KAPITEL 10

Lineare Algebra über $k[x_1, \ldots, x_n]$

Wir beschreiben in diesem Kapitel, wie man Gleichungssysteme mit Koeffizienten in multivariaten Polynomringen über einem Körper lösen kann.

1. Grundaufgaben für Moduln

In diesem Kapitel ist k stets ein Körper, $n \in \mathbb{N}$, und $k[\boldsymbol{x}] := k[x_1, \ldots, x_n]$.

DEFINITION 10.1. Sei $m \in \mathbb{N}$, und sei Sei $\boldsymbol{v} = (v_1, \ldots, v_m) \in k[\boldsymbol{x}]^m$. Die *Polynomdarstellung* $\Phi(\boldsymbol{v})$ *(bzw.* $\Phi_{\boldsymbol{e}}(\boldsymbol{v})$*) von* $\boldsymbol{v}$ *bezüglich der neuen Variablen* $\boldsymbol{e} = (e_1, \ldots, e_m)$ ist das Element $\sum_{i=1}^m v_i e_i$ im Polynomring $k[x_1, \ldots, x_n, e_1, \ldots, e_m]$.

Sei $E := \{e_i \mid i \in \underline{m}\}$ und E^2 die Menge $\{e_i e_j \mid i, j \in \underline{m}\}$. Der Ring $k[\boldsymbol{x}, \boldsymbol{e}]/\left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$ heißt *Idealisierung* des $k[\boldsymbol{x}]$-Moduls $k[\boldsymbol{x}]^m$. Wir können nun jeden Untermodul in ein Ideal von $k[\boldsymbol{x}, \boldsymbol{e}]/\left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$ verwandeln.

LEMMA 10.2. *Sei* $m \in \mathbb{N}$. *Mit* $\overline{\mathcal{I}}(k[\boldsymbol{x}]^m)$ *bezeichnen wir den von*

$$e_1 + \left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}, \ldots, e_m + \left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$$

erzeugten Untermodul des $k[\boldsymbol{x}]$*-Moduls* $k[\boldsymbol{x}, \boldsymbol{e}]/\left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$.

(1) $\mathcal{I} : k[\boldsymbol{x}]^m \to \overline{\mathcal{I}}(k[\boldsymbol{x}]^m)$, $\mathcal{I}(\boldsymbol{v}) := \Phi_{\boldsymbol{e}}(\boldsymbol{v}) + \left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$ *ist ein* $k[\boldsymbol{x}]$*-Modulisomorphismus.*
(2) *Die* $k[\boldsymbol{x}]$*-Untermodule des Moduls* $\overline{\mathcal{I}}(k[\boldsymbol{x}]^m)$ *sind genau die Ideale* I *des Rings* $k[\boldsymbol{x}, \boldsymbol{e}]/\left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$ *mit* $I \subseteq \langle E\rangle_{k[\boldsymbol{x},\boldsymbol{e}]} / \left\langle E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$.

KOROLLAR 10.3. *Jeder Untermodul von* $k[\boldsymbol{x}]^m$ *ist endlich erzeugt.*

Seien $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(l)} \in k[\boldsymbol{x}]^m$. Mit $\left[\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(l)}\right]$ bezeichnen wir den von diesen Vektoren erzeugten $k[\boldsymbol{x}]$-Untermodul von $k[\boldsymbol{x}]^m$.

Satz 10.4. *Die Abbildung* $\hat{\mathcal{I}} : \{M \mid M$ *ist* $k[\boldsymbol{x}]$*-Untermodul von* $k[\boldsymbol{x}]^m\} \to \{I \mid I$ *ist Ideal von* $k[\boldsymbol{x}, \boldsymbol{e}]\}$,

$$\hat{\mathcal{I}}(\left[\boldsymbol{v}^{(1)}, \dots, \boldsymbol{v}^{(l)}\right]) := \left\langle\{\Phi(\boldsymbol{v}^{(1)}), \dots, \Phi(\boldsymbol{v}^{(l)})\} \cup E^2\right\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$$

ist eine Bijektion zwischen den Untermoduln von $k[\boldsymbol{x}]$ *und den Idealen von* $k[\boldsymbol{x}, \boldsymbol{e}]$ *mit* $E^2 \subseteq I \subseteq \langle E\rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$. *Weiters gilt* $M_1 \subseteq M_2$ *genau dann, wenn* $\hat{\mathcal{I}}(M_1) \subseteq \hat{\mathcal{I}}(M_2)$.

Satz 10.5. *Seien* $r, s \in \mathbb{N}$, *sei* M *ein Untermodul von* $k[\boldsymbol{x}]^{s+r}$. *Dann gilt*

$$M \cap (\{0\}^s \times k[\boldsymbol{x}]^r) = \hat{\mathcal{I}}^{-1}(\hat{\mathcal{I}}(M) \cap k[\boldsymbol{x}, e_{s+1}, \dots, e_{s+r}]).$$

Daraus sehen wir, dass wir aus Erzeugern für M mithilfe der Eliminationseigenschaft von Gröbnerbasen $M \cap (0^s \times k[\boldsymbol{x}]^r)$ berechnen können.

Satz 10.6. *Seien* $n, r, s \in \mathbb{N}$, *und seien* $\boldsymbol{a}_1, \dots, \boldsymbol{a}_r \in k[x_1, \dots, x_n]^s$. *Seien* $\boldsymbol{b}_1, \dots, \boldsymbol{b}_r \in k[\boldsymbol{x}]^s \times k[\boldsymbol{x}]^r$ *definiert durch* $\boldsymbol{b}_1 := (\boldsymbol{a}_1, (1, 0, \dots, 0)), \dots, \boldsymbol{b}_r := (\boldsymbol{a}_r, (0, 0, \dots, 1))$. *Sei* $\Pi_r : k[\boldsymbol{x}]^s \times k[\boldsymbol{x}]^r \to k[x_1, \dots, x_n]^r$, $\Pi_r(\boldsymbol{v}, \boldsymbol{w}) := \boldsymbol{w}$ *die Projektion auf die zweite Komponente, und sei*

$$S := \{(y_1, \dots, y_r) \in k[\boldsymbol{x}]^r \mid \sum_{i=1}^{r} y_i \boldsymbol{a}_i = 0\}$$

der Modul der Syzygien von $\boldsymbol{a}_1, \dots, \boldsymbol{a}_r$, *und sei* $M \subseteq k[x_1, \dots, x_n]^{s+r}$ *der von* $\boldsymbol{b}_1, \dots \boldsymbol{b}_r$ *erzeugte* $k[\boldsymbol{x}]$*-Modul. Dann gilt*

$$S = \Pi_r(M \cap (\{0\}^s \times k[\boldsymbol{x}]^r)).$$

Beweis: $\supseteq$: Die Menge $N := \{(\boldsymbol{v}, (y_1, \dots, y_r)) \in k[\boldsymbol{x}]^s \times k[\boldsymbol{x}]^r \mid \boldsymbol{v} = \sum_{i=1}^{r} y_i \boldsymbol{a_i}\}$ ist ein $k[\boldsymbol{x}]$-Untermodul von $k[\boldsymbol{x}]^s \times k[\boldsymbol{x}]^r$. Da alle Erzeuger von M in N liegen, gilt $M \subseteq N$. Sei nun $\boldsymbol{w} \in P_r(M \cap (\{0\}^s \times k[\boldsymbol{x}]^r))$. Dann gilt $(\boldsymbol{0}, \boldsymbol{w}) \in M$, also $(\boldsymbol{0}, \boldsymbol{w}) \in N$ und folglich $\boldsymbol{0} = \sum w_i \boldsymbol{a}_i$, und somit $\boldsymbol{w} \in S$.

$\subseteq$: Sei $\boldsymbol{y} \in S$. Dann gilt $\sum_{i=1}^{r} y_i \boldsymbol{a}_i = \boldsymbol{0}$, also $\sum_{i=1}^{r} y_i \boldsymbol{b}_i = (\boldsymbol{0}, \boldsymbol{y})$. Folglich gilt $(\boldsymbol{0}, \boldsymbol{y}) \in M$ und somit $\boldsymbol{y} \in P_r(M \cap (0^s \times k[\boldsymbol{x}]^r))$. □

2. Matrizennormalformen

Definition 10.7. Sei k ein Körper, seien $n, r, s \in \mathbb{N}$, seien $\boldsymbol{e} = (e_1, \dots, e_s)$ neue Variablen, sei $\boldsymbol{x} = (x_1, \dots, x_n)$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Die

Monomordnung $\leq'$ auf $k[\boldsymbol{x}, \boldsymbol{e}]$ ist durch durch

$$\boldsymbol{e}^{\alpha}\boldsymbol{x}^{\beta} \geq' \boldsymbol{e}^{\alpha'}\boldsymbol{x}^{\beta'} \Leftrightarrow \alpha >_{\text{lex}} \alpha' \text{ oder } (\alpha = \alpha' \text{ und } \beta \geq \beta') \tag{2.1}$$

definiert. Eine Matrix $A \in k[\boldsymbol{x}]^{r\times s}$ mit Zeilenvektoren $a_1, \ldots, a_r \in k[\boldsymbol{x}]^s \setminus \{0\}$ ist in *Treppennormalform bezüglich* $\leq$, wenn für $G := \{\Phi_{\boldsymbol{e}}(a_1), \ldots, \Phi_{\boldsymbol{e}}(a_r)\}$ gilt:

(1) $G \cup E^2$ ist eine Gröbnerbasis bezüglich $\leq'$.
(2) Alle Elemente von G sind reduziert in $G \cup E^2$.
(3) $\textsc{Deg}_{\leq'}(\Phi_{\boldsymbol{e}}(a_1)) >' \cdots >' \textsc{Deg}_{\leq'}(\Phi_{\boldsymbol{e}}(a_r))$.

Sei R ein kommutativer Ring mit Eins. Mit $R^{m\times n}$ bezeichnen wir die Menge aller $m \times n$-Matrizen mit Einträgen aus R. Für $A \in R^{m\times n}$ ist $\text{col}(A) = \{Ax \mid x \in R^n\}$ der *Spaltenmodul* von A, $\text{row}(A) = \{yA \mid y \in R^m\}$ der *Zeilenmodul* von A. Die Menge $\ker(A) = \{y \in \mathbb{R}^n \mid Ay = 0\}$ ist der *Kern* oder *Nullmodul* von A.

Satz 10.8. *Sei k ein Körper, sei $A \in k[\boldsymbol{x}]^{r\times s}$, und sei $\leq$ eine zulässige Monomordnung für $k[\boldsymbol{x}]$. Dann gibt es genau eine Matrix H mit s Spalten, sodass* $\text{row}(A) = \text{row}(H)$ *und H in Treppennormalform bezüglich $\leq$ ist.*

Beweisskizze: Sei $\boldsymbol{e} := (e_1, \ldots, e_s)$ ein Tupel neuer Variablen, sei $E = \{e_1, \ldots, e_s\}$, seien $a_1, \ldots, a_r$ die Zeilenvektoren von A, sei G eine reduzierte Gröbnerbasis von $\{\Phi_{\boldsymbol{e}}(a_1), \ldots, \Phi_{\boldsymbol{e}}(a_r)\} \cup E^2$ bezüglich der in (2.1) definierten Monomordnung $\leq'$, und seien $g_1, \ldots, g_t$ die Elemente von $G \setminus E^2$ mit $\textsc{Deg}_{\leq'}(g_1) >' \cdots >' \textsc{Deg}_{\leq'}(g_t)$. Für $i \in \underline{t}$ sei $h_i \in k[\boldsymbol{x}]^s$ so, dass $\Phi_{\boldsymbol{e}}(h_i) = g_i$. Dann leistet die Matrix H, deren Zeilenvektoren $h_1, \ldots, h_t$ sind, das Gewünschte.

Die Eindeutigkeit folgt aus der Eindeutigkeit der reduzierten Gröbnerbasis. □

Lemma 10.9. *Sei $\leq$ eine zulässige Monomordnung in $k[\boldsymbol{x}]$, und sei $A = (a_{ij})_{(i,j)\in\underline{r}\times\underline{s}} \in k[\boldsymbol{x}]^{r\times s}$ in Treppennormalform bezüglich $\leq$. Für $i \in \underline{s}$ ist die i* te Stufe von A *die Menge*

$$S_i = \{a_{t,i} \mid t \in \underline{r}, a_{t,i} \neq 0, \text{ und } a_{t,1} = \cdots = a_{t,i-1} = 0\}.$$

Das i te Gabelideal *von* $\text{row}(A)$ *ist die Menge*

$$F_i = \{p \in k[\boldsymbol{x}] \mid \exists p_{i+1}, \ldots, p_s \in k[\boldsymbol{x}] : (\underbrace{0, \ldots, 0}_{i-1}, p, p_{i+1}, \ldots, p_s) \in \text{row}(A)\}.$$

Dann ist S_i eine reduzierte Gröbnerbasis des Ideals F_i bezüglich $\leq$.

Beweis: Sei $p \in F_i$ mit $p \neq 0$ und sei $\boldsymbol{v} = (\underbrace{0, \ldots, 0}_{i-1}, p, p_{i+1}, \ldots, p_s) \in \text{row}(A)$. Dann gilt $\Phi_{\boldsymbol{e}}(\boldsymbol{v}) \in \hat{\mathcal{I}}(\text{row}(A))$, also $pe_i + \sum_{j=i+1}^{s} p_j e_j \in \hat{\mathcal{I}}(\text{row}(A))$. Seien $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ die Zeilenvektoren von A. Da $\{\Phi_{\boldsymbol{e}}(\boldsymbol{a}_1), \ldots, \Phi_{\boldsymbol{e}}(\boldsymbol{a}_r)\} \cup E^2$ eine Gröbnerbasis von $\hat{\mathcal{I}}(\text{row}(A))$ ist, gibt es ein $t \in \underline{r}$, sodass $\text{LT}(\Phi_{\boldsymbol{e}}(\boldsymbol{a}_t)) \mid \text{LT}(pe_i + \sum_{j=i+1}^{s} p_j e_j)$, also $\text{LT}(\Phi_{\boldsymbol{e}}(\boldsymbol{a}_t)) \mid \text{LT}(p)e_i$. Dann gilt $e_i \mid \text{LT}(\Phi_{\boldsymbol{e}}(\boldsymbol{a}_t))$. Also gilt $\boldsymbol{a}_t \in S_i$. Der Vektor $\boldsymbol{a}_t$ ist daher von der Form $(0, \ldots, 0, a_{t,i}, a_{t,i+1}, \ldots, a_{t,s})$ mit $a_{t,i} \neq 0$. Somit gilt $\text{LT}(\Phi_{\boldsymbol{e}}(\boldsymbol{a}_t)) = a_{t,i}e_i$. Es gilt also $\text{LT}(\Phi_{\boldsymbol{e}}(\boldsymbol{a}_t))e_i \mid \text{LT}(p)e_i$ und somit $\text{LT}(a_{t,i}) \mid \text{LT}(p)$. Somit bildet S_i eine Gröbnerbasis von F_i. $\square$

SATZ 10.10. *Sei k ein Körper, sei $A \in k[\boldsymbol{x}]^{r \times s}$, und sei $\leq$ eine zulässige Monomordnung für $k[\boldsymbol{x}]$. Sei H die Treppennormalform von $(A|I_r)$ bezüglich $\leq$. Wir schreiben H in der Form*

$$H = \left(\begin{smallmatrix} B & C \\ 0 & D \end{smallmatrix} \right),$$

wobei B genau s Spalten und C genau r Spalten hat, und die letzte Zeile von B nicht der Nullvektor ist. Dann sind B und D in Treppennormalform, $\text{row}(B) = \text{row}(A)$, $\text{row}(D) = \ker(A^T)$ *und $B = CA$.*

Beweis: Seien $\boldsymbol{e} := (e_1, \ldots, e_s)$ und $\boldsymbol{f} = (f_1, \ldots, f_r)$ Tupel neuer Variablen. Wir bezeichnen die Zeilenvektoren von B mit $b_1, \ldots, b_m$, die Zeilenvektoren von C mit $c_1, \ldots, c_m$, und die Zeilenvektoren von D mit $d_1, \ldots, d_l$. Wir zeigen nun, dass B in Treppennormalform ist. Sei $G_1 := \{\Phi_{\boldsymbol{e}}(b_1), \ldots, \Phi_{\boldsymbol{e}}(b_m)\}$. Um zu zeigen, dass $G_1 \cup E^2$ eine Gröbnerbasis ist, wählen wir $p \in \langle G_1 \cup E^2 \rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$ mit $p \neq 0$ und zeigen, dass $\text{LT}(p)$ durch einen führenden Term von $G_1 \cup E^2$ teilbar ist. Da $p \in \langle G_1 \cup E^2 \rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$, gibt es $h_1(\boldsymbol{x}), \ldots, h_m(\boldsymbol{x}) \in k[\boldsymbol{x}]$ und $r \in \langle E^2 \rangle_{k[\boldsymbol{x},\boldsymbol{e}]}$, sodass

$$p(\boldsymbol{x}, \boldsymbol{e}) = (\sum_{i=1}^{m} h_i(\boldsymbol{x}) \Phi_{\boldsymbol{e}}(b_i)) + r(\boldsymbol{x}, \boldsymbol{e}).$$

Sei

$$q(\boldsymbol{x}, \boldsymbol{e}, \boldsymbol{f}) := (\sum_{i=1}^{m} h_i(\boldsymbol{x}) \Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i)) + r(\boldsymbol{x}, \boldsymbol{e}).$$

Wir betrachten nun $\text{LT}(q)$. Wenn in $\text{LT}(q)$ eine Variable f_j aus $\boldsymbol{f}$ vorkommt, so kann diese Variable nur in einem Summanden $h_i(\boldsymbol{x})\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i))$ vorkommen. Da f_j dann nur mit Exponent 1 auftritt, kann wegen der Ordnung der Variablen in q keine der Variablen aus $\boldsymbol{e}$ vorkommen. Damit kommt auch in $p(\boldsymbol{x}, \boldsymbol{e}) = q(\boldsymbol{x}, \boldsymbol{e}, 0)$ keine der Variablen aus $\boldsymbol{e}$ vor. Dann gilt aber $p = 0$. In $\text{LT}(q)$ kommt also kein f_j

vor. Wegen $p(\boldsymbol{x}, \boldsymbol{e}) = q(\boldsymbol{x}, \boldsymbol{e}, 0)$ kommt der Term $\mathrm{LT}(q)$ dann auch in p vor. Da $\mathrm{Supp}(p) \subseteq \mathrm{Supp}(q)$ gilt dann $\mathrm{LT}(p) = \mathrm{LT}(q)$.

Wenn nun $\mathrm{LT}(q) \notin \langle E^2 \rangle_{k[\boldsymbol{x},\boldsymbol{e},\boldsymbol{f}]}$, so verwenden wir, dass H in Treppennormalform ist, und somit

$$G = \{\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i) \mid i \in \underline{m}\} \cup \{\Phi_{\boldsymbol{f}}(d_j) \mid j \in \underline{l}\} \cup (E \cup F)^2$$

eine Gröbnerbasis ist. Es gibt dann also ein $i \in \underline{m}$, $\mathrm{LT}(\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i)) \mid \mathrm{LT}(q)$. Da $b_i \neq 0$, gilt $\mathrm{LT}(\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i)) = \mathrm{LT}(\Phi_{\boldsymbol{e}}(b_i))$. Somit gilt $\mathrm{LT}(\Phi_{\boldsymbol{e}}(b_i)) \mid \mathrm{LT}(p)$. Folglich ist $G_1 \cup E^2$ eine Gröbnerbasis.

Wegen $b_i \neq 0$ gilt $\mathrm{DEG}(\Phi_{\boldsymbol{e}}(b_i) = \mathrm{DEG}(\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i))$, und somit gilt $\mathrm{DEG}(\Phi_{\boldsymbol{e}}(b_1) >' \cdots >' \mathrm{DEG}(\Phi_{\boldsymbol{e}}(b_m))$.

Wir zeigen nun, dass G_1 in $G_1 \cup E^2$ reduziert ist. Nehmen wir an, $\mathrm{LT}(\Phi_{\boldsymbol{e}}(b_i))$ teilt ein Monom in $\Phi_{\boldsymbol{e}}(b_j)$. Wegen $\mathrm{LT}(\Phi_{\boldsymbol{e}}(b_i)) = \mathrm{LT}(\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i))$, teilt $\mathrm{LT}(\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_i, c_i))$ daher ein Monom aus $\Phi_{\boldsymbol{e}}(b_j)$. Alle Monome aus $\Phi_{\boldsymbol{e}}(b_j)$ kommen auch in $\Phi_{\boldsymbol{e},\boldsymbol{f}}(b_j, c_j)$ vor. Das steht aber dann im Widerspruch dazu, dass G in $G \cup (E \cup F)^2$ reduziert ist.

Wir zeigen als nächstes, dass auch D in Treppennormalform ist. Da $\{\Phi_{\boldsymbol{f}} d_1, \ldots, \Phi_{\boldsymbol{f}}(d_l)\} \cup F^2 = G \cap k[\boldsymbol{x}, \boldsymbol{f}]$ und $\boldsymbol{e} >> \boldsymbol{f} >> \boldsymbol{x}$, folgt das aus der Eliminationseigenschaft von Gröbnerbasen.

Da $\mathrm{row}(H) = \mathrm{row}(A|I_r)$, gibt es $S \in k[\boldsymbol{x}]^{r \times h}$ und $T \in k[\boldsymbol{x}]^{h \times r}$ mit $H = S(A|I_r)$ und $(A|I_r) = TH$. Daraus sieht man leicht, $\mathrm{row}(B) = \mathrm{row}(A)$.

Wir zeigen nun $\ker(A^T) = \mathrm{row}(D)$. "$\subseteq$": Sei $y \in k[\boldsymbol{x}]^r$ so dass, $A^T y = 0$, also $yA = 0$. Dann gilt $y(A|I_r) = (0, y)$. Somit gilt $\Phi_{\boldsymbol{e},\boldsymbol{f}}(0, y) \in \hat{\mathcal{I}}(\mathrm{row}(A|I_r)) \cap k[\boldsymbol{x}, \boldsymbol{f}]$. Wegen der Elimationseigenschaft von Gröbnerbasen gilt daher $\Phi_{\boldsymbol{e},\boldsymbol{f}}(0, y) \in \hat{\mathcal{I}}(\mathrm{row}(D))$, und somit $(0, y) \in \mathrm{row}(D)$. "$\supseteq$": Jedes $(x, y) \in \mathrm{row}(A|I_r)$ ist von der Form (zA, z) und erfüllt damit $x = yA$. Wenn nun $y \in \mathrm{row}(D)$, so gilt $(0, y) \in \mathrm{row}(0|D)$, und somit $(0, y) \in \mathrm{row}(A|I_r)$. Also gilt $0 = yA$, und somit $y \in \ker(A^T)$.

Für die Gleichung $B = CA$ beobachten wir, dass jeder Vektor $(x, y) \in \mathrm{row}(A|I_r)$ die Gleichheit $x = yA$ erfüllt. Daraus erhalten wir $B = CA$ (und auch $0 = DA$). $\square$

SATZ 10.11. *Sei $A \in k[\boldsymbol{x}]^{r \times s}$ und $b \in k[\boldsymbol{x}]^{r \times 1}$. Sei H die Treppennormalform von*

$$\left(\begin{array}{c|c} b^T & \\ A^T & I_{s+1} \end{array} \right).$$

Wir schreiben H in der Form

$$H = \begin{pmatrix} B & * & * \\ 0 & v & S \\ 0 & 0 & D \end{pmatrix},$$

wobei B genau r Spalten, v genau 1 Spalte, und D genau S Spalten hat, in der letzten Zeile von B nicht der Nullvektor steht, und der letzte Eintrag von v nicht 0 ist. Dann gilt:

(1) *Die Einträge von v sind die reduzierte Gröbnerbasis des Ideals*

$$(\mathrm{col}(A) : b) := \{p \in k[\boldsymbol{x}] \mid p\, b \in \mathrm{col}(A)\}$$

von $k[\boldsymbol{x}]$.

(2) *Das Gleichungssystem $Ax = b$ ist genau dann lösbar in $k[\boldsymbol{x}]^s$, wenn $v = (1)$. Dann hat S genau eine Zeile, und $-S$ ist eine Lösung von $Ax = b$.*

(3) *D ist in Treppennormalform,* und $\mathrm{row}(D) = \ker(A)$.

Beweisskizze: Wir setzen $A' := \left(\begin{smallmatrix} b^T \\ A^T \end{smallmatrix}\right)$, $r' := s + 1$, $s' := r$. Dann hat die Treppennormalform von $(A'|I_{r'})$ nach Satz 10.10 die Form $\left(\begin{smallmatrix} B' & C' \\ 0 & D' \end{smallmatrix}\right)$ mit $B' \in k[\boldsymbol{x}]^{m \times r}$ und $D' \in k[\boldsymbol{x}]^{l \times (s+1)}$. Wir schreiben $D' = \left(\begin{smallmatrix} v & S \\ 0 & D \end{smallmatrix}\right)$. Nach Satz 10.10 gilt $\mathrm{row}(D') = \ker((A')^T)$, also

$$\mathrm{row}(\left(\begin{smallmatrix} v & S \\ 0 & D \end{smallmatrix}\right)) = \ker(b|A) = \{(x, \boldsymbol{y}) \in k[\boldsymbol{x}]^{1+s} \mid bx + A\boldsymbol{y} = 0\}.$$

Außerdem ist $\left(\begin{smallmatrix} v & S \\ 0 & D \end{smallmatrix}\right)$ in Treppennormalform. Somit steht in den Zeilen von v eine reduzierte Gröbnerbasis des ersten Gabelideals F_1 von $\ker(b|A)$. Es gilt $F_1 = \{u \in k[\boldsymbol{x}] \mid \exists \boldsymbol{y} \in k[\boldsymbol{x}]^s : ub + A\boldsymbol{y} = 0\} = \{u \in k[\boldsymbol{x}] \mid ub \in \mathrm{col}(A)\} = (\mathrm{col}(A) : b)$.

Das Gleichungssystem $Ax = b$ ist genau dann lösbar wenn $1 \in (\mathrm{col}(A) : b)$. Dann ist die reduzierte Gröbnerbasis von $F_1 = \{1\}$ und somit $v = (1)$. In diesem Fall gilt $S \in k[\boldsymbol{x}]^{1 \times s}$, und wegen $(1|S) \in \mathrm{row}(\left(\begin{smallmatrix} v & S \\ 0 & D \end{smallmatrix}\right)) = \ker(b|A)$ auch $b + AS^T = 0$. Also ist $-S$ eine Lösung von $Ax = B$.

Da D' in Treppennormalform ist, gilt $\mathrm{row}(D) = \{\boldsymbol{y} \in k[\boldsymbol{x}]^s \mid (0, \boldsymbol{y}) \in \mathrm{row}(D')\} = \{\boldsymbol{y} \in k[\boldsymbol{x}]^s \mid A\boldsymbol{y} = 0\} = \ker(A)$. □

Übungsaufgaben 10.12