2) \cdot e_1 + (x_1 x_2 + x_3^2 - y_4 x_1 x_2) \cdot e_2$ durch B_{i1} und B bzgl. der Leuchttürme $y_i \cdot e_1$, $x_3 \cdot e_1$ und der Reichweiten $3 + 10 + i$, $3 + 10$ liefert:

$$\begin{aligned} R_{11} &= (u_{11} - u + u_{21}u_{11})e_1 + (v_{11} - v + u_{21}v_{11} + y_1 v_{21})e_2, \\ R_{21} &= (u_{21} + \tfrac{1}{2}u_{21}^2 - \tfrac{1}{2}x_1x_2)e_1 + (v_{21} + \tfrac{1}{2}y_2 v_{21} + \tfrac{1}{2}u_{21}v_{21})e_2, \\ R_{31} &= (u_{31} + x_1x_2u_{41} - x_1x_2 - u^2)e_1 + (v_{31} + x_1x_2v_{41} - x_3 v - uv)e_2, \\ R_{41} &= (u_{41} - \tfrac{1}{2}u_{41}^2 + \tfrac{1}{2}x_1^2)e_1 + (v_{41} - \tfrac{1}{2}y_4 v_{41} - \tfrac{1}{2}u_{41}v_{41})e_2, \\ R &= (u - u_{21}u_{11})e_1 + (v - u_{21}v_{11} - y_1 v_{21} + x_1x_2 + x_3^2 - y_4 x_1 x_2)e_2. \end{aligned}$$

Berechnet man noch die Babyreihen $u_{i1}(x_1, x_2)$, $u(x_1, x_2)$, $v_{i1}(x, y)$ und $v(x, y)$, so sieht man

$$u_{11}(x') = u(x') = v_{21}(x, y) = v_{41}(x, y) \equiv 0.$$

Dies vereinfacht den Muttercode der partiell reduzierten Standardbasis von J wesentlich. Es ergibt sich:

$$\begin{aligned} (U, V) = \; & ((u_{21} + \frac{1}{2}u_{21}^2 - \frac{1}{2}x_1x_2, u_{31} + x_1x_2u_{41} - x_1x_2, \\ & u_{41} - \frac{1}{2}u_{41}^2 + \frac{1}{2}x_1^2), (v_{11} - v + u_{21}v_{11}, \\ & v_{31} - x_3 v, v - u_{21}v_{11} + x_1x_2 + x_3^2 - y_4x_1x_2)). \end{aligned}$$

Nach dem Beweis von Satz 7.1 ist somit

$$((U, V, H), B)$$

ein Code der reduzierten Standardbasis $\tilde{g}$ von I. Will man diese explizit berechnen, so ergibt sich mit $v(x, y) = -x_3^2 + y_4x_1x_2 - x_1x_2 - (-1 + \sqrt{1 + x_1x_2})(x_3^2 - y_4x_1x_2 + x_1x_2)$

$$\tilde{g} = x_3 \cdot e_1 + \left(x_3^2\sqrt{1 + x_1x_2} + x_1x_2\sqrt{1 + x_1x_2}\sqrt{1 + x_1^2} \right) \cdot e_2.$$

Beispiel 7.6. Seien

$$g_1 := \frac{x_2}{1 + x_1} \cdot e_1 + x_1x_2 \cdot e_2 + x_1^3 \cdot e_3, \; g_2 := x_1^2x_2^2 \cdot e_1 + x_2 \cdot e_2 + x_1x_2^2 \cdot e_3$$

und $I = \langle g_1, g_2 \rangle \subseteq K[\![x_1, x_2]\!]^3$ der davon erzeugte Modul. Wie man schnell überprüfen kann, ist

$$\begin{aligned} (H, G) = \; & ((y_1 + y_1x_1 - x_2, y_2 - x_1x_2), \\ & (y_1 \cdot e_1 + y_2 \cdot e_2 + x_1^3 \cdot e_3, y_2^2 \cdot e_1 + x_2 \cdot e_2 + y_2x_2 \cdot e_3)) \end{aligned}$$

ein Familiencode von I.
Wir wollen nun eine reduzierte Standardbasis des x_2-regulären Moduls I bzgl. der Monomordnung $<_\eta = (<_{deglex}, C)$ mit $x_1 < x_2$ auf $\mathbb{N}^2 \times \{1, 2\}$ konstruieren. Dazu betrachten wir den Modul $J = \langle H_i \cdot e_l, G_k \rangle \subseteq K[\![x_1, x_2, y_1, y_2]\!]^3$, wobei $1 \leq i, k \leq 2$ und $1 \leq l \leq 3$. Dabei wählen wir als Fortsetzung von $<_\eta$ auf $K[\![x_1, x_2, y_1, y_2]\!]^3$ die

Monomordnung $<_\varepsilon = (<_{deglex}, C)$ mit $y_1 < y_2 < x_1 < x_2$. Mit Satz 6.1 ergibt sich folgende Standardbasis von J bzgl. $<_\varepsilon$:

$$H_i \cdot e_l,\ (x_2 - y_1x_1) \cdot e_1 + x_1x_2 \cdot e_2 + x_1^3 \cdot e_3,\ y_2^2 \cdot e_1 + x_2 \cdot e_2 + y_2x_2 \cdot e_3.$$

Setzen wir nun

$$\tilde{G} := ((x_2 - y_1x_1) \cdot e_1 + x_1x_2 \cdot e_2 + x_1^3 \cdot e_3, y_2^2 \cdot e_1 + x_2 \cdot e_2 + y_2x_2 \cdot e_3),$$

so ist $(H, \tilde{G})$ ein Familiencode der (noch nicht reduzierten) Standardbasis

$$\tilde{g} := \tilde{G}(x, h(x)) = (g_1, g_2)$$

von I bzgl. $<_\eta$.
Weiters gilt $\text{in}(J) = \langle y_i \cdot e_l, x_2 \cdot e_1, x_2 \cdot e_2 \rangle$ und folglich

$$\text{co}(J) = K[\![x_1]\!] \cdot e_1 \oplus K[\![x_2]\!] \cdot e_2 \oplus K[\![x_1, x_2]\!] \cdot e_3.$$

Daher hat die partiell reduzierte Standardbasis von J die Form

$$\begin{array}{lcl}
b_{il'} & = & y_i \cdot e_{l'} - b^\circ_{il'} - u_{il',1}(x_1) \cdot e_1 - u_{il',2}(x_1) \cdot e_2 - v_{il'}(x, y) \cdot e_3, \\
b_{i3} & = & H_i \cdot e_3, \\
b_1 & = & x_2 \cdot e_1 - b^\circ_1 - u_{1,1}(x_1) \cdot e_1 - u_{1,2}(x_1) \cdot e_2 - v_1(x, y) \cdot e_3, \\
b_2 & = & x_2 \cdot e_2 - b^\circ_2 - u_{2,1}(x_1) \cdot e_1 - u_{2,2}(x_1) \cdot e_2 - v_2(x, y) \cdot e_3,
\end{array}$$

wobei $1 \leq i, l' \leq 2$. Weiters sind dabei $u_{il',1}(x_1)$, $u_{il',2}(x_1)$, $u_{1,1}(x_1)$, $u_{1,2}(x_1)$, $u_{2,1}(x_1)$ und $u_{2,2}(x_1)$ in 0 verschwindende algebraische Potenzreihen in x_1 und $b^\circ_{il'}$, b°_1 und b°_2 Polynomvektoren in $K \cdot e_1 \oplus K \cdot e_2 \oplus K \cdot e_3$. Da aber $\text{in}(b_{il'}) = y_i \cdot e_{l'}$, $\text{in}(b_1) = x_2 \cdot e_1$ und $\text{in}(b_2) = x_2 \cdot e_2$ gelten soll, ergibt sich sofort

$$b^\circ_{il'} = b^\circ_1 = b^\circ_2 = 0.$$

Dem Beweis von Satz 7.1 folgend betrachten wir den Modul $J' = \langle H_i \cdot e_{l'}, G_k \rangle$. Dann definieren wir dessen virtuelle partiell reduzierte Standardbasis als

$$\begin{array}{lcl}
B_{il'} & = & y_i \cdot e_{l'} - u_{il',1} \cdot e_1 - u_{il',2} \cdot e_2 - v_{il'} \cdot e_3, \\
B_1 & = & x_2 \cdot e_1 - u_{1,1} \cdot e_1 - u_{1,2} \cdot e_2 - v_1 \cdot e_3, \\
B_2 & = & x_2 \cdot e_2 - u_{2,1} \cdot e_1 - u_{2,2} \cdot e_2 - v_2 \cdot e_3.
\end{array}$$

Babylonische Division von $H_i \cdot e_{l'}$ und $\tilde{G}_k$ durch $B_{il'}$, B_1 und B_2 bzgl. der Leuchttürme $y_i \cdot e_{l'}$, $x_2 \cdot e_1$, $x_2 \cdot e_2$ und der Reichweiten $n_{il'} = 2 + 18 + i$, $n_k = 2 + 18$ liefert folgende Reste:

$$\begin{array}{lcl}
R_{11} & = & (u_{11,1} + x_1u_{11,1} - u_{1,1})e_1 + (u_{11,2} + x_1u_{11,2} - u_{1,2})e_2 + \\
 & & (v_{11} + x_1v_{11} - v_1)e_3, \\
R_{12} & = & (u_{12,1} + x_1u_{12,1} - u_{2,1})e_1 + (u_{12,2} + x_1u_{12,2} - u_{2,2})e_2 + \\
 & & (v_{12} + x_1v_{12} - v_2)e_3, \\
R_{21} & = & (u_{21,1} - x_1u_{1,1})e_1 + (u_{21,2} - x_1u_{1,2})e_2 + \\
 & & (v_{21} - x_1v_1)e_3, \\
R_{22} & = & (u_{22,1} - x_1u_{2,1})e_1 + (u_{22,2} - x_1u_{2,2})e_2 + \\
 & & (v_{22} - x_1v_2)e_3, \\
R_1 & = & (u_{1,1} - x_1u_{11,1} + x_1u_{2,1})e_1 + (u_{1,2} - x_1u_{11,2} + x_1u_{2,2})e_2 + \\
 & & (v_1 - x_1v_{11,1} + x_1v_2 + x_1^3)e_3, \\
R_2 & = & (u_{2,1} + u_{21,1}^2 + u_{21,1}u_{22,1})e_1 + (u_{2,2} + u_{21,1}u_{21,2} + u_{21,2}u_{22,2})e_2 + \\
 & & (v_2 + v_{21}y_2 + x_2y_2)e_3.
\end{array}$$

Berechnet man die Babyreihen $u(x_1)$ und $v(x,y)$, so ergibt sich

$$u_{il',1}(x_1) = u_{il',2}(x_1) = u_{1,1}(x_1) = u_{1,2}(x_1) = u_{2,1}(x_1) = u_{2,2}(x_1) \equiv 0$$

und

$$\begin{aligned}
v_{11}(x_1) &= \frac{(x_1^2 - x_2y_2)x_1}{x_1^3y_2 + x_1^2y_2 - 1},\\
v_{12}(x_1) &= -\frac{y_2(x_1^5 + x_1^4 - x_2)}{(1+x_1)(x_1^3y_2 + x_1^2y_2 - 1)},\\
v_{21}(x_1) &= \frac{x_1^2(1+x_1)(x_1^2 - x_2y_2)}{x_1^3y_2 + x_1^2y_2 - 1},\\
v_{22}(x_1) &= -\frac{x_1y_2(x_1^5 + x_1^4 - x_2)}{x_1^3y_2 + x_1^2y_2 - 1},\\
v_1(x_1) &= \frac{(x_1^2 - x_2y_2)(1+x_1)x_1}{x_1^3y_2 + x_1^2y_2 - 1},\\
v_2(x_1) &= -\frac{y_2(x_1^5 + x_1^4 - x_2)}{x_1^3y_2 + x_1^2y_2 - 1}.
\end{aligned}$$

Daher ist

$$\begin{aligned}
(V,(B, H_i \cdot e_3)) = \;&((v_{11} + x_1v_{11} - v_1, v_{12} + x_1v_{12} - v_2, v_{21} - x_1v_1,\\
&v_{22} - x_1v_2, v_1 - x_1v_{11,1} + x_1v_2 + x_1^3, v_2 + v_{21}y_2 + x_2y_2),\\
&(B_{11}, B_{12}, B_{21}, B_{22}, B_1, B_2, H_1 \cdot e_3, H_2 \cdot e_3))
\end{aligned}$$

ein Familiencode der partiell reduzierten Standardbasis $b_{il'}$, b_1, b_2, $H_1 \cdot e_3$ und $H_2 \cdot e_3$ von J bzgl. $<_\varepsilon$. Setzt man in b_1 und b_2 für die Variablen y_1 und y_2 die Babyreihen $h_1(x) = \frac{x_2}{1+x_1}$ bzw. $h_2(x) = x_1x_2$ ein, so ergibt sich nach dem Beweis von Satz 7.1 die reduzierte Standardbasis von I bzgl. $<_\eta$:

$$\begin{aligned}
f_1 &:= b_1(x, h(x)) = x_2 \cdot e_1 - \tfrac{(x_1 - x_2^2)(1+x_1)x_1^2}{(x_1^4 + x_1^3x_2 - 1)} \cdot e_3,\\
f_2 &:= b_2(x, h(x)) = x_2 \cdot e_2 + \tfrac{x_1x_2(x_1^5 + x_1^4 - x_2)}{x_1^4x_2 + x_1^3x_2 - 1} \cdot e_3.
\end{aligned}$$

Satz 7.2. *Sei I ein x_n-regulärer Untermodul von $K[\![x]\!]^s = K[\![x_1, \ldots, x_n]\!]^s$, der von algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ erzeugt wird und mit der Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$ versehen ist. Weiters seien Familiencodes von $g_1, \ldots, g_r$ gegeben.*
Dann existiert für jeden algebraischen Potenzreihenvektor $f \in K[\![x]\!]^s$ ein endlicher Algorithmus, der aus einem Familiencode von f Familiencodes von algebraischen Potenzreihen $a_1, \ldots, a_r \in K[\![x]\!]$ und von einem algebraischen Potenzreihenvektor $c \in \mathrm{co}(I) \subseteq K[\![x]\!]^s$ berechnet, sodass

$$f = \sum_{k=1}^{r} a_k g_k + c,$$

eine formale Potenzreihendivision von f durch $I = \langle g_1, \ldots, g_r \rangle$ ist.

Bemerkung. Der Rest c der Division ist eindeutig und hängt nur von der Wahl der Monomordnung $<_\eta$ auf $K[\![x_1,\ldots,x_n]\!]^s$ ab.

Wir werden Satz 7.2 beweisen, indem wir zuerst aus $g_1,\ldots,g_r$ mit Hilfe von Satz 6.1 und 7.1 einen Familiencode einer reduzierten Standardbasis von I konstruieren.

Beweis. Auf Grund von Satz 6.1 können wir annehmen, dass der Modul I durch eine minimale Standardbasis $g_1,\ldots,g_r \in K[\![x]\!]^s$ mit Initialmonomvektoren $x_n^{d_k}\cdot e_k$ gegeben ist. Seien $(H,G)\in K[x,y]^p \times K[x,y]^{s\times r}$ ein Familiencode von $g_1,\ldots,g_r$ und $h=(h_1,\ldots,h_p)\in K[\![x]\!]^p$ der Babyreihenvektor des Muttercodes $H=(H_1,\ldots,H_p)$, also $g_k = G_k(x,h(x))$.

Nach Lemma 5.1 ist der Untermodul $J=\langle (y_i-h_i)\cdot e_l, g_k\rangle$ von $K[\![x,y]\!]^s$ gleich dem Untermodul $\langle H_i\cdot e_l, G_k\rangle$.
Sei $<_\varepsilon$ eine Erweiterung der Monomordnung $<_\eta$ auf $\mathbb{N}^{n+p}\times\{1,\ldots,s\}$ mit $y_i\cdot e_l <_\varepsilon \mathrm{in}(h_i)\cdot e_l$ und $y_i <_\varepsilon x_j$ für alle i,j,l (vgl. Lemma 5.2).
Auf Grund von Satz 7.1 können wir annehmen, dass wir bereits eine partiell reduzierte Standardbasis $b_{il'}$, $H_i\cdot e_{l''}$, b_k von J mit Initialmonomvektoren $y_i\cdot e_{l'}$, $y_i\cdot e_{l''}$, $x_n^{d_k}\cdot e_k$ bzgl. $<_\varepsilon$ besitzen ($1\le l', k\le r$, $r+1\le l''\le s$, $1\le i\le p$). Der Vatercode dieser partiell reduzierten Standardbasis besteht gerade aus der virtuellen partiell reduzierten Standardbasis $B_{il'}$, $H_i\cdot e_{l''}$, B_k von J. Der Muttercode von $b_{il'}$, $H_i\cdot e_{l''}$, b_k ist der Vektor (U,V) mit Komponenten $U_{il',mj}$, $U_{k,mj}$, $V_{il',m}$ und $V_{k,m}$. Die Komponenten $u_{il',mj}(x')$, $u_{k,mj}(x')$, $v_{il',m}(x,y)$ und $v_{k,m}(x,y)$ des zugehörigen Babyreihenvektors werden wir im Folgenden mit $(u(x'),v(x,y))$ abkürzen.

Wir wollen nun den algebraischen Potenzreihenvektor $f\in K[\![x]\!]^s$ durch den Untermodul $I=\langle g_k\rangle$ von $K[\![x]\!]^s$ dividieren. Dabei nehmen wir ohne Beschränkung der Allgemeinheit an, dass f denselben Babyreihenvektor h wie $g_1,\ldots,g_r$ besitzt (vgl. Konstruktion am Beginn von Kapitel 4. Dann schreiben wir f als

$$f = F(x,h(x))\in K[x,h]^s$$

mit Vatercode $F\in K[x,y]^s$.
Nun dividieren wir F babylonisch durch die Polynomvektoren $B_{il'}$ und B_k bzgl. der Leuchttürme $y_i\cdot e_{l'}$, $x_n^{d_k}\cdot e_k$ und der Reichweiten $n_{il'}=n+q+i$, $n_k=n+q$. Dabei sei q die Anzahl der u- und v-Variablen. Wir erhalten eine Zerlegung

$$F=\sum_{i,l'}\tilde{A}_{il'}\cdot B_{il'}+\sum_k \tilde{A}_k\cdot B_k + C \quad (*)$$

mit Polynomen $\tilde{A}_{il'},\tilde{A}_k\in K[x,u,v,y]$ und einem Polynomvektor $C\in \mathrm{co}(J')$, wobei $J'=\langle H_i\cdot e_{l'}, G_k\rangle$ (vgl. Beweis von Satz 7.1).
In Lemma 5.1 haben wir gezeigt, dass $J=\langle H_i\cdot e_l, G_k\rangle = \langle (y_i-h_i)\cdot e_l, g_k\rangle$ gilt. Weiters bilden die algebraischen Potenzreihenvektoren $b_{il'}$, $H_i\cdot e_{l''}$ und b_k laut unserer Annahme eine partiell reduzierte Standardbasis des Moduls J. Daher gilt insbesondere

$$\langle b_{il'}, H_i\cdot e_{l''}, b_k\rangle = \langle (y_i-h_i)\cdot e_l, g_k\rangle.$$

Ersetzt man in dieser Gleichung y_i durch h_i, so ergibt sich

$$\langle b_{il'}, H_i\cdot e_{l''}, b_k\rangle|_{y_i=h_i} = \langle (y_i-h_i)\cdot e_l, g_k\rangle|_{y_i=h_i} = \langle g_k\rangle = I.$$

Nach Satz 7.1 wissen wir aber, dass $b_k(x,h(x))$ eine reduzierte Standardbasis des Moduls I ist, d.h. $I=\langle b_k(x,h(x))\rangle\subseteq K[\![x]\!]^s$. Somit sind die Vektoren $b_{il'}$ und $H_i\cdot e_{l''}$

modulo $H\ K[x]$-Linearkombinationen von $b_1, \ldots, b_r$. Folglich sind die $B_{il'}(x,u,v,y)$ modulo $U_{il',mj}$, $U_{k,mj}$, $V_{il',m}$, $V_{k,m}$ und $H\ K[x]$-Linearkombinationen der Polynomvektoren $B_1, \ldots, B_r$.
Ersetzt man in der Zerlegung $(*)$ also y durch $h(x)$, u durch $u(x')$ und v durch $v(x,y)$, so erhält man eine Zerlegung

$$f = \sum_k a_k b_k + c$$

mit Potenzreihen $a_k \in K[\![x]\!]$ und einem Vektor $c \in K[\![x]\!]^s$. Klarerweise ist c ein algebraischer Potenzreihenvektor mit Muttercode (H,U,V) und Vatercode C. Weiters sind auch die $a_1, \ldots, a_r$ algebraische Potenzreihen. Denn deren Vatercodes $A_1, \ldots, A_r$ sind nach obigen Überlegungen gewisse $K[x]$-Linearkombinationen der Polynome $\tilde{A}_{il'}$ und $\tilde{A}_k$. Ihr Muttercode ist durch (H,U,V) gegeben.

Es bleibt zu zeigen, dass c ein Element von $\mathrm{co}(I)$ ist. Dazu entwickeln wir C folgendermaßen:

$$C = \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} C_{mj}(x',u) \cdot x_n^j \cdot e_m + \sum_{m=r+1}^{s} C_m(x,u,v,y) \cdot e_m,$$

wobei $C_{mj}(x',u)$ und $C_m(x,u,v,y)$ Polynome in (x',u) bzw. (x,u,v,y) sind.
Beachte, dass die Polynome $C_{mj}(x',u)$ nicht von v abhängen!
Ersetzt man in C die Variablen u, v und y durch $u(x')$, $v(x,y)$ und $h(x)$, so erhält man für c folgende Zerlegung:

$$c = \sum_{m=1}^{r} \sum_{j=0}^{d_m-1} C_{mj}(x',u(x')) \cdot x_n^j \cdot e_m + \sum_{m=r+1}^{s} C_m(x,u(x'),v(x),h(x)) \cdot e_m.$$

Daher gilt wie gewünscht $c \in \mathrm{co}(I)$. □

Beispiel 7.7. In diesem Beispiel wollen wir die algebraische Potenzreihe

$$f := x_1^2 + x_1^3 x_2 + x_2^3\sqrt{1+x_1x_2} + x_1x_2 \in K[\![x_1,x_2]\!]$$

durch das Ideal

$$I := \langle x_2^2\sqrt{1+x_1x_2}\rangle \subseteq K[\![x_1,x_2]\!]$$

dividieren.

Bemerkung. Da dieses Beispiel relativ einfach ist, können wir das Ergebnis der Division hier bereits erahnen: $f = x_2 \cdot x_2^2\sqrt{1+x_1x_2} + (x_1^2 + x_1^3x_2 + x_1x_2)$. Im Folgenden werden wir sehen, dass auch der Algorithmus von Satz 7.2 dasselbe Resultat liefert.

Als Monomordnung $<_\eta$ auf $K[\![x_1,x_2]\!]$ wählen wir die graduiert lexikographische Ordnung mit $x_2 < x_1$. Man kann leicht nachrechnen, dass

$$(H,G) = ((y_1 - x_2^2 - x_2^2y_2, y_2 + \frac{1}{2}y_2^2 - \frac{1}{2}x_1x_2), y_1)$$

ein Familiencode von I mit Babyreihenvektor

$$h(x) = (x_2^2\sqrt{1+x_1x_2}, -1 + \sqrt{1+x_1x_2})$$

ist. In Beispiel 7.1 haben wir gesehen, dass $g_1 := x_2^2\sqrt{1+x_1x_2}$ bereits eine minimale Standardbasis von I bzgl. $<_\eta$ ist. Weiters haben wir dort einen Code der reduzierten

Standardbasis des Ideals $J = \langle H_1, H_2, G\rangle$ bzgl. der Erweiterung $<_\varepsilon$ von $<_\eta$ auf die graduiert lexikographische Ordnung auf $\mathbb{N}^{2+2}$ mit $y_2 < y_1 < x_2 < x_1$ konstruiert:

$$(U, (B_1, B_2, B)) = (u_{2,1} - \frac{1}{2}x_1, (y_1, y_2 - u_{2,1}x_2, x_2^2)).$$

Folglich ist $b = x_2^2$ eine reduzierte Standardbasis von I bzgl. $<_\eta$.
Wir schreiben die algebraische Potenzreihe f als $f = F(x, h(x))$ mit

$$F = x_1^2(1 + y_2)^2 + x_2y_1 + x_1x_2.$$

Dem Beweis von Satz 7.2 folgend dividieren wir nun F babylonisch durch B_1, B_2 und B bzgl. der Leuchttürme y_1, y_2, x_2^2 und der Reichweiten $4, 5, 3$. Dabei erhalten wir die Zerlegung

$$F = \tilde{A}_1 \cdot B_1 + \tilde{A}_2 \cdot B_2 + \tilde{A} \cdot B + C \quad (*)$$

mit

$$\tilde{A}_1 = x_2,\ \tilde{A}_2 = x_1^2y_2 + 2x_1^2 + x_1^2u_{2,1}x_2,\ \tilde{A} = x_1^2u_{2,1}^2,$$
$$C = 2x_1^2u_{2,1}x_2 + x_1^2 + x_1x_2.$$

Ersetzt man in der Gleichung $(*)$ die Variablen y und $u_{2,1}$ durch $h(x)$ bzw. $u_{2,1}(x_1) = \frac{1}{2}x_1$, so erhält man

$$f = x_2\sqrt{1 + x_1x_2} \cdot b + (x_1^3x_2 + x_1^2 + x_1x_2)$$

mit Rest $c = x_1^3x_2 + x_1^2 + x_1x_2 \in \mathsf{co}(I)$.

Beispiel 7.8. Wir betrachten den algebraischen Potenzreihenvektor

$$f := (x^2\sqrt{1 + x + x^2} - x^2 + x^4) \cdot e_1 + (x^2\sqrt{1 + x} + x^3)e_2 \in K[\![x]\!]^2$$

und den Modul $I := \langle g_1, g_2\rangle \subseteq K[\![x]\!]^2$, wobei

$$g_1 := x^3\sqrt{1 + x + x^2} \cdot e_1 + x^2 \cdot e_2,\ g_2 := (x + x^2) \cdot e_1 + x\sqrt{1 + x} \cdot e_2.$$

Dabei sei $K[\![x]\!]^2$ mit der Monomordnung $<_\eta = (<_{lex}, C)$ versehen.
Wie wir in Beispiel 7.2 gesehen haben, ist

$$\begin{aligned}(H, \tilde{G}) \quad = \quad & ((y_1 - x^3y_2 - x^3, y_2 - \frac{1}{2}x - \frac{1}{2}x^2 + \frac{1}{2}y_2^2, y_3 - x^2,\\ & y_4 - x - x^2, y_5 + \frac{1}{2}y_5^2 - \frac{1}{2}x, y_6 - y_5^3 - 3y_5^2 - 2y_5),\\ & ((x^2 - y_2x^3)e_1 + (2y_5^2x + y_5^3x)e_2, (x + x^2)e_1 + (x + 2y_5^2 + y_5^3)e_2))\end{aligned}$$

ein Familiencode der minimalen Standardbasis

$$\begin{aligned}\tilde{g} \quad &= \quad \tilde{G}(x, h(x)) = ((x^2 + x^3 - x^3\sqrt{1 + x + x^2})e_1 + (x^2\sqrt{1 + x} - x^2), g_2)\\ &= \quad (x \cdot g_1 - g_2, g_2)\end{aligned}$$

von I bzgl. $<_\eta$. Weiters ist $H_i \cdot e_l$, $\tilde{G}_k$ eine Standardbasis des Moduls $J = \langle H_i \cdot e_l, G_k\rangle \subseteq K[\![x, y]\!]^2$ bzgl. der Erweiterung $<_\varepsilon = (<_{deglex}, C)$ von $<_\eta$ mit $y_6 < \ldots <$

$y_1 < x$. In Beispiel 7.2 haben wir außerdem folgenden Vatercode der reduzierten Standardbasis von J bzgl. $<_\varepsilon$ konstruiert

$$\begin{aligned} B_{il} &= y_i \cdot e_l - a_{il} \cdot x \cdot e_1, \\ B_1 &= x^2 \cdot e_1, \\ B_2 &= x \cdot e_2 + x \cdot e_1, \end{aligned}$$

wobei $a_{11} = a_{12} = a_{31} = a_{32} = 0$, $a_{21} = a_{51} = \frac{1}{2}$, $a_{22} = a_{52} = -\frac{1}{2}$, $a_{41} = a_{61} = 1$ und $a_{42} = a_{62} = -1$. Folglich ist

$$b_1 = x^2 \cdot e_1,\ b_2 = x \cdot e_2 + x \cdot e_1$$

eine reduzierte Standardbasis von I bzgl. $<_\eta$.
Um den algebraischen Potenzreihenvektor f durch das Ideal I zu dividieren, schreiben wir f als $f = F(x, h(x))$ mit

$$F = (x^2 y_2 + y_3^2) \cdot e_1 + (xy_6 + xy_4 - x^2) \cdot e_2.$$

Nun dividieren wir F babylonisch durch B_{il}, B_1 und B_2 bzgl. der Leuchttürme $y_i \cdot e_l$, $x_2^2 \cdot e_1$, $x_2 \cdot e_2$ und der Reichweiten $2 + i$, 2, 2. Es ergibt sich

$$F = x^2 \cdot B_{21} + y_3 \cdot B_{31} + x \cdot B_{42} + x \cdot B_{62} + (\frac{1}{2}x - 1) \cdot B_1 - x \cdot B_2.$$

Ersetzt man in dieser Gleichung die Variablen y_i durch die Potenzreihen $h_i(x)$, so erhält man

$$f = (\sqrt{1 + x + x^2} - 1 + x^2 - \sqrt{1 + x} - x) \cdot b_1 + (x\sqrt{1 + x} + x^2) \cdot b_2,$$

also $f \in I$.

Beispiel 7.9. In diesem Beispiel wollen wir den algebraischen Potenzreihenvektor

$$f := \left(\frac{x_1^2 x_2^2}{1 + x_1} + x_1 x_2 + x_1 \right) \cdot e_1 + \frac{x_2^2}{1 + x_1} \cdot e_2 + (x_1^2 x_2^2 + x_1^2 x_2) \cdot e_3$$

durch den Untermodul

$$I = \langle g_1, g_2 \rangle := \left\langle \frac{x_2}{1 + x_1} \cdot e_1 + x_1 x_2 \cdot e_2, x_1^2 x_2^2 \cdot e_1 + x_2 \cdot e_2 \right\rangle$$

von $K[\![x_1, x_2]\!]^2$ dividieren. In Beispiel 7.3 haben wir gezeigt, dass

$$(H, \tilde{G}) = ((y_1 + y_1 x_1 - x_2, y_2 - x_1 x_2), (y_1 e_1 + y_2 e_2, y_2^2 e_1 + x_2 e_2))$$

ein Code der minimalen Standardbasis

$$\tilde{g} = \tilde{G}(x, h(x)) = (g_1, g_2)$$

von I bzgl. der Monomordnung $<_\eta = (<_{deglex}, C)$ auf $\mathbb{N}^2 \times \{1, 2\}$ mit $x_1 < x_2$ ist. Weiters haben wir dort eine reduzierte Standardbasis des Moduls $J = \langle H_i \cdot e_l, \tilde{G}_k \rangle \subseteq K[\![x, y]\!]^2$ bzgl. der Erweiterung $<_\varepsilon = (<_{deglex}, C)$ mit $y_1 < y_2 < x_1 < x_2$ von $<_\eta$ konstruiert:

$$b_{il} = y_i \cdot e_l,\ b_1 = x_2 \cdot e_1,\ b_2 = x_2 \cdot e_2.$$

Ein Vatercode dieser reduzierten Standardbasis von J ist klarerweise $B_{il} = y_i \cdot e_l$, $B_1 = x_2 \cdot e_1$, $B_2 = x_2 \cdot e_2$. Nach Satz 7.1 ist dann b_1, b_2 eine reduzierte Standardbasis von I bzgl. $<_\eta$.
Um den algebraischen Potenzreihenvektor f durch den Modul I zu dividieren, schreiben wir f als $f = F(x, h(x))$ mit

$$F = (y_1 y_2 x_1 + x_1 x_2 + x_1) \cdot e_1 + (y1 x_2 + y_2^2 + x_1^3 x_2) \cdot e_2.$$

Babylonische Division von F durch B_{il}, B_1 und B_2 bzgl. der Leuchttürme $y_i \cdot e_l$, $x_2 \cdot e_1$, $x_2 \cdot e_2$ und der Reichweiten $2 + i$, 2, 2 liefert:

$$F \quad = \quad x_2 \cdot B_{12} + y_1 x_1 \cdot B_{21} + y_2 \cdot B_{22} + x_1 \cdot B_1 + x_1^3 \cdot B_2 + x_1 \cdot e_1.$$

Ersetzt man in der letzten Gleichung die Variable $y = (y_1, y_2)$ durch den Babyreihenvektor $h(x) = (\frac{x_2}{1+x_1}, x_1 x_2)$, so ergibt sich folgende Zerlegung von f

$$f = \left(x_1 + \frac{x_1^2 x_2}{1 + x_1} \right) \cdot b_1 + \left(x_1^3 + \frac{x_2}{1 + x_1} + x_1^2 x_2 \right) \cdot b_2 + x_1 \cdot e_1$$

mit Rest $c = x_1 \cdot e_1 \in \mathrm{co}(I)$.

Beispiel 7.10. Wir betrachten den algebraischen Potenzreihenvektor

$$f := \big((x^2 + x^3)x^3 + x^2 + x\big) \cdot e_1 + \big((x^2 + x^3)^4 x^3 + x^4 + x^2 + x\big) \cdot e_2 \in K[\![x]\!]^2$$

und den von

$$g := \big((x^2 + x^3)^2 x^2 + x\big) \cdot e_1 + \big(x^2 + x^3\big) \cdot e_2$$

erzeugten Untermodul $I = \langle g \rangle$ von $K[\![x]\!]^2$. Wie man leicht nachrechnen kann, ist

$$(H, G) = (y - x^2 - x^3, y \cdot e_1 + (x^2 y^2 + x) \cdot e_2)$$

ein Familiencode von g mit Babyreihe $h(x) = x^2 + x^3$. In Beispiel 7.4 haben wir gezeigt, dass

$$\tilde{G} = (x^2 + x^3) \cdot e_1 + (x + y^2 x^2) \cdot e_2$$

ein Vatercode der minimalen Standardbasis $\tilde{g} = \tilde{G}(x, h(x)) = g$ von I bzgl. der Monomordnung $<_\eta = (<_{lex}, C)$ ist. Weiters haben wir dort folgenden Familiencode der partiell reduzierte Standardbasis des Moduls $J = \langle H \cdot e_l, \tilde{G} \rangle \subseteq K[\![x, y]\!]^2$ bzgl. der Erweiterung $<_\varepsilon = (<_{deglex}, C)$ mit $y < x$ von $<_\eta$ auf $\mathbb{N}^{1+1} \times \{1, 2\}$ konstruiert:

$$\begin{aligned}(V, B) \quad = \quad & ((v_1 - xv - x^2 v, v + x^2 y v_1 + x^2 + x^3, y - x^2 - x^3), \\ & (y \cdot e_1 - v_1 \cdot e_2, H \cdot e_2, x \cdot e_1 - v \cdot e_2)).\end{aligned}$$

Aus dem Beweis von Satz 7.1 folgt, dass

$$b = x \cdot e_1 + v(x, h(x)) \cdot e_2 = x \cdot e_1 + \frac{x^2 + x^3}{1 + x(x^2 + x^3)^2} \cdot e_2$$

eine reduzierte Standardbasis von I bzgl. $<_\eta$ ist.
Um nun f durch I zu dividieren, führen wir die Babylonische Division des Vatercodes

$$F = (y^3 x^3 + x^2 + x) \cdot e_1 + (y^4 x^3 + x^4 + x^2 + x) \cdot e_2$$

von f durch $B_1 = y \cdot e_1 - v_1 \cdot e_2$ und $B = x \cdot e_1 - v \cdot e_2$ bzgl. der Leuchttürme $y \cdot e_1$, $x \cdot e_1$ und der Reichweiten 4, 3 durch:

$$F = y^2x^3 \cdot B_1 + (x+1) \cdot B + (y^4x^3 + x^4 + x^2 + x + y^2x^3v_1 + xv + v) \cdot e_2.$$

Ersetzt man in dieser Gleichung die Variablen y, v_1 und v durch

$$h(x) = x^2 + x^3,\ v_1(x) = -\frac{x(x+x^2)^2}{1+x(x^2+x^3)^2} \text{ bzw. } v(x) = -\frac{x^2+x^3}{1+x(x^2+x^3)^2},$$

so erhalten wir die Zerlegung

$$f = a \cdot b + c$$

von f mit Quotient

$$a = 1 + x + (x^2 + x^3)^3x^2$$

und Rest

$$c = \left((x^2+x^3)^4x^3 + x^4 + x^2 + x - \frac{(x+x^2)((x+x^2)^3x^6 - x^2 - x)}{1+x(x^2+x^3)^2}\right) \cdot e_2$$

in $\mathrm{co}(I)$.

7.2 Der allgemeine Fall

Wir werden die beiden folgenden Sätze 7.3 und 7.4 beweisen, indem wir zuerst aus $g_1, \ldots, g_r$ mit Hilfe der Sätze 7.1 und 7.2 sowie Induktion über die Anzahl der Variablen n einen Familiencode einer reduzierten Standardbasis von I konstruieren. Dann werden wir mittels Satz 7.2 den algebraischen Potenzreihenvektor f sukzessive durch die zuvor berechnete reduzierte Standardbasis von I dividieren. (Für die Endlichkeit des Algorithmus von Satz 7.4 ist es notwendig, dass wir f durch eine *reduzierte* Standardbasis von I dividieren.)

Satz 7.3. *Wir nehmen an, der von den algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ erzeugte und mit der Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$ versehene Modul $I \subseteq K[\![x]\!]^s$ erfüllt bzgl. $<_\eta$ Hironaka's Box-Bedingung. Dann kann man aus den Familiencodes der algebraischen Potenzreihenvektoren $g_1, \ldots, g_r$ mittels eines endlichen Algorithmus den Familiencode einer reduzierten Standardbasis von I bzgl. $<_\eta$ berechnen.*

Beweis. Die Idee des Beweises besteht darin, eine gegebene minimale Standardbasis von I, abhängig von den in den Initialmonomvektoren auftretenden Variablen, in zwei Gruppen zu zerlegen. Die erste Gruppe bestehe dabei aus jenen Erzeugern, deren Initialmonomvektoren reine x_n-Potenzen sind. In den Initialmonomvektoren der restlichen Erzeuger kommen stets auch andere Variablen vor.

Nach Satz 6.1 seien algebraische Potenzreihenvektoren $g_1, \ldots, g_r$ gegeben, die bereits eine minimale Standardbasis von I bilden. Auf Grund von Theorem 2 in [ACJHb] dürfen wir annehmen, dass $g_1, \ldots, g_r$ eine minimale Janet-Basis von I mit Reichweiten $n_1, \ldots, n_r$ sind. Wir ordnen $g_1, \ldots, g_r$ und permutieren die Komponenten von $K[\![x]\!]^s$ derart, dass für ein $t \leq r$ die Vektoren $g_1, \ldots, g_t$ bzgl. der gegebenen Monomordnung x_n-regulär mit Initialmonomvektoren $x_n^{d_k} \cdot e_k$ sind und dass in jedem der

Initialmonomvektoren der restlichen Vektoren $g_{t+1}, \ldots, g_r$ mindestens eine der Variablen $x_1, \ldots, x_{n-1}$ vorkommt. Wegen Lemma 3 in [ACJHb] sind die Reichweiten $n_{t+1}, \ldots, n_r$ von $g_{t+1}, \ldots, g_r$ alle $< n$. Dies impliziert

$$I = \sum_{k=1}^{t} K[\![x]\!] \cdot g_k + \sum_{k=t+1}^{r} K[\![x']\!] \cdot g_k.$$

Daher ist es in der nachfolgenden Division nicht notwendig, einen der algebraischen Potenzreihenvektoren $g_{t+1}, \ldots, g_r$ mit x_n zu multiplizieren.

Auf Grund von Satz 7.1 dürfen wir annehmen, dass die algebraischen Potenzreihenvektoren $g_1, \ldots, g_t$ bereits eine *reduzierte* Standardbasis des x_n-regulären Untermoduls $I_0 = \langle g_1, \ldots, g_t \rangle$ von $K[\![x]\!]^s$ bilden.
Mit Hilfe von Satz 7.2 können wir nun $g_{t+1}, \ldots, g_r$ mittels eines endlichen Algorithmus durch den x_n-regulären Modul $I_0 = \langle g_1, \ldots, g_t \rangle$ dividieren. Somit dürfen wir annehmen, dass die Vektoren $g_{t+1}, \ldots, g_r$ bereits in

$$M = \mathrm{co}(I_0) = \sum_{m=1}^{t} \sum_{j=0}^{d_m - 1} K[\![x']\!] \cdot x_n^j \cdot e_m + \sum_{m=t+1}^{s} K[\![x]\!] \cdot e_m$$

liegen. Da der Untermodul I nach Voraussetzung Hironaka's Box-Bedingung erfüllt, haben die Initialmonomvektoren von $g_{t+1}, \ldots, g_r$ ihren von null verschiedenen Eintrag im ersten Summanden

$$M_1 = \sum_{m=1}^{t} \sum_{j=0}^{d_m - 1} K[\![x']\!] \cdot x_n^j \cdot e_m$$

von M. Setzen wir nun

$$I' = \sum_{k=t+1}^{r} K[\![x']\!] \cdot g_k,$$

so gilt $I' \subseteq M$ und $\mathrm{in}(I') \subseteq M_1$.

Damit können wir nun folgendermaßen Induktion über n anwenden:

Als Erstes stellen wir fest, dass $\mathrm{in}(I')$ als Untermodul des freien endlichen $K[\![x']\!]$-Untermoduls M_1 wiederum Hironaka's Box-Bedingung erfüllt. Zweitens, es tritt keine Division im zweiten Summanden $M_2 = \sum_{m=t+1}^{s} K[\![x]\!] \cdot e_m$ von M auf. Damit können wir mittels Induktion über die Anzahl der Variablen n annehmen, dass wir wissen, wie man mittels eines endlichen Algorithmus, unter Zuhilfenahme von Codes, eine *reduzierte* Standardbasis des $K[\![x']\!]$-Untermoduls I' von M konstruiert. Diese Basis, betrachtet als Vektoren in $K[\![x]\!]^s$, bleibt bezüglich $g_1, \ldots, g_t$ reduziert, denn deren Elemente liegen in $M = \mathrm{co}(I_0)$.

Daher dürfen wir annehmen, dass $g_{t+1}, \ldots, g_r$ bereits eine reduzierte Standardbasis von I' bilden. Mittels Induktion über n können wir den Divisionsalgorithmus von Satz 7.2 auf I' als Untermodul von M anwenden. Daher wissen wir, wie man effektiv algebraische Potenzreihenvektoren in M durch I' dividiert.

Dies wenden wir nun auf die Reste $\overline{g_k} = x_n^{d_k} \cdot e_k - g_k$ von $g_1, \ldots, g_t$ an. Die algebraischen Potenzreihen $g_1, \ldots, g_t$ liegen in M, da sie eine reduzierte Standardbasis von I_0 sind und $M = \mathrm{co}(I_0)$ ist. Daher können wir die Reste $\overline{g_k}$ durch I' dividieren. Dies

erlaubt es, von Beginn an anzunehmen, dass die Vektoren $g_1, \ldots, g_t$ bzgl. $g_{t+1}, \ldots, g_r$ reduziert sind, d.h., dass $\overline{g_k}$ für $1 \leq k \leq t$ in $\mathrm{co}(I')$ liegen. Da $I \subseteq M = \mathrm{co}(I_0)$ gilt, bilden die neuen Vektoren $g_1, \ldots, g_t$ wieder eine reduzierte Standardbasis (der von ihnen erzeugte Modul kann verschieden von I_0 sein, aber sein Initialmodul ist derselbe). Insgesamt haben wir also die reduzierte Standardbasis $g_1, \ldots, g_r$ von I gefunden. Dies beweist Satz 7.3.

□

Satz 7.4. *Sei I ein Untermodul von $K[\![x]\!]^s = K[\![x_1, \ldots, x_n]\!]^s$, der von algebraischen Potenzreihenvektoren $g_1, \ldots, g_r \in K[\![x]\!]^s$ erzeugt wird. Wir nehmen an, dass I Hironaka's Box-Bedingung bzgl. einer Monomordnung $<_\eta$ auf $\mathbb{N}^n \times \{1, \ldots, s\}$ erfüllt. Weiters seien Familiencodes von $g_1, \ldots, g_r$ gegeben.*
Dann existiert für jeden algebraischen Potenzreihenvektor $f \in K[\![x]\!]^s$ ein endlicher Algorithmus, der aus einem Familiencode von f Familiencodes von algebraischen Potenzreihen $a_1, \ldots, a_r \in K[\![x]\!]$ und von einem algebraischen Potenzreihenvektor $c \in \mathrm{co}(I) \subseteq K[\![x]\!]^s$ berechnet, sodass

$$f = \sum_{k=1}^{r} a_k g_k + c,$$

eine formale Potenzreihendivision von f durch $I = \langle g_1, \ldots, g_r \rangle$ ist.

Bemerkung. Wie auch in Satz 7.2 ist der Rest c der Division eindeutig und hängt nur von der Wahl der Monomordnung $<_\eta$ auf $K[\![x_1, \ldots, x_n]\!]^s$ ab.

Beweis. Auf Grund von Satz 7.3 können wir annehmen, dass wir bereits einen Familiencode der reduzierten Standardbasis $g_1, \ldots, g_r$ des Untermoduls $I \subseteq K[\![x]\!]^s$ besitzen. Dann gehen wir ähnlich wie im Beweis von Satz 7.3 vor:
Wollen wir einen beliebigen algebraischen Potenzreihenvektor $f \in K[\![x]\!]^s$ durch den Untermodul $I = \langle g_1, \ldots, g_r \rangle \subseteq K[\![x]\!]^s$ dividieren, so können wir f zuerst mittels Satz 7.2 durch den Untermodul $I_0 = \langle g_1, \ldots, g_t \rangle$ (vgl. Konstruktion der reduzierten Standardbasis im Beweis von Satz 7.3), der ja x_n-regulär ist, dividieren. Dies liefert uns einen Rest in $M = \mathrm{co}(I_0)$. Dann können wir, unter Verwendung von Induktion über n und der Tatsache, dass $I' = \sum_{k=+1}^{r} K[\![x']\!] \cdot g_k$ als Untermodul von M wieder Hironaka's Box-Bedingung erfüllt, diesen Rest als Vektor in M durch I' dividieren. Der daraus resultierende Rest kann, via der Inklusion von M in $K[\![x]\!]^s$, als Vektor in $\mathrm{co}(I) \subseteq K[\![x]\!]^s$ interpretiert werden. Er wird mit der formalen Potenzreihendivision von f durch I in $K[\![x]\!]^s$ übereinstimmen. □

Beispiel 7.11. In diesem Beispiel wollen wir die algebraische Potenzreihe

$$f := x_3 + x_1x_2 + x_1x_2x_3 + x_2x_3^3 + x_3^4 + x_1x_2x_3^3 - x_1^3x_2^2x_3 - x_2^4x_3^2$$

durch das Ideal

$$I := \langle g_1, g_2, g_3 \rangle := \langle x_3^2 + x_1x_3^2 + x_2^3, x_2^2 + x_3x_2^2 + x_1^3, x_1x_2 + x_3^3 \rangle$$

von $K[\![x_1, x_2, x_3]\!]$ dividieren. Dabei sei $K[\![x_1, x_2, x_3]\!]$ mit der graduiert lexikographischen Ordnung auf $\mathbb{N}^3$ mit $x_1 < x_2 < x_3$ versehen.
Wie man sofort sieht, ist

$$\begin{aligned}(H, G) \quad = \quad & ((y_1 - x_3^2 - x_1x_3^2 - x_2^3, y_2 - x_2^2 - x_3x_2^2 - x_1^3, y_3 - x_1x_2 - x_3^3), \\ & (y_1, y_2, y_3))\end{aligned}$$

ein Familiencode von I.

Zuerst berechnen wir eine *minimale Standardbasis* von I (vergleiche Kapitel 6): Dazu erweitern wir die gegebene Ordnung auf die graduiert lexikographische Ordnung auf $\mathbb{N}^{3+3}$ mit $y_1 < y_2 < y_3 < x_1 < x_2 < x_3$ und berechnen eine minimale Standardbasis des Ideals $J := \langle H_1, H_2, H_3, G_1, G_2, G_3 \rangle \subseteq K[\![x, y]\!]$. Mit Hilfe von `Singular` ergibt sich

$$H_1,\ H_2,\ H_3,\ x_3^2 + x_1x_2^2 + x_2^3,\ x_2^2 + x_3x_2^2 + x_1^3,\ x_1x_2 + x_3^3,\ x_1^4.$$

Folglich ist $\tilde{G} = (x_3^2 + x_1x_2^2 + x_2^3, x_2^2 + x_3x_2^2 + x_1^3, x_1x_2 + x_3^3, x_1^4)$ ein Vatercode der minimalen Standardbasis

$$g_1,\ g_2, g_3, x_1^4$$

von I. Daraus ergibt sich

$$\text{in}(I) = \langle x_3^2, x_2^2, x_1x_2, x_1^4 \rangle.$$

Somit erfüllt das Ideal I Hironaka's Box-Bedingung.

Mit Hilfe von Theorem 2 und Lemma 2(b) aus [ACJHb] werden wir nun eine *minimale Janet-Basis* von I bzgl. der gegebenen Monomordnung konstruieren:
Dazu zerlegen wir das Initialideal $\text{in}(I) = \langle x_3^2, x_2^2, x_1x_2, x_1^4 \rangle \subseteq K[\![x]\!]$ von I, dem Beweis von Lemma 2(b) in [ACJHb] folgend, in eine disjunkte Summe:

$$\begin{aligned} \text{in}(I) \quad = \quad & K[\![x_1, x_2, x_3]\!] \cdot x_3^2 \oplus K[\![x_1, x_2]\!] \cdot x_2^2 \oplus K[\![x_1, x_2]\!] \cdot x_2^2x_3 \\ & \oplus K[\![x_1]\!] \cdot x_1x_2 \oplus K[\![x_1]\!] \cdot x_1x_2x_3 \oplus K[\![x_1]\!] \cdot x_1^4 \oplus K[\![x_1]\!] \cdot x_1^4x_3. \end{aligned}$$

Dem Beweis von Theorem 2 in [ACJHb] folgend berechnen wir nun mit Hilfe von `Singular` die Normalformen der Monome $x_3^2, x_2^2, x_2^2x_3, x_1x_2, x_1x_2x_3, x_1^4, x_1^4x_3$ bzgl. der zuvor berechneten Standardbasis g_1, g_2, g_3, x_1^4 von I (`Singular` verwendet dazu Mora's Tangentialkegel-Algorithmus). Wir erhalten die folgenden Reste:

$$0,\ -x_1^3 - x_2^2x_3,\ -x_1^3x_3 - x_2^2x_3^3,\ 0,\ 0,\ 0,\ 0.$$

Daher ist

$$\begin{gathered} P_1 := x_3^2,\ P_2 := x_2^2 + x_1^3 + x_2^2x_3,\ P_3 := x_2^2x_3 + x_1^3x_3 + x_2^2x_3^2, \\ P_4 = x_1x_2,\ P_5 := x_1x_2x_3,\ P_6 := x_1^4,\ P_7 := x_1^4x_3 \end{gathered}$$

eine Janet-Basis von I mit Leuchttürmen $x_3^2, x_2^2, x_2^2x_3, x_1x_2, x_1x_2x_3, x_1^4, x_1^4x_3$ und Reichweiten $3, 2, 2, 1, 1, 1, 1$.

Der nächste Schritt ist nun die Konstruktion einer *reduzierten Standardbasis* von I bzgl. der gegebenen graduierten Monomordnung:
Da $P_1, \ldots, P_7$ eine Janet-Basis von I mit Reichweiten $3, 2, 2, 1, 1, 1, 1$ sind, gilt insbesondere: $I = K[\![x_1, x_2, x_3]\!] \cdot P_1 + \sum_{k=2}^{7} K[\![x_1, x_2]\!] \cdot P_k$. Dem Beweis von Satz 7.3 folgend betrachten wir nun das Ideal

$$I_0 := \langle P_1 \rangle = \langle x_3^2 \rangle \subseteq K[\![x_1, x_2, x_3]\!].$$

Klarerweise ist P_1 bereits eine reduzierte Standardbasis von I.
Daher dividieren wir nun mit Hilfe von Satz 7.2 die restlichen Elemente $P_2, \ldots, P_7$ der Janet-Basis von I durch das x_3-reguläre Ideal $I_0 = \langle x_3^2 \rangle \subseteq K[\![x_1, x_2, x_3]\!]$ und erhalten:

$$P_2 = 0 \cdot P_1 + x_2^2 + x_1^3 + x_2^2 x_3,\ P_3 = x_2^2 \cdot P_1 + x_2^2 x_3 + x_1^3 x_3,$$
$$P_4 = 0 \cdot P_1 + x_1 x_2,\ P_5 = 0 \cdot P_1 + x_1 x_2 x_3,$$
$$P_6 = 0 \cdot P_1 + x_1^4,\ P_7 = 0 \cdot P_1 + x_1^4 x_3.$$

Wir setzen $\tilde{P}_3 := x_2^2 x_3 + x_1^3 x_3$ und $\tilde{P}_i := P_i$ für $i = 2, 4, 5, 6, 7$. Klarerweise gilt dann

$$\tilde{P}_2, \ldots, \tilde{P}_7 \in M =: \mathrm{co}(I_0) = K[\![x_1, x_2]\!] \oplus K[\![x_1, x_2]\!] \cdot x_3,$$

d.h., $\tilde{P}_2, \ldots, \tilde{P}_7$ sind bzgl. P_1 reduziert.
Wir betrachten nun das Ideal

$$I' = \sum_{k=2}^{7} K[\![x_1, x_2]\!] \cdot P_k \subseteq M$$

und suchen eine reduzierte Standardbasis davon. Dazu setzen wir zunächst

$$I_1 := \langle \tilde{P}_2, \tilde{P}_3 \rangle = \langle x_2^2 + x_1^3 + x_2^2 x_3, x_2^2 x_3 + x_1^3 x_3 \rangle \subseteq K[\![x_1, x_2]\!] \oplus K[\![x_1, x_2]\!] \cdot x_3.$$

Wie man leicht nachprüfen kann, ist

$$(x_2^2 + x_1^3) x_3,\ (x_2^2 + x_1^3) - x_1^3 x_3$$

eine Standardbasis des $K[\![x_1, x_2]\!]$-Ideals I_1 von M. Damit gilt: $\mathrm{in}(I') = \langle x_2^2 x_3, x_2^2 \rangle \subseteq M$. Folglich ist die reduzierte Standardbasis von I_1 von der Form

$$\begin{aligned} b_1 &= x_2^2 - b_1^\circ - u_{10}(x_1) - u_{11}(x_1) x_2 - \tilde{u}_{10}(x_1) x_3 - \tilde{u}_{11}(x_1) x_2 x_3, \\ b_2 &= x_2^2 x_3 - b_2^\circ - u_{20}(x_1) - u_{21}(x_1) x_2 - \tilde{u}_{20}(x_1) x_3 - \tilde{u}_{21}(x_1) x_2 x_3, \end{aligned}$$

wobei $b_1^\circ, b_2^\circ \in K \oplus K x_2 \oplus K x_3 \oplus K x_2 x_3$ und $u_{ij}, \tilde{u}_{ij}$ $(1 \leq i, j \leq 2)$ in 0 verschwindende Potenzreihen in x_2 sind. Da aber $\mathrm{in}(b_1) = x_2^2$ und $\mathrm{in}(b_2) = x_2^2 x_3$ gelten muss, ergibt sich sofort $b_1^\circ = b_2^\circ = 0$. Babylonische Division der Standardbasis $(x_2^2 + x_1^3) x_3,\ (x_2^2 + x_1^3) - x_1^3 x_3$ von I_1 durch die virtuelle reduzierte Standardbasis

$$\begin{aligned} B_1 &= x_2^2 - u_{10} - u_{11} x_2 - \tilde{u}_{10} x_3 - \tilde{u}_{11} x_2 x_3, \\ B_2 &= x_2^2 x_3 - u_{20} - u_{21} x_2 - \tilde{u}_{20} x_3 - \tilde{u}_{21} x_2 x_3 \end{aligned}$$

von I_1 bzgl. der Leuchttürme x_2^2, $x_2^2 x_3$ und der Reichweiten 10, 10 liefert die folgende reduzierte Standardbasis von $I' \subseteq M$:

$$b_1 = x_2^2 + x_1^3 - x_1^3 x_3,\ b_2 = x_2^2 x_3 + x_1^3 x_3.$$

Man beachte, dass $\tilde{P}_4, \ldots, \tilde{P}_7$ bereits in

$$N := \mathrm{co}(I_1) = K[\![x_1]\!] \oplus K[\![x_1]\!] \cdot x_2 \oplus K[\![x_1]\!] \cdot x_3 \oplus K[\![x_1]\!] \cdot x_2 x_3$$

liegen. Daher betrachten wir das Ideal

$$I'' = \sum_{k=4}^{7} (K[\![x_1]\!] \oplus K[\![x_1]\!] \cdot x_2) \cdot \tilde{P}_k \subseteq N.$$

Wie man sofort sieht, sind $\tilde{P}_4, \ldots, \tilde{P}_7$ bereits eine reduzierte Standardbasis des Ideals I''. Daher gilt: $\mathrm{in}(I'') = K \oplus \langle x_1^4, x_1 x_2, x_1^4 x_3, x_1 x_2 x_3 \rangle \subseteq N$ und

$$\begin{aligned} \mathrm{co}(I'') &= K \oplus K \cdot x_1 \oplus K \cdot x_1^2 \oplus K \cdot x_1^3 \oplus K \cdot x_2 \oplus K \cdot x_3 \\ &\quad \oplus K \cdot x_1 x_3 \oplus K \cdot x_1^2 x_3 \oplus K \cdot x_1^3 x_3 \oplus K \cdot x_2 x_3. \end{aligned}$$

Da die Reste $\overline{b_1} = x_2^2 - b_1 = -x_1^3 + x_1^3 x_3$ und $\overline{b_2} = x_2^2 x_3 - b_2 = x_1^3 x_3$ der reduzierten Standardbasis b_1, b_2 von I_1 bereits in co(I'') liegen, sind b_1 und b_2 bzgl. $\tilde{P}_4, \ldots, \tilde{P}_7$ reduziert. Damit bilden

$$b_1,\ b_2,\ x_1x_2,\ x_1x_2x_3,\ x_1^4,\ x_1^4x_3$$

eine reduzierte Standardbasis des $K[\![x_1, x_2]\!]$-Untermoduls I' von $M = K[\![x_1, x_2]\!] \oplus K[\![x_1, x_2]\!] \cdot x_3$.
Weil weiters $\overline{P_1} = x_3^2 - P_1 = 0$ gilt, ist die reduzierte Standardbasis P_1 von I_0 bereits bzgl. $b_1, b_2, \tilde{P}_4, \ldots, \tilde{P}_7$ reduziert. Folglich bilden

$$x_3^2,\ x_2^2 + x_1^3 - x_1^3x_3,\ x_2^2x_3 + x_1^3x_3,\ x_1x_2,\ x_1x_2x_3,\ x_1^4,\ x_1^4x_3$$

eine reduzierte Standardbasis des Ideals $I \subseteq K[\![x_1, x_2]\!]$ bzgl. der gegebenen graduierten Monomordnung.

Nun können wir mittels Satz 7.4 die *Division* der gegebenen algebraischen Potenzreihe

$$f = x_3 + x_1x_2 + x_1x_2x_3 + x_2x_3^3 + x_3^4 + x_1x_2x_3^3 - x_1^3x_2^2x_3 - x_2^4x_3^2$$

durch die soeben berechnete reduzierte Standardbasis des Ideals I durchführen:
Dazu dividieren wir f zuerst mit Hilfe von Satz 7.2 durch das x_3-reguläre Ideal $I_0 = \langle x_3^2 \rangle$. Es ergibt sich

$$f = (x_2x_3 + x_3^2 + x_1x_2x_3 - x_2^4) \cdot x_3^2 + (x_3 + x_1x_2 + x_1x_2x_3 - x_1^3x_2^2x_3).$$

Nun dividieren wir den Rest

$$R_0 := x_3 + x_1x_2 + x_1x_2x_3 - x_1^3x_2^2x_3 \in \text{co}(I_0) = K[\![x_1, x_2]\!] \oplus K[\![x_1, x_2]\!] \cdot x_3$$

dieser Division durch den Untermodul $I_1 = \langle x_2^2 + x_1^3 - x_1^3x_3, x_2^2x_3 + x_1^3x_3 \rangle \subseteq K[\![x_1, x_2]\!] \oplus K[\![x_1, x_2]\!] \cdot x_3$:

$$R_0 = -x_1^3 \cdot (x_2^2x_3 + x_1^3x_3) + (x_3 + x_1x_2 + x_1x_2x_3 + x_1^6x_3).$$

Division des Restes

$$R_1 := x_3 + x_1x_2 + x_1x_2x_3 + x_1^6x_3 \in \text{co}(I_1)$$

dieser Division durch $I'' = \langle \tilde{P}_4, \ldots, \tilde{P}_7 \rangle \subseteq \text{co}(I_1) = K[\![x_1]\!] \oplus K[\![x_1]\!] \cdot x_2 \oplus K[\![x_1]\!] \cdot x_3 \oplus K[\![x_1]\!] \cdot x_2x_3$ liefert

$$R_1 = 1 \cdot x_1x_2x_3 + x_1^2 \cdot x_1^4x_3 + (x_3 + x_1x_2)$$

mit Rest $R_2 := x_1x_2 \in \text{co}(I'') = \text{co}(I)$. Zusammengefasst ergibt sich

$$\begin{aligned} f \ &= \ (x_2x_3 + x_3^2 + x_1x_2x_3 - x_2^4) \cdot x_3^2 - x_1^3 \cdot (x_2^2x_3 + x_1^3x_3) \\ &\quad +1 \cdot x_1x_2x_3 + x_1^2 \cdot x_1^4x_3 + (x_3 + x_1x_2). \end{aligned}$$

Beispiel 7.12. Wir wollen den algebraischen Potenzreihenvektor

$$f := \left(x_2^3 + x_1x_2^2 + x_2\right) \cdot e_1 + \left(x_1x_2\sqrt{1 + x_1x_2} + x_1^2x_2 + x_2 + 1\right) \cdot e_2$$

durch den Modul $I := \langle g_1, g_2, g_3 \rangle \subseteq K[\![x_1, x_2]\!]^2$ dividieren, wobei

$$\begin{aligned} g_1 &:= x_2^2\sqrt{1+x_1x_2}\cdot e_1 + x_1^2 \cdot e_2, \\ g_2 &:= x_1^2 \cdot e_1 + x_2\sqrt{1+x_1+x_2^2}\cdot e_2, \\ g_3 &:= x_1 \cdot e_1 + x_1x_2 \cdot e_2. \end{aligned}$$

Dabei sei $K[\![x_1, x_2]\!]^2$ mit der Monomordnung $<_\eta = (<_{deglex}, C)$ mit $x_2 < x_1$ versehen.
Wie man leicht nachrechnen kann, ist

$$\begin{aligned} (H, G) = (&(y_1 - x_2^2 - y_2x_2^2, 2y_2 + y_2^2 - x_1x_2, \\ &y_3 - x_2 - y_4x_2, 2y_4 + y_4^2 - x_1 - x_2^2), \\ &(y_1e_1 + x_1^2e_2, x_1^2e_1 + y_3e_2, x_1e_1 + x_1x_2e_2)) \end{aligned}$$

ein Familiencode des Untermoduls I. Weiters ist die Monomordnung $<_\varepsilon = (<_{deglex}, C)$ mit $y_4 < y_3 < y_2 < y_1 < x_2 < x_1$ eine geeignete Erweiterung von $<_\eta$ auf $\mathbb{N}^{2+4} \times \{1, 2\}$.

Zur Berechnung einer *minimalen Standardbasis* von I bzgl. $<_\eta$ betrachten wir den Untermodul $J = \langle H_i \cdot e_1, H_i \cdot e_2, G_k \rangle \subseteq K[\![x_1, x_2, y_1, y_2, y_3, y_4]\!]^2$, wobei $1 \leq i \leq 4$. Es ist einfach nachzuprüfen, dass

$$\begin{gathered} H_ie_1,\ H_ie_2,\ x_2^2e_1 + x_1^2e_2 + y_2x_2^2e_1,\ x_2e_2 + y_4x_2e_2 + x_1^2e_1, \\ x_1e_1 + x_1x_2e_2,\ x_1^3e_2 + y_4y_1x_1x_2e_2 + y_1x_1^3e_1 \end{gathered}$$

eine minimale Standardbasis von J bzgl. $<_\varepsilon$ ist. Folglich ist

$$\begin{aligned} \tilde{G} := \big(&x_2^2e_1 + x_1^2e_2 + y_2x_2^2e_1, x_2e_2 + y_4x_2e_2 + x_1^2e_1, \\ &x_1e_1 + x_1x_2e_2, x_1^3e_2 + y_4y_1x_1x_2e_2 + y_1x_1^3e_1\big) \end{aligned}$$

ein Vatercode der minimalen Standardbasis

$$\begin{aligned} \tilde{g} &:= \tilde{G}(x, h(x)) \\ &= (g_1, g_2, g_3, g_4), \end{aligned}$$

wobei

$$g_4 = x_1^3x_2^2\sqrt{1+x_1x_2}\cdot e_1 + \left(x_1x_2^3\sqrt{1+x_1x_2}\left(\sqrt{1+x_1+x_2^2}-1\right) + x_1^3\right)\cdot e_2,$$

von I bzgl. $<_\eta$.

Mit Hilfe von Theorem 1 und Lemma 2(b) aus [ACJHb] konstruieren wir nun eine *minimale Janet-Basis* von I:
Dazu zerlegen wir den Initialmodul

$$\text{in}(J) = \langle y_i \cdot e_1, y_i \cdot e_2, x_2^2 \cdot e_1, x_2 \cdot e_2, x_1 \cdot e_1, x_1^3 \cdot e_2 \rangle$$

in die folgende direkte Summe:

$$\begin{aligned} \text{in}(J) = &K[\![x_1, x_2, y_1, y_2, y_3, y_4]\!] \cdot y_4e_1 \oplus K[\![x_1, x_2, y_1, y_2, y_3]\!] \cdot y_3e_1 \\ &\oplus K[\![x_1, x_2, y_1, y_2]\!] \cdot y_2e_1 \oplus K[\![x_1, x_2, y_1]\!] \cdot y_1e_1 \oplus K[\![x_1, x_2]\!] \cdot x_2^2e_1 \\ &\oplus K[\![x_1]\!] \cdot x_1x_2e_1 \oplus K[\![x_1]\!] \cdot x_1e_1 \\ &\oplus K[\![x_1, x_2, y_1, y_2, y_3, y_4]\!] \cdot y_4e_2 \oplus K[\![x_1, x_2, y_1, y_2, y_3]\!] \cdot y_3e_2 \\ &\oplus K[\![x_1, x_2, y_1, y_2]\!] \cdot y_2e_2 \oplus K[\![x_1, x_2, y_1]\!] \cdot y_1e_2 \oplus K[\![x_1, x_2]\!] \cdot x_2e_2 \\ &\oplus K[\![x_1]\!] \cdot x_1^3e_2. \end{aligned}$$

Dem Beweis von Theorem 2 in [ACJHb] folgend berechnen wir jetzt die Normalformen der Monomvektoren $y_ie_1, y_ie_2, x_2^2e_1, x_1x_2e_1, x_1e_1, x_2e_2, x_1^3e_2$ bzgl. der zuvor berechneten Standardbasis von J und erhalten die folgende Janet-Basis von J:

$$y_4e_1 + \tfrac{1}{2}x_1^2e_2 + \tfrac{1}{2}y_2x_2^2e_1 - \tfrac{1}{2}y_4x_1x_2e_2 - \tfrac{1}{2}x_1^3e_1,\ y_3e_1 - x_2e_1 - y_4x_2e_1,$$
$$y_2e_2,\ y_1e_1 - x_1^2e_2,\ x_2^2e_1 + x_1^2e_2 + y_2x_2^2e_1,\ x_1x_2e_1,\ x_1e_1,$$
$$y_4e_2 - \tfrac{1}{2}x_1e_2 + \tfrac{1}{2}y_4^2e_2 - \tfrac{1}{2}x_2^2e_2,\ y_3e_2,\ y_2e_2,\ y_1e_2,\ x_2e_2,\ x_1^3e_2.$$

Daher ist

$$x_2^2e_1 + x_1^2e_2 + h_2(x)x_2^2e_1,\ x_1x_2e_1,\ x_1e_1,\ x_2e_2,\ x_1^3e_2$$

eine Janet-Basis von I mit Leuchttürmen $x_2^2e_1, x_1x_2e_1, x_1e_1, x_2e_2, x_1^3e_2$ und Reichweiten $2, 1, 1, 2, 1$.

Somit setzen wir

$$P_1 := x_2^2e_1 + x_1^2e_2 + h_2(x)x_2^2e_1 = x_2^2\sqrt{1 + x_1x_2} \cdot e_1 + x_1^2 \cdot e_2$$
$$P_2 := x_2e_2,\ P_3 := x_1x_2e_1,\ P_4 := x_1e_1,\ P_5 := x_1^3e_2$$

und suchen nun eine *reduzierte Standardbasis* von

$$I = K[\![x_1, x_2]\!] \cdot P_1 \oplus K[\![x_1, x_2]\!] \cdot P_2 + K[\![x_1]\!] \cdot P_3 \oplus K[\![x_1]\!] \cdot P_4 \oplus K[\![x_1]\!] \cdot P_5.$$

Dazu betrachten wir, dem Beweis von Satz 7.3 folgend, zuerst den Untermodul

$$I_0 = \langle P_1, P_2 \rangle \subseteq K[\![x_1, x_2]\!]^2.$$

Dieser kann durch den Familiencode $(H_2, (x_2^2e_1 + x_1^2e_2 + x_2^2y_2e_1, x_2e_2))$ beschrieben werden und ist x_2-regulär. Somit können wir eine reduzierte Standardbasis von I_0 konstruieren, indem wir mittels Satz 7.1 eine reduzierte Standardbasis des Moduls

$$J_0 = \langle H_2 \cdot e_1, H_2 \cdot e_2, P_1, P_2 \rangle$$

berechnen. Nach einer längeren Rechnung ergibt sich die folgende reduzierte Standardbasis bzgl. der Monomordnung $<_\varepsilon$ von J_0:

$$\begin{aligned} b_1 &= x_2^2e_1 + x_1^2e_2, \\ b_2 &= x_2e_2, \\ b_3 &= y_2e_1 - \frac{1}{2}x_1x_2e_1 - \frac{1}{8}x_1^4e_2, \\ b_4 &= y_2e_2. \end{aligned}$$

Somit bilden b_1 und b_2 eine reduzierte Standardbasis von I bzgl. $<_\eta$. Weiters gilt:

$$M = \mathrm{co}(I_0) = K[\![x_1]\!] \cdot e_1 \oplus K[\![x_1]\!] \cdot x_2 \cdot e_1 \oplus K[\![x_1]\!] \cdot e_2$$

und $P_3, P_4, P_5 \in M$, d.h., P_3, P_4, P_5 sind bereits bzgl. b_1, b_2 reduziert.
Daher betrachten wir nun den Untermodul

$$I' = \sum_{k=3}^{5} K[\![x_1]\!] \cdot P_k$$

von M. Man sieht sofort, dass $P_3 = x_1 \cdot e_1$, $P_4 = x_1x_2 \cdot e_1$ und $P_5 = x_1^3 \cdot e_2$ bereits eine reduzierte Standardbasis dieses $K[\![x_1]\!]$-Untermoduls I' von M bilden.
Da die Reste $\overline{b_1} = x_2^2 \cdot e_1 - b_1 = -x_1^2 \cdot e_2$ und $\overline{b_2} = x_2 \cdot e_2 - b_2 = 0$ bereits in

$$\mathrm{co}(I') = K \cdot e_1 \oplus K \cdot e_2 \oplus K \cdot e_2 \oplus K \cdot x_1 \cdot e_2 \oplus K \cdot x_1^2 \cdot e_2$$

liegen, sind b_1 und b_2 schon bzgl. P_3, P_4, P_5 reduziert.
Zusammengefasst erhalten wir also die folgende reduzierte Standardbasis von I bzgl. $<_\eta$:

$$x_2^2 \cdot e_1 + x_1^2 \cdot e_2,\ x_2 \cdot e_2,\ x_1 \cdot e_1,\ x_1x_2 \cdot e_1,\ x_1^3 \cdot e_1.$$

Damit können wir nun die *Division* des gegebenen algebraischen Potenzreihenvektors

$$f := \left(x_2^3 + x_1x_2^2 + x_2\right) \cdot e_1 + \left(x_1x_2\sqrt{1 + x_1x_2} + x_1^2x_2 + x_2 + 1\right) \cdot e_2$$

mit Familiencode

$$(H_2, F) = (H_2, (x_2^3 + x_1x_2^2 + x_2)e_1 + (x_1x_2 + x_1x_2y_2 + x_1^2x_2 + x_2 + 1))$$

durch die reduzierte Standardbasis von I durchführen:
Dem Beweis von Satz 7.4 folgend dividieren wir dazu f zuerst durch den Untermodul $I_0 = \langle x_2^2e_1 + x_1^2e_2 + h_2(x)x_2^2e_1, x_2e_2\rangle$. Wie wir oben gesehen haben, bilden $x_2^2e_1 + x_1^2e_2$ und x_2e_2 eine reduzierte Standardbasis von I_0. Weiters ist (wie man leicht nachrechnen kann)

$$\begin{aligned} B_1 &= x_2^2e_1 - u_{33}e_2, \\ B_2 &= x_2e_2, \\ B_3 &= y_2e_1 - u_{12}x_2e_1 - u_{13}e_2, \\ B_2 &= y_2e_2, \end{aligned}$$

ein Vatercode und

$$U = (2u_{12} - x_1, 2u_{13} + u_{12}^2u_{33}, u_{33} + x_1^2)$$

ein Muttercode der reduzierten Standardbasis $b_1, \ldots, b_4$ von J_0. Daher dividieren wir nun dem Beweis von Satz 7.2 folgend den Vatercode F des algebraischen Potenzreihenvektors f durch die virtuelle reduzierte Standardbasis B_1, B_2, B_3, B_4 von J_0:

$$F = (x_2 + x_1)B_1 + (x_1 + x_1^2 + 1 + u_{33})B_2 + x_1x_2B_4 + x_1u_{33}e_2 + x_2e_1 + e_2.$$

Substituieren wir in dieser Zerlegung y_2 durch $h_2(x) = -1 + \sqrt{1 + x_1x_2}$ und $u = (u_{12}, u_{13}, u_{33})$ durch $u(x') = (u_{12}(x'), u_{13}(x'), u_{33}(x')) = (\frac{1}{2}x_1, \frac{1}{8}x_1^4, -x_1^2)$, so ergibt sich die folgende Zerlegung von f

$$f = (x_2 + x_1)b_1 + \left(x_1 + 1 + x_1(\sqrt{1 + x_1x_2} - 1)\right) b_2 + (x_2e_1 + e_2 - x_1^3e_2)$$

mit Rest

$$c := x_2 \cdot e_1 + e_2 - x_1^3 \cdot e_2 \in \mathrm{co}(I_0) = K[\![x_1]\!] \cdot e_1 \oplus K[\![x_1]\!] \cdot x_2 \cdot e_1 \oplus K[\![x_1]\!] \cdot e_2.$$

Dem Beweis von Satz 7.4 folgend dividieren wir diesen Rest c nun durch den Untermodul $I' = K[\![x_1]\!] \cdot P_3 + K[\![x_1]\!] \cdot P_4 + K[\![x_1]\!] \cdot P_5$ von $\mathrm{co}(I_0)$ und erhalten

$$c = -1 \cdot P_5 + (x_2 \cdot e_1 + e_2)$$

mit Rest $x_2e_1 + e_2 \in \mathrm{co}(I')$. Zusammengefasst ergibt sich also die folgende Zerlegung von f:

$$f = (x_2 + x_1)b_1 + \left(x_1 + 1 + x_1(\sqrt{1 + x_1x_2} - 1)\right) b_2 - 1 \cdot P_5 + (x_2 \cdot e_1 + e_2).$$

Beispiel 7.13. In diesem Beispiel wollen wir eine reduzierte Standardbasis des Moduls $I = \langle g_1, g_2, g_3 \rangle \subseteq K[\![x_1, x_2]\!]^3$ konstruieren, wobei

$$g_1 := x_2^2 e_1 + x_1^3 e_2 + x_1^4 x_2,\ g_2 := x_1 x_2 e_1 + x_2^3 e_2 + x_1^5 e_3,\ g_3 := x_2 e_2 + x_1^2 e_2.$$

Dabei sei $K[\![x_1, x_2]\!]^3$ mit der Monomordnung $<_\eta = (<_{deglex}, C)$ mit $x_1 < x_2$ versehen. Der Modul I erfüllt, wie wir unten sehen werden, Hironaka's Box-Bedingung. Daher können wir den Beweis von Satz 7.3 anwenden, um eine reduzierte Standardbasis von I zu konstruieren:

Dazu berechnen wir zuerst eine *minimale Standardbasis* von I bzgl. $<_\eta$:

$$x_2^2 e_1 + x_1^3 e_2 + x_1^4 x_2 e_3,\ x_2 e_2 + x_1^4 e_2,\ x_1 x_2 e_1 + x_2^3 e_2 + x_1^5 e_3,\ x_1^4 e_2 - x_2^4 e_2.$$

Daraus folgt sofort $\mathrm{in}(I) = \langle x_2^2 e_1, x_2 e_2, x_1 x_2 e_1, x_1^4 e_2 \rangle$ und somit

$$\begin{aligned} \mathrm{co}(I) &= K \cdot x_2 \cdot e_1 \oplus K[\![x_1]\!] \cdot e_1 \oplus K \cdot e_2 \oplus K \cdot x_1 \cdot e_2 \\ &\quad \oplus K \cdot x_1^2 \cdot e_2 \oplus K \cdot x_1^3 \cdot e_2 \oplus K[\![x_1, x_2]\!] \cdot e_3. \end{aligned}$$

Dies zeigt, dass der Modul I tatsächlich Hironaka's Box-Bedingung bzgl. $<_\eta$ erfüllt.

Der nächste Schritt ist die Konstruktion einer *minimalen Janet-Basis* von I:
Dazu zerlegen wir den Initialmodul $\mathrm{in}(I)$ von I mittels Lemma 2(b) in [ACJHb] in die folgende direkte Summe:

$$\mathrm{in}(I) = K[\![x_1, x_2]\!] \cdot x_2^2 e_1 \oplus K[\![x_1]\!] \cdot x_1 x_2 e_1 \oplus K[\![x_1, x_2]\!] \cdot x_2 e_2 \oplus K[\![x_1]\!] \cdot x_1^4 e_2.$$

Berechnung der Normalformen von $x_2^2 e_2$, $x_1 x_2 e_1$, $x_2 e_2$ und $x_1^4 e_2$ bzgl. der zuvor berechneten Standardbasis von I ergibt

$$-x_1^3 e_2 - x_1^4 x_2 e_3,\ -x_1^2 e_2,\ -x_1^5 e_3 - x_2^5 e_2, 0.$$

Damit bilden

$$\begin{aligned} P_1 &= x_2^2 e_1 + x_1^3 e_2 + x_1^4 x_2 e_3, \\ P_2 &= x_2 e_2 + x_1^2 e_2, \\ P_3 &= x_1 x_2 e_1 + x_1^5 e_3 + x_2^5 e_2, \\ P_4 &= x_1^4 e_2 \end{aligned}$$

nach Theorem 2 in [ACJHb] eine minimale Janet-Basis von I.

Um nun eine *reduzierte Standardbasis* von I zu konstruieren, betrachten wir, dem Beweis von Satz 7.3 folgend, den x_2-regulären Untermodul

$$I_0 := \langle P_1, P_2 \rangle \subseteq K[\![x_1, x_2]\!]^3.$$

Wie man leicht sieht, bilden P_1 und P_2 bereits eine reduzierte Standardbasis von I_0. Da der Vektor P_3 noch nicht bzgl. P_1 und P_2 reduziert ist, dividieren wir ihn mit Hilfe von Satz 7.2 durch $I_0 = \langle P_1, P_2 \rangle$ und erhalten

$$P_3 = (x_2^4 - x_1^2 x_2^3 + x_1^4 x_2^2 - x_1^6 x_2 + x_1^8) P_2 + (x_1 x_2 e_1 + x_1^5 e_3 - x_1^{10} e_2).$$

Daher gilt mit

$$\tilde{P}_3 := x_1 x_2 e_1 + x_1^5 e_3 - x_1^{10} e_2,\ \tilde{P}_4 := P_4,$$

für den von uns betrachteten Modul: $I = \langle P_1, P_2, P_3, P_4\rangle = \langle P_1, P_2, \tilde{P}_3, \tilde{P}_4\rangle$.
Dem Beweis von Satz 7.3 folgend müssen wir nun eine reduzierte Standardbasis des $K[\![x_1]\!]$-Untermoduls

$$I' = K[\![x_1]\!] \cdot \tilde{P}_3 + K[\![x_1]\!] \cdot \tilde{P}_4$$

von $M := \mathrm{co}(I_0) = K[\![x_1]\!] \cdot e_1 \oplus K[\![x_1]\!] \cdot x_2 \cdot e_1 \oplus K[\![x_1]\!] \cdot e_2 \oplus K[\![x_1, x_2]\!] \cdot e_3$ finden. Man kann leicht überprüfen, dass $\tilde{P}_3$ und $\tilde{P}_4$ bereits eine minimale Standardbasis von I' bilden. Daraus folgt $\mathrm{in}(I') = \langle x_1x_2e_1, x_1^4e_2\rangle$ und somit

$$\mathrm{co}(I') = Kx_2e_1 \oplus K[\![x_1]\!]e_1 \oplus Ke_2 \oplus Kx_1e_2 \oplus Kx_1^2e_2 \oplus Kx_1^3e_2 \oplus K[\![x_1, x_2]\!]e_3.$$

Folglich erfüllt der Initialmodul $\mathrm{in}(I')$ als $K[\![x_1]\!]$-Untermodul von $M_1 = K[\![x_1]\!] \cdot e_1 \oplus K[\![x_1]\!] \cdot x_2 \cdot e_1 \oplus K[\![x_1]\!] \cdot e_2$ wieder Hironaka's Box-Bedingung. Weiters ist die reduzierte Standardbasis von I' von der Gestalt

$$\begin{aligned} b_1 &= x_1x_2e_1 - v_1(x_1)e_1 - v_2(x_1)e_3, \\ b_2 &= x_1^4 \cdot e_2 \end{aligned}$$

(der Vektor $\tilde{P}_4$ ist bereits reduziert), wobei und $v_1(x_1)$ und $v_2(x_1)$ in 0 verschwindende algebraische Potenzreihen sind. Division von $\tilde{P}_3$ durch die virtuelle reduzierte Standardbasis

$$\begin{aligned} B_1 &= x_1x_2e_1 - v_1e_1 - v_2e_3, \\ B_2 &= x_1^4 \cdot e_2, \end{aligned}$$

von I' liefert

$$\tilde{P}_3 = B_1 - x_1^6B_2 + v_1e_1 + (v_2 + x_1^3)e_3.$$

Daraus ergibt sich die folgende reduzierte Standardbasis von I':

$$b_1 = x_1x_2e_1 + x_1^3e_3,\ b_2 = x_1^4e_2.$$

Da die Standardbasis P_1, P_2 des Untermoduls $I_0 \subseteq K[\![x_1, x_2]\!]^3$ bereits bzgl. b_1, b_2 reduziert ist, bilden

$$P_1 = x_2^2e_1 + x_1^3e_2 + x_1^4e_2e_3, P_2 = x_2e_2 + x_1^2e_2, b_1 = x_1x_2e_1 - x_1^3e_3, b_2 = x_1^4e_2$$

eine bzgl. $<_\eta$ reduzierte Standardbasis des Moduls I.

8 Appendix: Codes einiger algebraischer Potenzreihen

g	(H, G)
$\sqrt[3]{1+x}-1$	(y^3+3y^2+3y-x, y)
$\frac{1}{1+x+x^2}-1$	$(yx^2+yx+y+x+x^2, y)$
$x\sqrt{1+x}$	$((y_1-y_2^3-3y_2^2-2y_2, 2y_2+y_2^2-x), y_1)$
$-x\sqrt{1+x}$	$((y_1-y_2^3+3y_2^2-2y_2, 2y_2-y_2^2+x), y_1)$
$x^3\sqrt{1+x+x^2}$	$((y_1-x^3y_2-x^3, 2y_2+y_2^2-x-x^2), y_1)$
$(x^2+x)\sqrt{1+x^2}$	$((y_1-y_2^3-y_2^2-xy_2-x, 2y_2+y_2^2-x^2), y_1)$
$x_2^2\sqrt{1+x_1x_2}$	$((y_1-x_2^2-x_2^2y_2, 2y_2+y_2^2-x_1x_2), y_1)$
$x_1x_3\sqrt{1+x_1^2}-x_2^2$	$((y_1-x_1x_3y_2-x_1x_3+x_2^2, 2y_2+y_2^2-x_1^2), y_1)$
$x_1x_3\sqrt{1+x_1^2}+x_2^2$	$((y_1+x_1x_3y_2-x_1x_3-x_2^2, 2y_2-y_2^2+x_1^2), y_1)$
$\frac{x_3}{\sqrt{1+x_1x_2}}$	$((y_1+y_1y_2-x_3, 2y_2+y_2^2-x_1x_2), y_1)$
$x_3\sqrt{1+x_1+x_2^2}$	$((y_1-x_3-y_2x_3, 2y_2+y_2^2-x_2^2-x_1), y_1)$
$\frac{x_2^2}{x_1x_3+1}$	$(y_1+y_1x_1x_3-x_2^2, y_1)$
$x_3^2\sqrt{1+x_1x_2}-x_3^2$	$((y_1-x_3^2y_2, 2y_2+y_2^2-x_1x_2), y_1)$

Literatur

[ACJHa] M. Alonso, F. Castro-Jiménez, and H. Hauser. Effective algebraic power series. In preparation.

[ACJHb] M. Alonso, F. Castro-Jiménez, and H. Hauser. Polynomial echelons and babylonian division. Preprint.

[AMR92] M. Alonso, T. Mora, and M. Raimondo. A computational model for algebraic power series. *J. Pure Appl. Algebra*, 77(1):1–38, 1992.

[Art69] M. Artin. Algebraic approximation of structures over complete local rings. *Inst. Hautes Études Sci. Publ. Math.*, (36):23–58, 1969.

[dJP00] T. de Jong and G. Pfister. *Local analytic geometry*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 2000. Basic theory and applications.

[GP02] G.-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer-Verlag, Berlin, 2002. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[Hir77] H. Hironaka. Idealistic exponents of singularity. *Algebraic Geometry, The Johns Hopkins Centennial Lectures*, John Hopkins University Press:52–125, 1977.

[MPT92] T. Mora, G. Pfister, and C. Traverso. An introduction to the tangent cone algorithm. *Robotics and nonlinear geometry*, 6:199–270, 1992. Advances in computing research.

[Mum99] D. Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, expanded edition, 1999.

[Rui93] J. M. Ruiz. *The basic theory of power series*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1993.

[Sha94] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994.

[ZS75] O. Zariski and P. Samuel. *Commutative algebra. Vol. 1*. Springer-Verlag, New York, 1975.