Null-dimensionale Ideale und Ersetzungsregeln

Holger Bluhm

01. Juli

Diese Arbeit beschäftigt sich mit der Beschreibung von null-dimensionalen Idealen. Das verwendete Konzept wird durch die folgende exakte Sequenz ersichtlich:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & P \arrow[r, "\rho"] \arrow[d, "\varphi"'] & P/I \arrow[r] \arrow[dl, "\cong"] & 0 \\ & & V(O) & & \end{tikzcd}$$

In dem K-Vektorraum $P = K[x_1, \ldots, x_n]$ finden wir einen zu P/I isomorphen K-Untervektorraum $V(O)$. Dies induziert eine K-lineare surjektive Abbildung $\varphi : P \to V(O)$ mit $\ker(\varphi) = I$. Damit ist $V(O)$ ein zyklischer P-Modul erzeugt durch $\varphi(1)$ via n paarweise kommutierender Endomorphismen. Im Folgenden wollen wir die Abbildung φ benennen und genauer untersuchen.

Definition 1.1 *Sei I ein null-dimensionales Ideal in P und $\mathcal{O} = (h_1, \ldots, h_\mu)$ ein Tupel von Polynomen, so dass $\bar{\mathcal{O}} = (\bar{h}_1, \ldots, \bar{h}_\mu)$ eine Basis von P/I als K-Vektorraum ist. Bezeichne weiter $V(\mathcal{O})$ den von den Elementen von $\mathcal{O}$ erzeugten K-Vektorraum in P. Dann ist durch $\mathrm{NF}_{\mathcal{O},I} : P \to V(\mathcal{O})$, $\mathrm{NF}_{\mathcal{O},I}(f) = \sum_{i=1}^{\mu} a_i h_i$ mit $a_1, \ldots, a_\mu$ gegeben durch $\rho(f) = \sum_{i=1}^{\mu} a_i \bar{h}_i$ eine lineare Abbildung definiert. $\mathrm{NF}_{\mathcal{O},I}$ heißt* **Normalformabbildung** *bzgl. $(\mathcal{O}, I)$ und $\mathrm{NF}_{\mathcal{O},I}(f)$* **Normalform** *bzgl. $(\mathcal{O}, I)$. Existiert ein Algorithmus, der $\mathrm{NF}_{\mathcal{O},I}(f)$ für jedes $f \in P$ berechnet, so heißt $\mathrm{NF}_{\mathcal{O},I}$* **explizit***.*

Bemerkung 1.2 *Für die Normalformabbildung $\mathrm{NF}_{\mathcal{O},I}$ gelten folgende Eigenschaften:*

- (*a*) $f - \mathrm{NF}_{\mathcal{O},I}(f) \in I$ *für alle* $f \in P$,
- (*b*) $\mathrm{NF}_{\mathcal{O},I}(\mathrm{NF}_{\mathcal{O},I}(f)) = \mathrm{NF}_{\mathcal{O},I}(f)$ *für alle* $f \in P$,
- (*c*) $\mathrm{NF}_{\mathcal{O},I}(fg) = \mathrm{NF}_{\mathcal{O},I}(\mathrm{NF}_{\mathcal{O},I}(f)\mathrm{NF}_{\mathcal{O},I}(g))$ *für alle* $f, g \in P$,
- (*d*) $V(\mathcal{O})$ *ist ein durch* $\mathrm{NF}_{\mathcal{O},I}(1)$ *erzeugter zyklischer* P*-Modul.*

Korollar 1.3 *Seien I ein null-dimensionales Ideal in P, $\mathcal{O} = (t_1, \ldots, t_\mu)$ ein Tupel von Polynomen, so dass $\bar{\mathcal{O}} = (\bar{t}_1, \ldots, \bar{t}_\mu)$ eine Basis von P/I als K-Vektorraum ist, $w = \mathrm{NF}_{\mathcal{O},I}(1)$ und $M^{\mathcal{O}}_{x_1}, \ldots, M^{\mathcal{O}}_{x_n}$ die Multiplikationsmatrizen von P/I. Für $f \in P$ ist*

$$\mathrm{NF}_{\mathcal{O},I}(f) = \mathcal{O} \cdot f(M^{\mathcal{O}}_{x_1}, \ldots, M^{\mathcal{O}}_{x_n}) \cdot M^{\mathcal{O}}_w$$

und damit $\mathrm{NF}_{\mathcal{O},I}$ eine explizite Normalformabbildung bzgl. $(\mathcal{O}, I)$. □

Beispiel 1.4 Seien $N = \{(0,0), (0,-1), (1,0), (1,1), (-1,1)\} \subset \mathbb{Q}^2$, $I \subset P = \mathbb{Q}[x, y]$ das Verschwindungsideal von N und $\mathcal{O} = (1, x, y, x^2, y^2)$. Dann ist $(1, \bar{x}, \bar{y}, \bar{x}^2, \bar{y}^2)$ eine $\mathbb{Q}$-Basis von P/I. Es soll nun $\mathrm{NF}_{\mathcal{O},I}(x^6y^2)$ berechnet werden. Dazu bestimmen wir die Multiplikationsmatrizen $M^{\mathcal{O}}_x$ und $M^{\mathcal{O}}_y$ und erhalten

$$M_x^{\mathcal{O}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \qquad M_y^{\mathcal{O}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & \frac{1}{2} & 0 & \frac{1}{2} & 1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 1 & \frac{1}{2} & 0 \end{pmatrix},$$

wobei $w = (1,0,0,0,0)^{tr}$. Die Matrizen $M_x^{\mathcal{O}}$ und $M_y^{\mathcal{O}}$ kommutieren und mit Korollar 3.3 ist

$$\mathrm{NF}_{\mathcal{O},I}(x^6y^2) = \mathcal{O} \cdot (M_x^{\mathcal{O}})^6 (M_y^{\mathcal{O}})^2 \cdot w = \frac{1}{2}y + \frac{1}{2}y^2$$

Definition 1.5 *Sei O eine nicht-leere Menge von Potenzprodukten. O heißt* **Ordnungsideal**, *wenn für alle t' mit $t'|t$ für ein $t \in O$ auch $t' \in O$ gilt. Insbesondere ist $1 \in O$.*

Definition 1.6 *Ein Paar (g,t) heißt* **markiertes Polynom** *(g markiert durch t), wenn $g \in P\backslash\{0\}$ und $t \in \mathrm{supp}(g)$ mit Koeffizient 1 ist. Ist $\mathcal{G} = (g_1,\dots,g_\nu)$ ein Tupel von Polynomen $g_i \neq 0$, $\mathcal{T} = (t_1,\dots,t_\nu)$ ein Tupel von Potenzprodukten und sind $(g_1,t_1),\dots,(g_v,t_\nu)$ markierte Polynome, so heit $\mathcal{G}$ markiert durch $\mathcal{T}$.*

Definition 1.7 *Sei $\mathcal{G} = (g_1,\dots,g_\nu)$ ein Tupel von Polynomen $g_i \neq 0$ markiert durch $\mathcal{T} = (t_1,\dots,t_\nu)$ und $g,g' \in P$. Existieren ein $c \in K$, $t \in \mathbb{T}^n$ und ein Index $i \in \{1,\dots,\nu\}$, so dass $g' = g - ctg_i$ und $tt_i \notin \mathrm{supp}(g')$, so heißt g* **reduziert** *zu g' unter Benutzung der Ersetzungsregeln definiert durch die markierten Polynome (g_i,t_i). Für einen solchen Reduktionsschritt schreiben wir kurz $g \xrightarrow{g_i} g'$.*

Beispiel 1.8 Sei $P = K[x,y]$ und $\mathcal{G} = (g)$ mit $g = xy - x^2 - y^2$ markiert durch xy. Dann kann die Reduktionskette $x^2y \xrightarrow{g} x^3 + xy^2 \xrightarrow{g} x^3 + x^2y + y^3$ unendlich fortgesetzt werden.

Das Beispiel zeigt, dass wir für ein Terminieren der Reduktionen mehr benötigen. Dazu zunächst die folgende

Definition 1.9 *Sei $O = \{t_1,\dots,t_\mu\}$ ein Ordnungsideal. Dann heißt die Menge*

$$O^+ = \{t \in \mathbb{T}^n\backslash O \mid \exists\, i \in \{1,\dots,n\} \text{ mit } x_i t' = t \text{ für ein } t' \in O\}.$$

der **Rand** *von O (siehe auch Anhang).*

Definition 1.10 *Sei $\mathcal{P} = K\langle x_1,\dots,x_n\rangle$ der Ring der nicht-kommutativen Polynome in den Unbestimmten $x_1,\dots,x_n$ und $\pi : \mathcal{P} \to P$ der kanonische K-lineare Ringepimorphismus. Seien $x_1,\dots,x_n$ geordnet mit $x_1 > x_2 > \cdots > x_n$. Dann wird jeder kommutative Term t kanonisch repräsentiert durch $t = {x_1}^{a_1}{x_2}^{a_2}\cdots{x_n}^{a_n}$, und wir definieren mit $\lambda : P \to \mathcal{P}$ die K-lineare Abbildung, die jedem Term t den nicht-kommutativen Term ${x_1}^{a_1}{x_2}^{a_2}\cdots{x_n}^{a_n}$ zuordnet. Damit ist $\pi \circ \lambda = id_P$. Im Folgenden identifizieren wir $f \in P$ mit $\lambda(f) \in \mathcal{P}$.*

Definition 1.11 *Sei $\mathcal{O}$ ein Tupel von Termen in P, so dass O ein Ordnungsideal ist, und $\mathcal{O}^+ = (b_1,\dots,b_\nu)$ mit der zugrundeliegenden Menge O^+. Ferner sei $\mathcal{G} = (g_1,\dots,g_\nu)$ ein Tupel von Polynomen $g_i \neq 0$ markiert durch $\mathcal{O}^+$ mit $\mathrm{supp}(b_j - g_j) \subseteq O$ für $j = 1,\dots,\nu$. Dann definieren wir die K-lineare Abbildung $\mathrm{NR}_{O,G} : \mathcal{P} \to V(O)$ wie folgt:*

a) $\mathrm{NR}_{O,G}(\tau) = \pi(\tau)$, *falls* $\pi(\tau) \in O$,
b) $\mathrm{NR}_{O,G}(x_i\tau) = b_j - g_j$, *falls* $\pi(x_i\tau) = b_j \in O^+$ *und* $\pi(\tau) \in O$,
c) $\mathrm{NR}_{O,G}(x_i\tau) = \mathrm{NR}_{O,G}(x_i\mathrm{NR}_{O,G}(\tau))$, *falls weder a) noch b) eintritt.*

$\mathrm{NR}_{O,G}$ *ist wohldefiniert und heißt die* **normale Restabbildung** *bzgl.* (O,G). f *heißt* **irreduzibel** *bzgl.* (O,G), *wenn* $\mathrm{supp}(\pi(f)) \subseteq O$ *und damit* $\mathrm{NR}_{O,G}(f) = \pi(f)$ *gilt.*

Proposition 1.12 *Sei* $\mathcal{O}$ *ein Tupel von Termen in* P, *so dass* O *ein Ordnungsideal ist, und* $\mathcal{O}^+ = (b_1, \ldots, b_\nu)$ *mit der zugrundeliegenden Menge* O^+. *Ferner sei* $\mathcal{G} = (g_1, \ldots, g_\nu)$ *ein Tupel von Polynomen* $g_i \neq 0$ *markiert durch* $\mathcal{O}^+$ *mit* $\mathrm{supp}(b_j - g_j) \subseteq O$ *für* $j = 1, \ldots, \nu$, I *das von* $G = \{g_1, \ldots, g_\nu\}$ *erzeute Ideal und* $f \in \mathcal{P}$. *Dann gilt*

a) $\pi(f) - \mathrm{NR}_{O,G}(f) \in I$ *für alle* $f \in \mathcal{P}$,
b) $\mathrm{NR}_{O,G}(x_if) - \mathrm{NR}_{O,G}(fx_i) \in I$ *für alle* $f \in \mathcal{P}$, $i = 1, \ldots n$.

Beweis. b) folgt sofort aus a), denn wegen $\pi(x_if) = \pi(fx_i)$ ist $\mathrm{NR}_{O,G}(x_if) - \mathrm{NR}_{O,G}(fx_i) = \mathrm{NR}_{O,G}(x_if) - \pi(x_if) + \pi(fx_i) - \mathrm{NR}_{O,G}(fx_i) \in I$. Bleibt also noch a) zu zeigen.
Œ sei nun $f = \tau$ ein Term. Betrachte jetzt die drei Fälle aus der Definition von $\mathrm{NR}_{O,G}$.
Fall 1: $\pi(\tau) \in O$. Dann ist $\pi(\tau) - \mathrm{NR}_{O,G}(\tau) = 0 \in I$.
Fall 2: $\tau = x_i\tilde{\tau}$ mit $\pi(x_i\tilde{\tau}) = b_j \in O^+$, $\pi(\tilde{\tau}) \in O$. Dann folgt
$\pi(\tau) - \mathrm{NR}_{O,G}(\tau) = \pi(x_i\tilde{\tau}) - \mathrm{NR}_{O,G}(x_i\tilde{\tau}) = b_j - (b_j - g_j) = g_j \in I$.
Fall 3: $\tau = x_i\tilde{\tau}$ mit $\pi(\tilde{\tau}) \notin O$ und $\pi(\tau) \notin O$. Mit Induktion nach dem Grad von τ (Induktionsanfang klar wegen $\pi(1) \in O$) ist dann

$$\begin{aligned}
\mathrm{NR}_{O,G}(x_i\tilde{\tau}) &= \mathrm{NR}_{O,G}(x_i\mathrm{NR}_{O,G}(\tilde{\tau})) = \mathrm{NR}_{O,G}(x_i\sum_{t\in O} c_t t) = \sum_{t\in O} c_t\mathrm{NR}_{O,G}(x_it) \\
&\equiv \sum_{t\in O} c_t\pi(x_it) \pmod{I} = \pi(\sum_{t\in O} c_t x_i t) = \pi(x_i\mathrm{NR}_{O,G}(\tilde{\tau})) \\
&\overset{Ind.Vor.}{\equiv} \pi(x_i\pi(\tilde{\tau})) \pmod{I} = \pi(x_i\tilde{\tau}).
\end{aligned}$$

□

Beispiel 1.13 Wir betrachten wieder das Ordnungsideal $O = \{1, x, y, x^2, y^2\}$ mit dem Rand $O^+ = \{xy, x^3, y^3, x^2y, xy^2\}$. Sei nun $\mathcal{G} = (g_1, g_2, g_3, g_4, g_5) = (xy - x^2 - y^2, x^3 - x^2, y^3 - y^2, x^2y - x^2, xy^2 - y^2)$ ein Tupel von Polynomen markiert durch $\mathcal{O}^+$, welches ein Ideal I erzeugt. Dann ist $\mathrm{NR}_{O,G}(yx^2) = x^2$ und

$$\mathrm{NR}_{O,G}(x^2y) = \mathrm{NR}_{O,G}(x\mathrm{NR}_{O,G}(xy)) = \mathrm{NR}_{O,G}(x(x^2 + y^2)) = x^2 + y^2.$$

Damit folgt $y^2 = (x^2 + y^2) - x^2 = \mathrm{NR}_{O,G}(x^2y) - \mathrm{NR}_{O,G}(yx^2) \in I$ nach 1.12b).
Ferner lässt sich aus der Berechnung von $\mathrm{NR}_{O,G}(x^2y)$ eine Darstellung von y^2 in den Erzeugenden von I ermitteln. Wir erhalten

$$x^2y = x \cdot xy = x(x^2 + y^2 + g_1) = x^3 + xy^2 + xg_1 = g_2 + x^2 + g_5 + y^2$$

und damit $y^2 = g_4 - g_2 - g_5$.

Proposition 1.14 *Sei* I *ein null-dimensionales Ideal in* P, $O = \{t_1, \ldots, t_\mu\}$ *ein Ordnungsideal, so dass* $\bar{O} = \{\bar{t}_1, \ldots, \bar{t}_\mu\}$ *eine Basis von* P/I *als* K*-Vektorraum ist, und* $O^+ = \{b_1, \ldots, b_\nu\}$. *Dann gilt*

a) Für alle $j = 1, \ldots, \nu$ *existiert eine eindeutige Linearkombination* $\sum_{k=1}^{\mu} a_{kj}t_k$ *mit* $a_{kj} \in K$, $k \in \{1, \ldots, \mu\}$, $j \in \{1, \ldots, \nu\}$ *und* $g_j = b_j - \sum_{k=1}^{\mu} a_{kj}t_k \in I$.
b) Das Ideal I *wird von* $\{g_1, \ldots, g_\nu\}$ *erzeugt.*

Beweis. a) Da $\bar{O}$ eine Basis von P/I ist, lässt sich b_j in P/I eindeutig darstellen als $\bar{b}_j = \sum_{k=1}^{\mu} a_{kj}\bar{t}_k$, und damit ist $g_j := b_j - \sum_{k=1}^{\mu} a_{kj}t_k \equiv 0 \pmod I$, also $g_j \in I$.
Um b) zu zeigen, sei J das von $\{g_1, \ldots, g_\nu\}$ erzeugte Ideal. Zu beweisen ist nun, dass $J = I$ ist. Wegen $J \subseteq I$ bleibt noch $I \subseteq J$ zu zeigen. Wir zeigen dazu, dass $P = V(O) + J$ ist, also dass $t \in V(O) + J$ ist für alle Terme t. Mit Induktion nach $d = \deg(t)$:

d=0: $1 \in V(O)$, da O ein Ordnungsideal ist.

d-1$\rightarrow d$: Sei t ein Term vom Grad $d > 0$. Es existiert ein $l \in \{1, \ldots, n\}$, so dass $t = x_l t'$. t' hat Grad $d-1$ und nach Induktionsvoraussetzung gilt daher $t' = \sum_{i=1}^{\mu} a_i t_i + g$ mit $a_i \in K$ für $i = 1, \ldots, \mu$ und $g \in J$. Damit ist $t = \sum_{i=1}^{\mu} a_i x_l t_i + x_l g$.
Ist $x_l t_i \in O$ für alle $i \in \{1, \ldots, \mu\}$, so sind wir fertig. Ist andernfalls $x_l t_i \in O^+$ für ein $i \in \{1, \ldots, \mu\}$, so ist $x_l t_i = b_j = \sum_{k=1}^{\mu} a_{kj} t_k \in V(O) + J$ für ein $j \in \{1, \ldots, \nu\}$ und damit auch t. □

Definition 1.15 *In der Situation von 1.14 sei zusätzlich $\mathcal{O}^+ = (b_1, \ldots, b_\nu)$ mit zugrundeliegender Menge O^+ und $\mathcal{G} = (g_1, \ldots, g_\nu)$ markiert durch $\mathcal{O}^+$. Dann heißt das Paar $(\mathcal{G}, \mathcal{O}^+)$* **Randbasis** *von I bzgl. O.*

Beispiel 1.16 Sei wieder $O = \{1, x, y, x^2, y^2\}$ mit $O^+ = \{xy, x^3, y^3, x^2y, xy^2\}$. Dann ist $g_1 = xy - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2$, $g_2 = x^3 - x$, $g_3 = y^3 - y$, $g_4 = x^2y - \frac{1}{2}y - \frac{1}{2}y^2$ und $g_5 = xy^2 - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2$. Wir erhalten nun mit $F = (g_1, g_2, g_3, g_4, g_5)$ markiert durch $\mathcal{O}^+$ die Randbasis von I bzgl. O.

Definition 1.17 *Sei $\mathcal{O} = (t_1, \ldots, t_\mu)$, so dass O ein Ordnungsideal ist, $\mathcal{O}^+ = (b_1, \ldots, b_\nu)$ mit zugrundeliegender Menge O^+ und $\mathcal{G} = (g_1, \ldots, g_\nu)$ ein Tupel von Polynomen $g_i \neq 0$ markiert durch $\mathcal{O}^+$ mit $\operatorname{supp}(g_k - b_k) \subseteq O$ für $k = 1, \ldots, \nu$. Wir konstruieren nun Matrizen $\mathcal{M}_1, \ldots, \mathcal{M}_n \in \operatorname{Mat}_\mu(K)$ wie folgt. Ist $x_k t_j \in O$, dann ist $(0, \ldots, 0, 1, 0, \ldots, 0)^{tr}$ die j-te Spalte von $\mathcal{M}_k$ mit der 1 an der dem Potenzprodukt $x_k t_j$ entsprechenden Position in $\mathcal{O}$. Ist $x_k t_j \in O^+$, dann ist $x_k t_j = b_i$ für ein $i \in \{1, \ldots, \nu\}$, und die j-te Spalte von $\mathcal{M}_k$ besteht aus den Koeffizienten von $(t_1, \ldots, t_\mu)$ in der Darstellung von $b_i - g_i$ als Linearkombination der Elemente von O. Die Matrizen $\mathcal{M}_1, \ldots, \mathcal{M}_n$ heißen die zu $(\mathcal{G}, \mathcal{O}^+)$* **assoziierten Matrizen***.*

Es gibt nun einen interessanten Zusammenhang zwischen der normalen Restabbildung $\mathrm{NR}_{O,G}$ und den zu $(\mathcal{G}, \mathcal{O}^+)$ assoziierten Matrizen.

Proposition 1.18 *Sei $\mathcal{O} = (t_1, \ldots, t_\mu)$, so dass O ein Ordnungsideal ist, $t_1 = 1$, $\mathcal{O}^+ = (b_1, \ldots, b_\nu)$ mit zugrundeliegender Menge O^+ und $\mathcal{G} = (g_1, \ldots, g_\nu)$ ein Tupel von Polynomen $g_i \neq 0$ markiert durch $\mathcal{O}^+$ mit $\operatorname{supp}(g_j - b_j) \subseteq O$ für $j = 1, \ldots, \nu$. Ferner seien $\mathcal{M}_1, \ldots, \mathcal{M}_n \in \operatorname{Mat}_\mu(K)$ die zu $(\mathcal{G}, \mathcal{O}^+)$ assoziierten Matrizen. Dann gilt*

$$\mathrm{NR}_{O,G}(x_{i_1} x_{i_2} \cdots x_{i_s}) = \mathcal{O} \cdot \mathcal{M}_{i_1} \mathcal{M}_{i_2} \cdots \mathcal{M}_{i_s} \cdot \mathcal{M}_{t_1}^{\mathcal{O}}.$$

für jedes nicht-kommutative Potenzprodukt $x_{i_1} x_{i_2} \cdots x_{i_s}$.

Beweis. Wir zeigen die Behauptung mit Induktion nach dem Grad d.

d=0: Wegen $t_1 = 1$ ist $\mathrm{NR}_{O,G}(1) = 1 = \mathcal{O} \cdot \mathcal{M}_{t_1}^{\mathcal{O}}$.

d-1$\rightarrow d$: Sei $\tau = x_{i_1} x_{i_2} \cdots x_{i_d}$. Nach Induktionsvoraussetzung gilt $\mathrm{NR}_{O,G}(\tau) = \mathrm{NR}_{O,G}(x_{i_1} \mathrm{NR}_{O,G}(x_{i_2} \cdots x_{i_d})) = \mathrm{NR}_{O,G}(x_{i_1} \mathcal{O} \cdot \mathcal{M}_{i_2} \cdots \mathcal{M}_{i_d} \cdot \mathcal{M}_{t_1}^{\mathcal{O}})$.
Bezeichnen wir mit v den Spaltenvektor $\mathcal{M}_{i_2} \cdots \mathcal{M}_{i_d} \cdot \mathcal{M}_{t_1}^{\mathcal{O}}$, dann ist

$\mathrm{NR}_{O,G}(\tau) = \mathrm{NR}_{O,G}(x_{i_1}\mathcal{O} \cdot v) = \mathrm{NR}_{O,G}(x_{i_1}(v_1 t_1 + \ldots + v_\mu t_\mu))$. Wir müssen nun zeigen, dass $\mathrm{NR}_{O,G}(x_{i_1}\mathcal{O} \cdot v) = \mathcal{O} \cdot \mathcal{M}_{i_1} \cdot v$ gilt. Wegen der Linearität von $\mathrm{NR}_{O,G}$ reicht es $\mathrm{NR}_{O,G}(x_{i_1} t_j) = \mathcal{O} \cdot \mathcal{M}_{i_1} \cdot \mathcal{M}^{\mathcal{O}}_{t_j}$ für $j = 1, \ldots, \mu$ zu zeigen. Dies jedoch ist klar, da $\mathrm{NR}_{O,G}(x_{i_1} t_j) = \sum_{k=1}^{\mu} a_k t_k$ mit $(a_1, \ldots, a_\mu)^{tr}$ j-te Spalte von $\mathcal{M}_{i_1}$. □

Beispiel 1.19 Wir betrachten wieder das Beispiel 1.13. Für die zu $(\mathcal{G}, \mathcal{O}^+)$ assoziierten Matrizen erhalten wir

$$\mathcal{M}_x = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad \mathcal{M}_y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Eine Berechnung von $\mathcal{M} = {\mathcal{M}_x}^2 \mathcal{M}_y - \mathcal{M}_y {\mathcal{M}_x}^2$ ergibt

$$\mathcal{M} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Nach der obigen Proposition ist nun $\mathrm{NR}_{O,G}(x^2 y - y x^2) = (1, x, y, x^2, y^2) \cdot \mathcal{M} \cdot \mathcal{M}^{\mathcal{O}}_{t_1} = y^2$, was dem Ergebnis von Beispiel 1.13 entspricht.

Theorem 1.20 *Sei $\mathcal{O} = (t_1, \ldots, t_\mu)$, so dass O ein Ordnungsideal ist, $t_1 = 1$, $\mathcal{O}^+ = (b_1, \ldots, b_\nu)$ mit zugrundeliegender Menge O^+ und $\mathcal{G} = (g_1, \ldots, g_\nu)$ ein Tupel von Polynomen $g_i \neq 0$ markiert durch $\mathcal{O}^+$ mit $\mathrm{supp}(g_j - b_j) \subseteq O$ für $j = 1, \ldots, \nu$. Ferner sei I das von $G = \{g_1, \ldots, g_\nu\}$ erzeugte Ideal. Dann sind die folgenden Aussagen äquivalent:*

a) Die Menge $\bar{O} = \{\bar{t}_1, \ldots, \bar{t}_\mu\}$ ist eine Basis von P/I als K-Vektorraum.
b) Das Paar $(\mathcal{G}, \mathcal{O}^+)$ ist die Randbasis von I bzgl. O.
c) Die zu $(\mathcal{G}, \mathcal{O}^+)$ assoziierten Matrizen $\mathcal{M}_1, \ldots, \mathcal{M}_n$ sind paarweise kommutierend.

Beweis.
"a) ⇒ b)": Sei $\bar{O} = \{\bar{t}_1, \ldots, \bar{t}_\mu\}$ eine Basis von P/I als K-Vektorraum. Dann ist I ein null-dim. Ideal und nach 1.14 lässt sich eine Randbasis $(\mathcal{G}', \mathcal{O}^+)$ von I mit $\mathcal{G}' = (g'_1, \ldots, g'_\nu)$ berechnen und $g'_j = b_j - \sum_{k=1}^{\mu} a'_{kj} t_k \in I$. Wegen $g_j = b_j - \sum_{k=1}^{\mu} a_{kj} t_k$ ist $\bar{b}_j = \sum_{k=1}^{\mu} a_{kj} \bar{t}_k = \sum_{k=1}^{\mu} a'_{kj} \bar{t}_k$ in P/I. Also folgt $a_{kj} = a'_{kj}$ für alle $k = 1, \ldots, \mu$ und damit $g_j = g'_j$ für $j = 1, \ldots, \nu$. Also ist $\mathcal{G}' = \mathcal{G}$ und $(\mathcal{G}, \mathcal{O}^+)$ eine Randbasis von I bzgl. O.

"b) ⇒ c)": Sei nun $(\mathcal{G}, \mathcal{O}^+)$ die Randbasis von I bzgl. O. Dann ist $\bar{O}$ eine Basis von P/I und wir definieren $\mathrm{NF}_{O,I} : P \to V(O)$. Für $k = 1, \ldots, n$ und $j = 1, \ldots, \mu$ ist $x_k t_j \in O$ oder $x_k t_j \in O^+$. Daher ist $\mathrm{NF}_{O,I}(x_k t_j) = \mathrm{NR}_{O,G}(x_k t_j)$ und mit 1.3 und 1.18 erhalten wir

$$\mathcal{O} \cdot \mathcal{M}^{\mathcal{O}}_{x_k} \cdot t_j(M^{\mathcal{O}}_{x_1}, \ldots, \mathcal{M}^{\mathcal{O}}_{x_n}) \cdot \mathcal{M}^{\mathcal{O}}_{e_1} = \mathcal{O} \cdot \mathcal{M}_k \cdot t_j(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot \mathcal{M}^{\mathcal{O}}_{t_1},$$

also $\mathcal{O} \cdot \mathcal{M}^{\mathcal{O}}_{x_k} \cdot \mathcal{M}^{\mathcal{O}}_{t_j} = \mathcal{O} \cdot \mathcal{M}_k \cdot \mathcal{M}^{\mathcal{O}}_{t_j}$. Aufgrund der linearen Unabhängigkeit der Elemente in $\bar{O}$ folgt nun die Gleichheit der j-ten Spalte von $\mathcal{M}^{\mathcal{O}}_{x_k}$ und $\mathcal{M}_k$. Für $j = 1, \ldots, \mu$ ergibt sich damit $\mathcal{M}_k = \mathcal{M}^{\mathcal{O}}_{x_k}$ für $k = 1, \ldots, n$. Wir wissen, dass $\mathcal{M}_{x_1}^{\mathcal{O}}, \ldots, \mathcal{M}_{x_n}^{\mathcal{O}}$ paarweise kommutieren und damit auch die zu $(\mathcal{G}, \mathcal{O}^+)$ assozierten Matrizen $\mathcal{M}_1, \ldots, \mathcal{M}_n$.

"c) $\Rightarrow$ a)": Seien $\mathcal{M}_1, \ldots, \mathcal{M}_n$ die zu $(\mathcal{G}, \mathcal{O}^+)$ assozierten, paarweise kommutierenden Matrizen. Mit 1.18 können wir dann eine K-lineare Abbildung $\varphi : P \to V(O)$ definieren. Zu zeigen ist nun die Surjektivität von φ. Dafür genügt es, $\varphi(t_i) = t_i$ für $i = 1, \ldots, \mu$ zu zeigen. Mit Induktion nach dem Grad d von t_i:

d=0: Für $t_i = 1$ ist nichts zu zeigen.

d-1$\rightarrow d$: Sei nun $d = deg(t_i) > 0$. Es existiert ein $k \in \{1, \ldots, n\}$, so dass $t_i = x_k t_j$ mit $t_j \in O$. Dann ist

$\varphi(t_i) = \mathcal{O} \cdot \mathcal{M}_k \cdot t_j(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot \mathcal{M}_{t_1}^{\mathcal{O}} = \mathcal{O} \cdot \mathcal{M}_k \cdot \mathcal{M}_{t_j}^{\mathcal{O}}$.

Nun ist aber $\mathcal{M}_k \cdot \mathcal{M}_{t_j}^{\mathcal{O}}$ die j-te Spalte von $\mathcal{M}_k$, also $(0, \ldots, 0, 1, 0, \ldots, 0)^{tr}$, mit der 1 an der i-ten Stelle. Es ist also $\varphi(t_i) = t_i$ und φ damit surjektiv. Nun ist $\bar{O}$ eine Basis von $P/\ker(\varphi)$, und es bleibt $\ker(\varphi) = (g_1, \ldots, g_\nu)$ zu zeigen. Konstruiere mit 1.14 eine Randbasis $(\mathcal{G}', \mathcal{O}^+)$ von $\ker(\varphi)$ mit $\mathcal{G}' = (g_1', \ldots, g_\nu')$ und $g_j' = b_j - \sum_{k=1}^{\mu} a_{kj}' t_k \in \ker(\varphi)$. Ist nun $I \subseteq \ker(\varphi)$, so folgt $g_j = g_j'$ für $j = 1, \ldots, \nu$ und wir sind fertig. Zeige also, dass $g_j \in \ker(\varphi)$.

Für g_j existieren $l \in \{1, \ldots, n\}$ und $m \in \{1, \ldots, \mu\}$, so dass

$$\begin{aligned}
\varphi(g_j) = \varphi(b_j - \sum_{k=1}^{\mu} a_{kj} t_k) = \varphi(b_j) - (\sum_{k=1}^{\mu} a_{kj} \varphi(t_k) &= \varphi(x_l t_m) - \sum_{k=1}^{\mu} a_{kj} t_k \\
&= \mathcal{O} \cdot \mathcal{M}_l \cdot t_m(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot \mathcal{M}_{t_1}^{\mathcal{O}} - \sum_{k=1}^{\mu} a_{kj} t_k \\
&= \mathcal{O} \cdot \mathcal{M}_l \cdot \mathcal{M}_{t_m}^{\mathcal{O}} - \sum_{k=1}^{\mu} a_{kj} t_k = \mathcal{O} \cdot (a_{1j}, \ldots, a_{\mu,j})^{tr} - \sum_{k=1}^{\mu} a_{kj} t_k \\
&= \sum_{k=1}^{\mu} a_{kj} t_k - \sum_{k=1}^{\mu} a_{kj} t_k = 0.
\end{aligned}$$

Also ist $I = \ker(\varphi)$ und somit $\bar{O}$ Basis von P/I. □

Korollar 1.21 *Ist eine der äquivalenten Bedingungen aus dem obigen Theorem erfüllt, dann gilt*

a) *Das Ideal I ist null-dimensional und* $\dim(P/I) = \mu$.
b) *Die zu* $(\mathcal{G}, \mathcal{O}^+)$ *assoziierten Matrizen* $\mathcal{M}_1, \ldots, \mathcal{M}_n$ *sind die Multiplikationsmatrizen von* $\mathrm{NF}_{O,I}$.
c) *Die normale Restabbildung* $\mathrm{NR}_{O,G}$ *induziert eine Abbildung* $P \to V(O)$, *welche* $\mathrm{NF}_{O,I}$ *ist.*

Beweis. a) folgt direkt aus 1.20a) und der Beweis von b) ist im Beweis von "b) $\Rightarrow$ c)" enthalten. Genauso folgt c) aus dem Beweis von "c) $\Rightarrow$ a)". □

Beispiel 1.22 Wir wollen nun wieder wie in Beispiel 1.4 $\mathrm{NF}_{O,I}(x^6y^2)$ berechnen. Jedoch benutzen wir diesmal die in 1.16 berechnete Randbasis F. Es ist $x^6y^2 = x^3y^2 \cdot x^3$ und wir erhalten nach einem Reduktionsschritt mit dem durch x^3 markierten Polynom g_2 nun $x^4y^2 = xy^2 \cdot x^3$. Nochmalige Reduktion mit g_2 ergibt $x^2y^2 = xy \cdot xy$. Mit g_1 markiert durch xy erhalten wir weiter

$$xy(x + \tfrac{1}{2}y - x^2 + \tfrac{1}{2}y^2) = x^2y + \tfrac{1}{2}xy^2 - x^3y + \tfrac{1}{2}xy^3.$$

Mit g_2 und g_3 (markiert durch y^3) ergibt sich

$$x^2y + \frac{1}{2}xy^2 - xy + \frac{1}{2}xy = -\frac{1}{2}xy + x^2y + \frac{1}{2}xy^2$$

und mit g_1, g_4 und g_5 (markiert durch x^2y bzw. xy^2) letztlich

$$-\frac{1}{2}(-x^2 + \frac{1}{2}y^2 + x + \frac{1}{2}y) + \frac{1}{2}y^2 + \frac{1}{2}y + \frac{1}{2}(x^2 + \frac{1}{2}y^2 + x + \frac{1}{2}y) = \frac{1}{2}y + \frac{1}{2}y^2.$$

Also ist $\mathrm{NF}_{O,I}(x^6y^2) = \frac{1}{2}y + \frac{1}{2}y^2$, was dem Resultat Beispiel 1.5 entspricht. Dabei kommt es nicht auf die hier gewählten Reduktionen an, denn wegen 1.21c) erhalten wir stets dasselbe Ergebnis.

Anhang

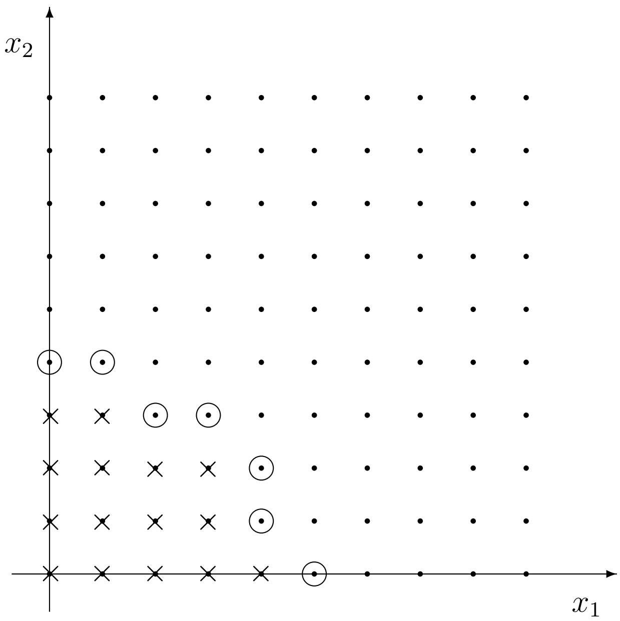

Abbildung: Der Rand O^+ eines Ordnungsideals O

$\times \;\widehat{=}\;$ Element im Ordnungsideal O
$\odot \;\widehat{=}\;$ Element im Rand O^+ von O