KAPITEL 6

Gröbnerbasen

1. Grundlagen aus der Mengenlehre und der Ordnungstheorie

Sei X eine Menge, und sei p eine natürliche Zahl. Dann bezeichnen wir mit $\binom{X}{p}$ die Menge aller p-elementigen Teilmengen von X, also

$$\binom{X}{p} = \{Y \mid Y \subseteq X \text{ und } |Y| = p\}.$$

SATZ 6.1 (Satz von Ramsey, [**Ram29**]). *Sei X eine unendliche Menge, und seien $p, t \in \mathbb{N}$. Sei $F : \binom{X}{p} \to \{1, \ldots, t\}$. Dann gibt es eine unendliche Teilmenge Y von X, sodass F auf $\binom{Y}{p}$ konstant ist.*

Beweis: Induktion nach p. Für $p = 1$ sehen wir, dass $X = \bigcup_{i=1}^{t} \{x \in X \mid F(\{x\}) = i\}$. Da X also Vereinigung von t Mengen ist, muss eine dieser Mengen unendlich sein. Diese unendliche Menge ist das gesuchte Y.

Induktionsschritt: Sei $p \geq 2$, und sei F eine Färbung der p-elementigen Teilmengen von $\mathbb{N}$ mit t Farben. Für jedes $a \in \mathbb{N}$ definieren wir eine Färbung G_a der $(p-1)$-elementigen Teilmengen von $X \setminus \{a\}$ durch

$$G_a(M) := F(M \cup \{a\})$$

für alle $M \in \binom{X \setminus \{a\}}{p}$. Nun definieren wir eine Folge $(x_i)_{i \in \mathbb{N}_0}$ aus X, und eine Folge $(Y_i)_{i \in \mathbb{N}_0}$ von Teilmengen von X. Wir definieren $Y_0 := X$, und wählen x_0 als ein Element von X. Wir werden nun die Folgen $(x_i)_{i \in \mathbb{N}_0}$ und $(Y_i)_{i \in \mathbb{N}_0}$ so definieren, dass jedes Y_i eine unendliche Teilmenge von X ist, und dass $x_i \in Y_i$. Wir definieren die Folgen rekursiv. Sei dazu $i \in \mathbb{N}_0$. Da $Y_i \setminus \{x_i\}$ unendlich ist, gibt es nach Induktionsvoraussetzung eine unendliche Teilmenge Y_{i+1} von $Y_i \setminus \{x_i\}$, sodass alle $(p-1)$-elementigen Teilmengen von Y_{i+1} die gleiche Farbe unter der Färbung G_{x_i} haben. Das Element x_{i+1} wählen wir aus Y_{i+1}.

Wir betrachten nun die Menge

$$Z := \{x_i \mid i \in \mathbb{N}_0\}.$$

Für jede p-elementige Teilmenge A von Z definieren wir den *kleinsten Index in* A, $\mathrm{ind}(A)$, als das kleinste $j \in \mathbb{N}_0$, sodass $x_j \in A$. Wir zeigen nun:

$$\text{Für alle } A, B \in \binom{Z}{p} \text{ mit } \mathrm{ind}(A) = \mathrm{ind}(B) \text{ gilt } F(A) = F(B).$$

Sei dazu $i := \mathrm{ind}(A)$. Alle x_j mit $j > i$ liegen in Y_{i+1}. Folglich ist A eine Teilmenge von $Y_{j+1} \cup \{x_i\}$. Ebenso ist B eine Teilmenge von $Y_{j+1} \cup \{x_i\}$. Wegen der Konstruktion von Y_{j+1} ist $G_{x_i}(A \setminus \{x_i\}) = G_{x_i}(B \setminus \{x_i\})$. Also gilt $F(A) = F(B)$.

Nun betrachten wir die Abbildung $h : \mathbb{N}_0 \to \{1, \ldots, t\}$, die durch

$$h(i) := F(\{x_i, \ldots, x_{i+p-1}\})$$

für $i \in \mathbb{N}_0$ definiert ist. Es gibt eine unendliche Teilmenge J von $\mathbb{N}_0$, sodass $h|_J$ konstant ist. Wir behaupten nun, dass

$$Y := \{x_j \mid j \in J\}$$

die gewünschten Eigenschaften erfüllt.

Seien dazu C und D p-elementige Teilmengen von Y, und seien $c_1 < \cdots < c_p$ und $d_1 < \cdots < d_p$ so, dass $C = \{x_{c_1}, x_{c_2}, \ldots, x_{c_p}\}$ und $D = \{x_{d_1}, x_{d_2}, \ldots, x_{d_p}\}$. Da $\mathrm{ind}(C) = c_1 = \mathrm{ind}(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$, gilt

$$F(C) = F(\{x_{c_1}, x_{c_1+1}, \ldots, x_{c_1+p-1}\})$$

und ebenso

$$F(D) = F(\{x_{d_1}, x_{d_1+1}, \ldots, x_{d_1+p-1}\}).$$

Also gilt $F(C) = h(c_1)$ und $F(D) = h(d_1)$. Da x_{c_1} in Y liegt, gilt $c_1 \in J$; ebenso gilt $d_1 \in J$, und folglich $h(c_1) = h(d_1)$. Also haben C und D die gleiche Farbe. □

Eine geordnete Menge $(M, \leq)$ erfüllt die (DCC) (absteigende Kettenbedingung, *descending chain condition*), wenn es keine unendliche echt absteigende Folge $m_1 > m_2 > m_3 > \cdots$ von Elementen aus M gibt. Zwei Elemente $s, t \in M$ sind *unvergleichbar*, wenn weder $s \leq t$ noch $t \leq s$ gilt. Wir schreiben dafür $s \parallel t$. Eine Teilmenge T von M ist eine *Antikette*, wenn alle $t_1, t_2 \in T$ mit $t_1 \neq t_2$ unvergleichbar sind.

Sei $m \in \mathbb{N}$. Auf ${\mathbb{N}_0}^m$ definieren wir die Ordnungsrelation $\sqsubseteq$. Seien $\boldsymbol{a} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ und $\boldsymbol{b} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$. Dann gilt $\boldsymbol{a} \sqsubseteq \boldsymbol{b}$, wenn für alle $i \in \{1, \ldots, m\}$ gilt: $\boldsymbol{a}_i \leq \boldsymbol{b}_i$. Wir betrachten nun die geordnete Menge $({\mathbb{N}_0}^m, \sqsubseteq)$.

LEMMA 6.2. *Sei $m \in \mathbb{N}$ und sei $S = \langle \boldsymbol{a}^{(i)} \mid i \in \mathbb{N} \rangle$ eine Folge von Elementen aus ${\mathbb{N}_0}^m$. Dann gibt es eine unendliche Folge $t_1 < t_2 < \cdots$ von natürlichen Zahlen, sodass $\langle \boldsymbol{a}^{(t_i)} \mid i \in \mathbb{N} \rangle$ eine bezüglich $\sqsubseteq$ schwach monoton wachsende unendliche Teilfolge von S ist.*

Beweis: Für $i \in \mathbb{N}$ und $k \in \{1, \ldots, m\}$ bezeichnen wir die k-te Komponente von $\boldsymbol{a}^{(i)}$ mit $\boldsymbol{a}_k^{(i)}$.

Wir färben nun jede 2-elementige Teilmenge $\{i, j\}$ von $\mathbb{N}$ mit $i < j$ mit einer von 2^m Farben. As Farben wählen wir die Funktionen von $\{1, \ldots, m\}$ nach $\{\mathbf{1}, \mathbf{2}\}$. Wir definieren nun die Farbe $C(\{i, j\})$ der Menge $\{i, j\}$ durch

$$C(\{i,j\})\,(k) := \begin{cases} \mathbf{1} & \text{wenn } \boldsymbol{a}_k^{(i)} \leq \boldsymbol{a}_k^{(j)}, \\ \mathbf{2} & \text{wenn } \boldsymbol{a}_k^{(i)} > \boldsymbol{a}_k^{(j)}. \end{cases}$$

Nach dem Satz von Ramsey, Satz 6.1, hat $\mathbb{N}$ eine unendliche Teilmenge T, sodass alle 2-elementigen Teilmengen von T die gleiche Farbe C haben.

Wir zeigen nun, dass $C(k) = \mathbf{1}$ für alle $k \in \{1, \ldots, m\}$ gilt. Nehmen wir an, es gibt ein k mit $C(k) = \mathbf{2}$. Seien $t_1 < t_2 < t_3 < \ldots$ die Elemente von T. Wenn $C(k) = \mathbf{2}$, dann gilt

$$\boldsymbol{a}_k^{(t_1)} > \boldsymbol{a}_k^{(t_2)} > \boldsymbol{a}_k^{(t_3)} > \cdots,$$

im Widerspruch dazu, dass $(\mathbb{N}, \leq)$ die (DCC) erfüllt.

Da also $C(k) = \mathbf{1}$ für alle k, gilt $\boldsymbol{a}^{(t_1)} \sqsubseteq \boldsymbol{a}^{(t_2)} \sqsubseteq \boldsymbol{a}^{(t_3)} \sqsubseteq \cdots$. □

SATZ 6.3 (Dicksons Lemma, cf. [**Dic13**, Lemma A]). *Sei $m \in \mathbb{N}$. Dann sind alle Antiketten in $({\mathbb{N}_0}^m, \sqsubseteq)$ endlich.*

Beweis: Nach Lemma 6.2 kann $({\mathbb{N}_0}^m, \sqsubseteq)$ keine unendliche Antikette enthalten. □

DEFINITION 6.4. Eine Teilmenge I von ${\mathbb{N}_0}^m$ ist ein *Ordnungsfilter*, wenn für alle $\boldsymbol{a} \in I$ und $\boldsymbol{b} \in {\mathbb{N}_0}^m$ mit $\boldsymbol{a} \sqsubseteq \boldsymbol{b}$ auch $\boldsymbol{b} \in I$ gilt.

Für eine Teilmenge I von ${\mathbb{N}_0}^m$ bezeichnen wir mit $\mathcal{M}(I)$ die Menge aller minimalen Elemente von I. Für eine Teilmenge M von $\mathbb{N}_0^m$ definieren wir $\mathcal{U}(M)$ durch $\mathcal{U}(M) := \{\boldsymbol{a} \in \mathbb{N}_0^m \mid \text{ es gibt } \boldsymbol{z} \in M, \text{ sodass } \boldsymbol{z} \leq \boldsymbol{a}\}$. $\mathcal{U}(M)$ ist stets ein Ordnungsfilter.

LEMMA 6.5. *Sei $I \subseteq {\mathbb{N}_0}^m$ ein Ordnungsfilter bezüglich $\sqsubseteq$. Dann ist $\mathcal{M}(I)$ endlich, und es gilt $I = \mathcal{U}(\mathcal{M}(I))$.*

Beweis: $\mathcal{M}(I)$ ist eine Antikette, und daher wegen des Dicksonschen Lemmas (Satz 6.3) endlich. Sei nun $\boldsymbol{i} \in I$. Da $(\mathbb{N}_0^m, \sqsubseteq)$ keine unendlich absteigenden Ketten hat, gibt es ein minimales Element $\boldsymbol{z} \in I$ mit $\boldsymbol{z} \leq \boldsymbol{i}$. Daher gilt $\boldsymbol{i} \in \mathcal{U}(\mathcal{M}(I))$. Da $\mathcal{M}(I) \subseteq I$, erhalten wir die Inklusion $\mathcal{U}(\mathcal{M}(I)) \subseteq I$ unmittelbar aus der Tatsache, dass I ein Ordnungsfilter ist. □

SATZ 6.6. *Let $m \in \mathbb{N}$. Dann hat die Menge $\mathbb{N}_0^m$ keine unendliche aufsteigende Kette $U_1 \subset U_2 \subset U_3 \ldots$ von Ordnungsfiltern.*

Sei $U := \bigcup\{U_i \mid i \in \mathbb{N}\}$. Die Menge U ist ein Ordnungsfilter. Daher ist die Menge $\mathcal{M}(U)$ der bezüglich $\sqsubseteq$ minimalen Elemente von U endlich. Es gibt also ein $j \in \mathbb{N}$, sodass $\mathcal{M}(U) \subseteq U_j$. Daher gilt $\mathcal{U}(\mathcal{M}(U)) \subseteq \mathcal{U}(U_j)$, und folglich $U \subseteq U_j$. □

2. Multivariate Polynomdivision

DEFINITION 6.7. Sei $n \in \mathbb{N}$, und sei $\leq$ eine Ordnung auf ${\mathbb{N}_0}^n$. Die Ordnung $\leq$ ist *zulässig*, wenn folgendes gilt:

(1) $\leq$ ist linear.
(2) Für alle $\alpha, \beta \in {\mathbb{N}_0}^n$ mit $\alpha \sqsubseteq \beta$ gilt auch $\alpha \leq \beta$.
(3) Für alle $\alpha, \beta, \gamma \in {\mathbb{N}_0}^n$ mit $\alpha \leq \beta$ gilt auch $\alpha + \gamma \leq \beta + \gamma$.

LEMMA 6.8. *Sei $n \in \mathbb{N}$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Dann erfüllt $({\mathbb{N}_0}^n, \leq)$ die* (DCC).

Sei $\boldsymbol{a}^{(1)} > \boldsymbol{a}^{(2)} > \cdots$ eine bezüglich $\leq$ unendliche absteigende Kette in ${\mathbb{N}_0}^n$. Nach Lemma 6.2 gibt es $t_1, t_2 \in \mathbb{N}$ mit $t_1 < t_2$, sodass $\boldsymbol{a}^{(t_1)} \sqsubseteq \boldsymbol{a}^{(t_2)}$. Da $\leq$ zulässig ist, gilt $\boldsymbol{a}^{(t_1)} \leq \boldsymbol{a}^{(t_2)}$, im Widerspruch zu $\boldsymbol{a}^{(t_1)} > \boldsymbol{a}^{(t_2)}$. □

DEFINITION 6.9. Sei k ein kommutativer Ring mit Eins, und sei R der Polynomring $k[x_1, \ldots, x_n]$. Für $\alpha = (\alpha_1, \ldots, \alpha_n) \in {\mathbb{N}_0}^n$ definieren wir $\boldsymbol{x}^\alpha$ durch

$$\boldsymbol{x}^\alpha := {x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n}.$$

DEFINITION 6.10. Sei $n \in \mathbb{N}$, sei k ein kommutativer Ring mit Eins, sei I eine endliche Teilmenge von ${\mathbb{N}_0}^n$, sei $c : I \to k$, sei

$$f = \sum_{\alpha \in I} c_\alpha \boldsymbol{x}^\alpha$$

ein Element von $k[x_1, \ldots, x_n]$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Dann definieren wir den *Multigrad* von f bezüglich $\leq$ durch

$$\textsc{Deg}(f) := (-1, \ldots, -1), \text{ wenn } f = 0,$$

und

$$\textsc{Deg}(f) := \max_{\leq}\{\alpha \in {\mathbb{N}_0}^n \mid c_\alpha \neq 0\}, \text{ wenn } f \neq 0.$$

Definition 6.11. Sei $n \in \mathbb{N}$, sei k ein kommutativer Ring mit Eins, und sei

$$f = \sum_{\alpha \in {\mathbb{N}_0}^n} c_\alpha \boldsymbol{x}^\alpha$$

ein Element von $k[x_1, \ldots, x_n]$ mit $f \neq 0$, und sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$. Sei γ der Multigrad von f. Dann definieren wir

$$\begin{aligned} \textsc{Lm}(f) &:= \boldsymbol{x}^\gamma, \\ \textsc{Lc}(f) &:= c_\gamma, \\ \textsc{Lt}(f) &:= c_\gamma \boldsymbol{x}^\gamma. \end{aligned}$$

Definition 6.12. Sei $n \in \mathbb{N}$, sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$, sei $s \in \mathbb{N}$, und seien $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Eine Folge $(a_1, \ldots, a_s, r) \in k[x_1, \ldots, x_n]^{s+1}$ ist eine *Standarddarstellung* von f durch $(f_1, \ldots, f_s)$ bezüglich $\leq$, wenn folgendes gilt:

(1) $f = \sum_{i=1}^{s} a_i f_i + r$.
(2) $r = 0$, oder es gibt eine endliche Teilmenge I von ${\mathbb{N}_0}^n$, sodass

$$r = \sum_{\alpha \in I} c_\alpha \boldsymbol{x}^\alpha$$

gilt, und dass für alle $\alpha \in I$ und alle $i \in \{1, \ldots, s\}$ mit $f_i \neq 0$ das Monom $\boldsymbol{x}^\alpha$ kein Vielfaches von $\textsc{Lm}(f_i)$ ist.
(3) Für alle $i \in \{1, \ldots, s\}$ gilt $\textsc{Deg}(a_i f_i) \leq \textsc{Deg}(f)$.

Das Polynom r heißt auch *Rest* der Darstellung.

Satz 6.13. *Sei $n \in \mathbb{N}$, sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$, sei $s \in \mathbb{N}$, und seien $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Dann gibt es eine Standarddarstellung $(a_1, \ldots, a_s, r)$ von f durch $(f_1, \ldots, f_s)$.*

Beweis: Seien $s \in \mathbb{N}$ und $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Wir zeigen nun, dass jedes Polynom f eine Standarddarstellung durch $(f_1, \ldots, f_s)$ besitzt. Als zulässige Ordnung erfüllt $\leq$ die (DCC), folglich enthält jede nichtleere Teilmenge von ${\mathbb{N}_0}^n$ ein bezüglich $\leq$ minimales Element.

Sei nun f ein Polynom mit minimalem Multigrad (bezüglich $\leq$), das keine Standarddarstellung durch $(f_1, \ldots, f_s)$ besitzt.

1. Fall: $f = 0$: Da $0 = \sum_{i=1}^{s} 0 f_i + 0$ eine Standarddarstellung ist, kann dieser Fall nicht eintreten.

2. Fall: $f \neq 0$: In diesem Fall gehen wir so vor: sei $g \in k[\boldsymbol{x}]$ so, dass

$$f = \textsc{Lt}(f) + g.$$

Wir werden aus einer Standarddarstellung von g eine Standarddarstellung von f bauen. Dazu unterscheiden wir zwei Fälle.

2.1. Fall: Es gibt ein $i \in \{1, \ldots, s\}$*, sodass* $f_i \neq 0$ *und* $\textsc{Lm}(f_i) | \textsc{Lm}(f)$*:* Dann gilt

$$\textsc{Deg}(f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i) < \textsc{Deg}(f).$$

Wegen der Minimalität von f gibt es $b_1, \ldots, b_s \in k[\boldsymbol{x}]$, sodass folgendes gilt:

$$f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i = \sum_{j=1}^{s} b_j f_j + r,$$

für alle $j \in \{1, \ldots, s\}$ gilt $\textsc{Deg}(b_j f_j) \leq \textsc{Deg}(f - \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i)$, und kein Monomom in r ist durch ein $\textsc{Lm}(f_j)$ mit $j \in \{1, \ldots, s\}$ teilbar.

Dann gilt

$$f = \Big(\sum_{\substack{j \in \{1,\ldots,s\} \\ j \neq i}} b_j f_j \Big) + \left(b_i + \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} \right) f_i + r$$

Da $\textsc{Deg}(b_i f_i + \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i)$ höchstens gleich dem Multigrad eines der Summanden ist, und $\textsc{Deg}(b_i f_i) < \textsc{Deg}(f)$ und $\textsc{Deg}(\frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)} f_i) = \textsc{Deg}(f)$, ist

$$(b_1, \ldots, b_{i-1},\ b_i + \frac{\textsc{Lt}(f)}{\textsc{Lt}(f_i)},\ b_{i+1}, \ldots, b_s, r)$$

eine Standarddarstellung von f durch $(f_1, \ldots, f_s)$, im Widerspruch zur Wahl von f.

2.2. Fall: Es gibt kein $i \in \{1, \ldots, s\}$*, sodass* $f_i \neq 0$ *und* $\textsc{Lm}(f_i) | \textsc{Lm}(f)$*:* Es gilt $\textsc{Deg}(f - \textsc{Lt}(f)) < \textsc{Deg}(f)$. Wegen der Minimalität von f besitzt $f - \textsc{Lt}(f)$ eine Standarddarstellung

$$f - \textsc{Lt}(f) = \sum_{j=1}^{s} b_j f_j + r.$$

Da das Mononom $\text{LM}(f)$ durch kein $\text{LM}(f_i)$ teilbar ist, ist

$$f = \sum_{j=1}^{s} b_j f_j + (r + \text{LT}(f))$$

eine Standarddarstellung von f, im Widerspruch zur Wahl von F. Folglich besitzt jedes Polynom eine Standarddarstellung bezüglich $(f_1, \ldots, f_s)$. □

3. Monomiale Ideale

DEFINITION 6.14. Sei $n \in \mathbb{N}$, sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Das Ideal I ist *monomial*, wenn es eine Teilmenge A von ${\mathbb{N}_0}^n$ gibt, sodass $I = \langle \{ \boldsymbol{x}^\alpha \mid \alpha \in A \} \rangle_{k[\boldsymbol{x}]}$.

SATZ 6.15. *Sei $n \in \mathbb{N}$, sei k ein Körper, sei I ein monomiales Ideal von $k[x_1, \ldots, x_n]$, und sei $A \subseteq {\mathbb{N}_0}^n$ so, dass*

$$I = \langle \{ \boldsymbol{x}^\alpha \mid \alpha \in A \} \rangle_{k[\boldsymbol{x}]} .$$

Dann gibt es eine endliche Teilmenge B von A, sodass

$$I = \left\langle \{ \boldsymbol{x}^\beta \mid \beta \in B \} \right\rangle_{k[\boldsymbol{x}]} .$$

Beweis: Wir nehmen an, es gibt keine solche endliche Teilmenge B von A. Wir wählen $\alpha_1 \in A$. Nun konstruieren wir rekursiv eine Folge $\langle \alpha_i \mid i \in \mathbb{N} \rangle$ aus A in folgender Weise: Sei $i \geq 2$. Es gilt nun

$$\{ \boldsymbol{x}^\alpha \mid \alpha \in A \} \not\subseteq \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{i-1}} \rangle_{k[\boldsymbol{x}]} .$$

Nehmen wir an, es gilt $\subseteq$: Dann gilt $I = \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{i-1}} \rangle_{k[\boldsymbol{x}]}$, im Widerspruch zur Annahme, dass es keine solche endliche Teilmenge von A gibt. Wir wählen α_i als ein $\alpha \in A$, sodass

$$\boldsymbol{x}^\alpha \notin \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{i-1}} \rangle_{k[\boldsymbol{x}]}$$

Wegen Lemma 6.2 gibt es nun k, l in $\mathbb{N}$ mit $k < l$ und $\alpha_k \sqsubseteq \alpha_l$. Dann gilt $\boldsymbol{x}^{\alpha_l} \in \langle \boldsymbol{x}^{\alpha_1}, \ldots, \boldsymbol{x}^{\alpha_{l-1}} \rangle_{k[\boldsymbol{x}]}$, im Widerspruch zur Wahl von α_l. □

KOROLLAR 6.16. *Sei $n \in \mathbb{N}$, sei k ein Körper, und sei I ein monomiales Ideal von $k[x_1, \ldots, x_n]$. Dann ist I endlich erzeugt.*

DEFINITION 6.17. Sei $n \in \mathbb{N}$, k ein Körper, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I eine Teilmenge von $k[x_1, \ldots, x_n]$. Dann definieren wir

$$\operatorname{LT}(I) \;:=\; \{\operatorname{LT}(f) \mid f \in I, f \neq 0\}.$$

SATZ 6.18. *Sei $n \in \mathbb{N}$, k ein Körper, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I ein Ideal von $k[x_1, \ldots, x_n]$. Dann gibt es $t \in \mathbb{N}_0$ und $g_1, \ldots, g_t \in I \setminus \{0\}$, sodass $\langle \operatorname{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$.*

Beweis: Sei $J := \langle \operatorname{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \operatorname{LM}(I) \rangle_{k[\boldsymbol{x}]}$. Klarerweise gilt dann für

$$A := \{\alpha \in {\mathbb{N}_0}^n \mid \text{ es gibt } f \in I, \text{ sodass } \operatorname{LM}(f) = \boldsymbol{x}^\alpha\}$$

die Gleichheit $J = \langle \{\boldsymbol{x}^\alpha \mid \alpha \in A\} \rangle_{k[\boldsymbol{x}]}$. Es gibt also nach Satz 6.15 eine endliche Teilmenge $B = \{\beta_1, \ldots, \beta_t\}$ von A, sodass

$$J = \left\langle \{\boldsymbol{x}^{\beta_i} \mid i \in \{1, \ldots, t\}\} \right\rangle_{k[\boldsymbol{x}]}.$$

Für jedes $i \in \{1, \ldots, t\}$ wählen wir nun ein $g_i \in I$, sodass $g_i \in I$ und $\operatorname{LM}(g_i) = \boldsymbol{x}^{\beta_i}$. Dann gilt $J = \langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. □

LEMMA 6.19. *Sei $n \in \mathbb{N}$, sei k ein Körper, sei I ein monomiales Ideal von $k[x_1, \ldots, x_n]$, und sei $A \subseteq {\mathbb{N}_0}^n$ so, dass*

$$I = \langle \{\boldsymbol{x}^\alpha \mid \alpha \in A\} \rangle_{k[\boldsymbol{x}]}.$$

Sei B eine endliche Teilmenge von ${\mathbb{N}_0}^n$, und sei $f = \sum_{\beta \in B} c_\beta \boldsymbol{x}^\beta \in k[x_1, \ldots, x_n]$. Dann sind äquivalent:

1. *$f \in I$.*
2. *Für alle $\beta \in B$ mit $c_\beta \neq 0$ gibt es ein $\alpha \in A$, sodass $\alpha \sqsubseteq \beta$.*

Beweis: (2)⇒(1): Da jeder Summand $c_\beta \boldsymbol{x}^\beta$ nach Voraussetzung in I liegt, liegt auch f in I. (1)⇒(2): Sei $f \in I$. Dann gibt es $m \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_m \in A$ und $p_1, \ldots, p_m \in k[x_1, \ldots, x_n]$, sodass

$$f = \sum_{i=1}^{m} p_i \cdot \boldsymbol{x}^{\alpha_i}.$$

Durch Ausmultiplizieren der rechten Seite sieht man, dass es für jedes in f auftretende Monom $\boldsymbol{x}^\beta$ ein j und $\gamma \in {\mathbb{N}_0}^n$ gibt, sodass

$$\boldsymbol{x}^\beta = \boldsymbol{x}^{\alpha_j + \gamma}.$$

Also gilt $\alpha_j \sqsubseteq \beta$. □

SATZ 6.20. *Sei $n \in \mathbb{N}$, sei k ein Körper, sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $t \in \mathbb{N}_0$, und seien $g_1, \ldots, g_t \in I \setminus \{0\}$ so, dass $\langle \mathrm{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. Dann gilt $I = \langle g_1, \ldots, g_t \rangle_{k[\boldsymbol{x}]}$.*

Beweis: Die Inklusion $\supseteq$ folgt aus der Tatsache, dass jedes g_i in I liegt. Für den Beweis von $\subseteq$ wählen wir $f \in I$. Sei $f = \sum_{i=1}^{t} a_i g_i + r$ eine Standarddarstellung von f durch $(g_1, \ldots, g_t)$. Wenn $r = 0$, so liegt f im von $\{g_1, \ldots, g_t\}$ erzeugten Ideal. Wir nehmen nun an, $r \neq 0$. Es gilt $r = f - \sum_{i=1}^{t} a_i g_i \in I$. Folglich gilt $\mathrm{LT}(r) \in \mathrm{LT}(I)$. Nach Voraussetzung gilt also

$$\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}.$$

Wegen Lemma 6.19 gibt es also ein $i \in \{1, \ldots, t\}$, sodass $\mathrm{LT}(g_i) | \mathrm{LT}(r)$. Dann kann r aber nicht der Rest einer Standarddarstellung von f durch $(g_1, \ldots, g_t)$ sein. Der Fall $r \neq 0$ kann also nicht eintreten. □

SATZ 6.21 (Hilbertscher Basissatz für Polynomringe über Körpern). *Sei k ein Körper, $n \in \mathbb{N}$. Dann ist jedes Ideal von $k[x_1, \ldots, x_n]$ endlich erzeugt.*

Beweis: Sei I ein Ideal von $k[x_1, \ldots, x_n]$. Nach Satz 6.18 gibt es $t \in \mathbb{N}_0$ und $g_1, \ldots, g_t \in I \setminus \{0\}$, sodass $\langle \mathrm{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$. Wegen Satz 6.20 erzeugen dann die Polynome $g_1, \ldots, g_t$ das Ideal I. □

4. Gröbnerbasen

DEFINITION 6.22. Sei k ein Körper, $n \in \mathbb{N}$, und sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^n$. Sei I ein Ideal von $k[x_1, \ldots, x_n]$. Eine endliche Teilmenge $G = \{g_1, \ldots, g_t\}$ von $k[x_1, \ldots, x_n]$ ist eine *Gröbnerbasis* von I bezüglich $\leq$, wenn

(1) $G \subseteq I \setminus \{0\}$,
(2) $\langle \mathrm{LT}(I) \rangle_{k[\boldsymbol{x}]} = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$.

Nach Satz 6.18 besitzt jedes Ideal eine Gröbnerbasis. Wenn nun I ein Ideal von $k[x_1, \ldots, x_n]$, und G eine Gröbnerbasis von I ist, so gilt nach Satz 6.20 auch $\langle G \rangle_{k[\boldsymbol{x}]} = I$.

SATZ 6.23. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $t \in \mathbb{N}_0$, und sei $G = \{g_1, \ldots, g_t\}$ eine Gröbnerbasis von I. Sei $r \in I$ so, dass kein Monom in r durch irgendein $\mathrm{LT}(g_i)$ teilbar ist. Dann gilt $r = 0$.*

Beweis: Wenn $r \neq 0$, so liegt $\mathrm{LT}(r) \in \mathrm{LT}(I)$, also in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Wegen Lemma 6.19 gibt es also ein $i \in \{1, \ldots, t\}$, sodass $\mathrm{LT}(g_i) | \mathrm{LT}(r)$. Das steht im Widerspruch zu den Voraussetzungen an r. □

SATZ 6.24. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $t \in \mathbb{N}_0$, und sei $G = \{g_1, \ldots, g_t\}$ eine Gröbnerbasis von I. Seien $r_1, r_2 \in k[x_1, \ldots, x_n]$ so, dass*

(1) $r_1 - r_2 \in I$,
(2) *Kein Monom in r_1 ist durch irgendein $\mathrm{LT}(g_i)$ teilbar,*
(3) *Kein Monom in r_2 ist durch irgendein $\mathrm{LT}(g_i)$ teilbar.*

Dann gilt $r_1 = r_2$.

Beweis: Wir nehmen an, $r_1 - r_2 \neq 0$. Dann gilt $\mathrm{LM}(r_1 - r_2) \in \mathrm{LT}(I)$. Da G eine Gröbnerbasis ist, gilt also $\mathrm{LM}(r_1 - r_2) \in \langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Das führende Monom von $r_1 - r_2$ muss auch in einem der Polynome r_1 oder r_2 vorkommen. Somit enthält eines der r_i ein Monom in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Nach Lemma 6.19 ist dieses Monom durch eines der $\mathrm{LM}(g_i)$ teilbar. Das steht im Widerspruch zu den Voraussetzungen an r_1 und r_2. □

KOROLLAR 6.25. *Sei k ein Körper, sei $n \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $t \in \mathbb{N}_0$, und sei $G = \{g_1, \ldots, g_t\}$ eine Gröbnerbasis von I. Sei $f \in k[x_1, \ldots, x_n]$, und seien*

$$f = \sum_{i=1}^{t} a_i g_i + r_1 = \sum_{i=1}^{t} b_i g_i + r_2$$

Standarddarstellungen von f durch $(g_1, \ldots, g_t)$. Dann gilt $r_1 = r_2$. Wenn außerdem $f \in I$, so gilt $r_1 = r_2 = 0$.

Beweis: Da $r_1 - r_2 \in I$, folgt die erste Behauptung aus Satz 6.24. Wenn $f \in I$ gilt, so folgt $r_1 = 0$ aus Satz 6.23. □

DEFINITION 6.26. Sei $n \in \mathbb{N}$, sei $\leq$ eine zulässige Ordnung von ${\mathbb{N}_0}^n$, sei $s \in \mathbb{N}$, und seien $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Ein Polynom $r \in k[x_1, \ldots, x_n]$ ist ein *möglicher Rest bei einer Standarddarstellung von f durch $(f_1, \ldots, f_s)$ bezüglich $\leq$*, wenn es eine Standarddarstellung $f = \sum_{i=1}^{s} a_i f_i + r$ von f durch $(f_1, \ldots, f_s)$ bezüglich $\leq$ gibt.

5. Konstruktion von Gröbnerbasen

Wir fixieren für die Sektionen 5 und 6 eine zulässige Ordnung $\leq$ auf ${\mathbb{N}_0}^n$.

DEFINITION 6.27. Sei k ein Körper, $n \in \mathbb{N}$. Seien $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n) \in {\mathbb{N}_0}^n$. Sei $\gamma = (\gamma_1, \ldots, \gamma_n)$ definiert durch $\gamma_i := \max(\alpha_i, \beta_i)$ für $i \in \{1, \ldots, n\}$. Wir definieren $\text{LCM}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta) := \boldsymbol{x}^\gamma$.

LEMMA 6.28. *Sei k ein Körper, $n \in \mathbb{N}$, und seien $\alpha, \beta \in {\mathbb{N}_0}^n$. Sei f ein Polynom mit $\boldsymbol{x}^\alpha | f$ und $\boldsymbol{x}^\beta | f$. Dann gilt $\text{LCM}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta) | f$.*

Beweis: Sei $\gamma \in {\mathbb{N}_0}^n$ so, dass $\boldsymbol{x}^\gamma = \text{LCM}(\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta)$. Nach Lemma 6.19 gilt für jedes in f vorkommende Monom $\boldsymbol{x}^\mu$, dass $\alpha \sqsubseteq \mu$ und $\beta \sqsubseteq \mu$. Also gilt $\gamma \sqsubseteq \mu$, und somit $\boldsymbol{x}^\gamma | \boldsymbol{x}^\mu$. □

DEFINITION 6.29. Sei k ein Körper, $n \in \mathbb{N}$, und seien $f, g \in k[x_1, \ldots, x_n] \setminus \{0\}$. Das *S-Polynom* oder *Subtraktionspolynom* von f und g ist definiert durch

$$S(f,g) := \frac{\text{LCM}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} \cdot f - \frac{\text{LCM}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} \cdot g.$$

LEMMA 6.30. *Sei k ein Körper, $n \in \mathbb{N}$, und seien $f, g \in k[x_1, \ldots, x_n] \setminus \{0\}$. Sei γ so, dass $\boldsymbol{x}^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$. Dann gilt $\text{DEG}(S(f,g)) < \gamma$.*

Beweis: Seien $f_1, g_1 \in k[x]$ so, dass $f = \text{LT}(f) + f_1$ und $g = \text{LT}(g) + g_1$. Dann gilt

$$\begin{aligned}
S(f,g) &= \frac{\boldsymbol{x}^{\gamma - \text{DEG}(f)}}{\text{LC}(f)} \cdot f - \frac{\boldsymbol{x}^{\gamma - \text{DEG}(g)}}{\text{LC}(g)} \cdot g \\
&= \frac{\boldsymbol{x}^{\gamma - \text{DEG}(f)}}{\text{LC}(f)} \cdot \text{LT}(f) - \frac{\boldsymbol{x}^{\gamma - \text{DEG}(g)}}{\text{LC}(g)} \cdot \text{LT}(g) + \frac{\boldsymbol{x}^{\gamma - \text{DEG}(f)}}{\text{LC}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \text{DEG}(g)}}{\text{LC}(g)} \cdot g_1 \\
&= \boldsymbol{x}^{\gamma - \text{DEG}(f)} \cdot \text{LM}(f) - \boldsymbol{x}^{\gamma - \text{DEG}(g)} \cdot \text{LM}(g) + \frac{\boldsymbol{x}^{\gamma - \text{DEG}(f)}}{\text{LC}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \text{DEG}(g)}}{\text{LC}(g)} \cdot g_1 \\
&= \boldsymbol{x}^\gamma - \boldsymbol{x}^\gamma + \frac{\boldsymbol{x}^{\gamma - \text{DEG}(f)}}{\text{LC}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \text{DEG}(g)}}{\text{LC}(g)} \cdot g_1 \\
&= \frac{\boldsymbol{x}^{\gamma - \text{DEG}(f)}}{\text{LC}(f)} \cdot f_1 - \frac{\boldsymbol{x}^{\gamma - \text{DEG}(g)}}{\text{LC}(g)} \cdot g_1.
\end{aligned}$$

Diese beiden Summanden haben wegen der Zulässigkeitseigenschaft (3) aus Definition 6.7 Multigrad $\leq \gamma$; keiner dieser Summanden hat Multigrad $= \gamma$. Die Summe hat also Multigrad $< \gamma$. □

LEMMA 6.31. *Sei k ein Körper, seien $n, s \in \mathbb{N}$, und $f_1, \ldots, f_s \in k\backslash\{0\}$, $c_1, \ldots, c_s \in k \setminus \{0\}$, und $\delta, \alpha_1, \ldots, \alpha_s \in {\mathbb{N}_0}^n$ so, dass folgendes gilt:*

(1) *Für alle $i \in \{1, \ldots, s\}$ gilt* $\text{DEG}(\boldsymbol{x}^{\alpha_i} f_i) = \delta$.
(2) $\text{DEG}(\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i) < \delta$.

Dann gibt es $b_1, \ldots, b_{s-1} \in k$, sodass

$$\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i = \sum_{j=1}^{s-1} b_j \frac{\boldsymbol{x}^{\delta}}{\text{LCM}(\text{LM}(f_j), \text{LM}(f_s))} S(f_j, f_s). \tag{5.1}$$

Beweis Für $j \in \{1, \ldots, s-1\}$ sei $\gamma_j \in {\mathbb{N}_0}^n$ so, dass

$$\boldsymbol{x}^{\gamma_j} = \text{LCM}(\text{LM}(f_j), \text{LM}(f_s)).$$

Dann lässt sich die behauptete Gleichung (5.1) als

$$\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i = \sum_{j=1}^{s-1} b_j \boldsymbol{x}^{\delta - \gamma_j} S(f_j, f_s)$$

schreiben.

In der Summe auf der linken Seite von (5.1) hat jeder Summand Multigrad δ. Da nach Voraussetzung (2) die Summe kleineren Multigrad hat, muss der Koeffizient von $\boldsymbol{x}^{\delta}$ in $\sum_{i=1}^{s-1} c_i \boldsymbol{x}^{\alpha_i} f_i$ gleich 0 sein. Es gilt also

$$\sum_{i=1}^{s} c_i \text{LC}(f_i) = 0.$$

Dann gilt

$$\begin{aligned}
\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i &= \sum_{i=1}^{s-1} \left(c_i \boldsymbol{x}^{\alpha_i} f_i - c_i \frac{\text{LC}(f_i)}{\text{LC}(f_s)} \boldsymbol{x}^{\alpha_s} f_s \right) \\
&\quad + \left(\sum_{i-1}^{s-1} c_i \frac{\text{LC}(f_i)}{\text{LC}(f_s)} \boldsymbol{x}^{\alpha_s} f_s \right) + c_s \boldsymbol{x}^{\alpha_s} f_s \\
&= \sum_{i=1}^{s-1} \left(c_i \boldsymbol{x}^{\alpha_i} f_i - c_i \frac{\text{LC}(f_i)}{\text{LC}(f_s)} \boldsymbol{x}^{\alpha_s} f_s \right) + \left(\sum_{i=1}^{s} c_i \frac{\text{LC}(f_i)}{\text{LC}(f_s)} \right) \boldsymbol{x}^{\alpha_s} f_s.
\end{aligned}$$

Da $\sum_{i=1}^{s} c_i \text{LC}(f_i) = 0$, gilt

$$\begin{aligned}
\sum_{i=1}^{s} c_i \boldsymbol{x}^{\alpha_i} f_i &= \sum_{i=1}^{s-1} c_i \left(\frac{\boldsymbol{x}^{\delta}}{\text{LM}(f_i)} f_i - \frac{\text{LC}(f_i)}{\text{LC}(f_s)} \frac{\boldsymbol{x}^{\delta}}{\text{LM}(f_s)} f_s \right) \\
&= \sum_{i=1}^{s-1} c_i \text{LC}(f_i) \left(\frac{\boldsymbol{x}^{\delta}}{\text{LT}(f_i)} f_i - \frac{\boldsymbol{x}^{\delta}}{\text{LT}(f_s)} f_s \right) \\
&= \sum_{i=1}^{s-1} c_i \text{LC}(f_i) \boldsymbol{x}^{\delta - \gamma_i} \left(\frac{\boldsymbol{x}^{\gamma_i}}{\text{LT}(f_i)} f_i - \frac{\boldsymbol{x}^{\gamma_i}}{\text{LT}(f_s)} f_s \right) \\
&= \sum_{i=1}^{s-1} c_i \text{LC}(f_i) \boldsymbol{x}^{\delta - \gamma_i} S(f_i, f_s).
\end{aligned}$$

□

SATZ 6.32 (Buchbergers Kriterium, cf. [**Buc70**]). *Sei k ein Körper, seien $n, t \in \mathbb{N}$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $G = \{g_1, \ldots, g_t\}$ eine endliche Teilmenge von $I \setminus \{0\}$, sodass folgendes gilt:*

1. $\langle G \rangle_{k[\boldsymbol{x}]} = I$,
2. *Für alle $i, j \in \{1, \ldots, t\}$ mit $i < j$ ist 0 ein möglicher Rest einer Standarddarstellung von $S(g_i, g_j)$ durch $(g_1, \ldots, g_t)$.*

Dann ist G eine Gröbnerbasis von I.

Beweis: Sei $f \in I$ mit $f \neq 0$. Wir zeigen, dass $\text{LT}(f)$ im Ideal $\langle LT(g_1), \ldots, \text{LT}(g_t) \rangle_{k[\boldsymbol{x}]}$ liegt. Da G das Ideal I erzeugt, gibt es $h'_1, \ldots, h'_t \in k[x_1, \ldots, x_n]$, sodass

$$f = \sum_{i=1}^{t} h'_i g_i.$$

Für jede solche Darstellung sei

$$\delta' := \max\{\text{DEG}(h'_i g_i) \mid i \in \{1, \ldots, t\}\}.$$

Seien nun $h_1, \ldots, h_t \in k[x_1, \ldots, x_n]$ so unter allen Darstellungen von f als $\sum_{i=1}^{t} h'_i f_i$, dass δ' minimal wird, und sei

$$\delta := \max\{\text{DEG}(h_i g_i) \mid i \in \{1, \ldots, t\}\}.$$

Es gilt

$$f = \sum_{i=1}^{t} h_i g_i,$$

also $\textsc{Deg}(f) \leq \delta$.

1. Fall: $\textsc{Deg}(f) = \delta$*:* Sei $i \in \{1, \ldots, t\}$ so, dass $\textsc{Deg}(h_i g_i) = \delta$. Dann gilt $\textsc{Lt}(g_i) | \textsc{Lt}(f)$, und somit $\textsc{Lt}(f) \in \langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}$.

2. Fall: $\textsc{Deg}(f) < \delta$*:* Für $i \in \{1, \ldots, t\}$ sei $m(i) := \textsc{Deg}(h_i g_i)$. Es gilt dann

$$\begin{aligned} f = \sum_{i=1}^{t} h_i g_i = & \sum_{\substack{i=1 \\ m(i)=\delta}}^{t} h_i g_i + \sum_{\substack{i=1 \\ m(i)<\delta}}^{t} h_i g_i \\ = & \sum_{\substack{i=1 \\ m(i)=\delta}}^{t} \textsc{Lt}(h_i) g_i + \sum_{\substack{i=1 \\ m(i)=\delta}}^{t} (h_i - \textsc{Lt}(h_i)) g_i + \sum_{\substack{i=1 \\ m(i)<\delta}}^{t} h_i g_i. \end{aligned}$$

Alle Summanden der zweiten und dritten Summe haben Multigrad $< \delta$. Da auch $\textsc{Deg}(f) < \delta$, gilt

$$\textsc{Deg}\Big(\sum_{\substack{i=1 \\ m(i)=\delta}}^{t} \textsc{Lt}(h_i) g_i \Big) < \delta.$$

Seien $s \in \mathbb{N}$ und $i_1, \ldots, i_s$ so, dass $i_1 < \cdots < i_s$ und $\{i_j \mid j \in \{1, \ldots, s\}\} = \{i \in \{1, \ldots, t\} \mid m(i) = \delta\}$. Wir verwenden nun Lemma 6.31 für $f_j := g_{i_j}$, $c_j := \textsc{Lc}(h_{i_j})$ und α_j so, dass $\boldsymbol{x}^{\alpha_j} := \textsc{Lm}(h_{i_j})$ $(j \in \{1, \ldots, s\})$. Aus diesem Lemma erhalten wir für $j, l \in \{1, \ldots, t\}$ mit $j < l$ Körperelemente $b_{j,l} \in k$, sodass

$$\sum_{\substack{i=1 \\ m(i)=\delta}}^{t} \textsc{Lt}(h_i) g_i = \sum_{\substack{j,l \in \{1,\ldots,t\} \\ j<l}} b_{j,l} \frac{\boldsymbol{x}^{\delta}}{\textsc{Lcm}(\textsc{Lm}(g_j), \textsc{Lm}(g_l))} S(g_j, g_l).$$

Da $S(g_j, g_l)$ nach Voraussetzung eine Standarddarstellung mit Rest 0 besitzt, gibt es für $j < l$ Polynome $a_{j,l,1}, \ldots, a_{j,l,t} \in k[\boldsymbol{x}]$, sodass

$$S(g_j, g_l) = \sum_{i=1}^{t} a_{j,l,i} \cdot g_i,$$

und $\text{DEG}(a_{j,l,i}g_i) \leq \text{DEG}(S(g_j, g_l))$ für alle $i \in \{1, \ldots, t\}$. Sei nun $\gamma_{j,l} \in {\mathbb{N}_0}^n$ so, dass $\boldsymbol{x}^{\gamma_{j,l}} = \text{LCM}(\text{LM}(g_j), \text{LM}(g_l))$. Also gilt

$$\begin{aligned}
&\sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<l}} b_{j,l}\frac{\boldsymbol{x}^\delta}{\text{LCM}(\text{LM}(g_j), \text{LM}(g_l))}S(g_j, g_l)\\
&\qquad = \sum_{i=1}^{t} \sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<l}} b_{j,l}\frac{\boldsymbol{x}^\delta}{\text{LCM}(\text{LM}(g_j), \text{LM}(g_l))}a_{j,l,i}g_i\\
&\qquad = \sum_{i=1}^{t} \sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<l}} b_{j,l}\boldsymbol{x}^{\delta-\gamma_{j,l}}a_{j,l,i}g_i.
\end{aligned}$$

Wir berechnen nun den Multigrad des (j, l, i)-ten Summanden

$$\sigma(j, l, i) := b_{j,l}\boldsymbol{x}^{\delta-\gamma_{j,l}}a_{j,l,i}g_i.$$

Es gilt $\text{DEG}(\sigma(j, l, i)) \leq \delta - \gamma_{j,l} + \text{DEG}(a_{j,l,i}g_i) \leq \delta - \gamma_{j,l} + \text{DEG}(S(g_j, g_l))$. Wegen Lemma 6.30 gilt $\text{DEG}(S(g_j, g_l)) < \gamma_{j,l}$, also gilt

$$\text{DEG}(\sigma(j, l, i)) < \delta.$$

Daher ist

$$f = \sum_{\substack{i=1\\ m(i)=\delta}}^{t} \Big(\big(\sum_{\substack{j,l\in\{1,\ldots,t\}\\ j<k}} b_{j,l}\boldsymbol{x}^{\delta-\gamma j,l}a_{i,j,l}\big) + (h_i - \text{LT}(h_i))\Big) \cdot g_i + \sum_{\substack{i=1\\ m(i)<\delta}}^{t} h_i g_i$$

eine Darstellung von f, in der jeder Summand Multigrad $< \delta$ hat. Das ist ein Widerspruch zur Wahl von δ. Der 2. Fall kann also nicht eintreten. □

Das Hinzufügen eines möglichen Restes des betrachteten S-Polynoms bewirkt, dass dieses S-Polynom 0 als möglichen Rest hat:

LEMMA 6.33. *Sei k ein Körper, $n \in \mathbb{N}$, sei $(f_1, \ldots, f_s)$ eine Folge von Polynomen aus $k[x_1, \ldots, x_n]$. Sei $f \in k[x_1, \ldots, x_n]$, und sei $r \in k[x_1, \ldots, x_n]$ ein möglicher Rest von f bei einer Standarddarstellung von f durch $(f_1, \ldots, f_s)$. Dann ist 0 ein möglicher Rest von f bei einer Standarddarstellung von f durch $(f_1, \ldots, f_s, r)$.*

Beweis: Sei $f = \sum_{i=1}^{s} a_i f_i + r$ eine Standarddarstellung von f durch $(f_1, \ldots, f_s)$. Da $r = f - \sum_{i=1}^{s} a_i f_i$, gilt $\textsc{Deg}(r) \leq \textsc{Deg}(f)$. Also ist $f = \sum_{i=1}^{s} a_i f_i + 1r + 0$ eine Standarddarstellung von f durch $(f_1, \ldots, f_s, r)$ mit Rest 0. □

Algorithmus 6.34 (Buchbergers Algorithmus zur Konstruktion einer Gröbnerbasis).
Eingabe: $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$.
Ausgabe: $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ so, dass $G := \{g_1, \ldots, g_t\}$ eine Gröbnerbasis für $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$ ist.

1 $G \leftarrow (f_1, \ldots, f_s)$
2 $P \leftarrow \emptyset$
3 **while** $\exists f, g \in G : f \neq g$ und $\{f, g\} \notin P$
4 **do** $P \leftarrow P \cup \big\{\{f, g\}\big\}$
5 $r \leftarrow \begin{cases} \text{Ein möglicher Rest von } S(f,g) \\ \text{bei Standarddarstellung durch } G \end{cases}$
6 **if** $r \neq 0$
7 **then** $G \leftarrow (G, r)$

Satz 6.35. *Sei k ein Körper, und seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$. Der Algorithmus 6.34 terminiert und liefert als Ergebnis eine Gröbnerbasis für $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$.*

Beweis: Wir zeigen als erstes, dass der Algorithmus terminiert. Wir betrachten am Beginn jedes Durchlaufs der *while*-Schleife das Paar $(\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}, |\binom{G}{2} \setminus P|)$. Nehmen wir an, die Schleife würde unendlich oft durchlaufen. Wegen des Hilbertschen Basissatzes gibt es keine unendlichen aufsteigenden Ketten von Idealen von $k[x_1, \ldots, x_n]$.

Ab irgendeinem Durchlauf bleibt also $\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}$ konstant. Ab diesem Durchlauf der Schleife kann aber der Fall $r \neq 0$ nicht mehr eintreten. Wenn nämlich r ein möglicher Rest von $S(f, g)$ bei einer Standarddarstellung durch G ist, und $r \neq 0$, so liegt $\textsc{Lt}(r)$ nicht in $\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]}$. Dann gilt aber $\langle \textsc{Lt}(G) \rangle_{k[\boldsymbol{x}]} \neq \langle \textsc{Lt}(G \cup \{r\}) \rangle_{k[\boldsymbol{x}]}$.

Folglich erniedrigt sich ab diesem Durchlauf die zweite Komponente $|\binom{G}{2} \setminus P|$. Diese Komponente kann nicht negativ werden.

Somit kann die *while*-Schleife nicht unendlich oft durchlaufen werden, also terminiert der Algorithmus.

Wir zeigen nun die Korrektheit des Algorithmus: Am Beginn jedes Durchlaufs der *while*-Schleife gilt, dass für alle $f, g \in G$ mit $\{f, g\} \in P$ das S-Polynom $S(f, g)$ eine Standarddarstellung durch G mit Rest 0 hat. Das gilt offensichtlich beim ersten Betreten der *while*-Schleife wegen $P = \emptyset$. Im weiteren Verlauf garantiert Lemma 6.33, das diese Bedingung erhalten bleibt.

Wenn die *while*-Schleife verlassen wird, liegen alle Elemente aus $\binom{G}{2}$ in P. Folglich haben alle S-Polynome von Paaren von Polynomen aus G das Polynom 0 als möglichen Rest bei Standarddarstellung durch G. Nach Satz 6.32 ist G daher eine Gröbnerbasis von $\langle G \rangle_{k[\boldsymbol{x}]}$. $\langle G \rangle_{k[\boldsymbol{x}]}$ ist aber während des gesamten Verlaufs des Algorithmus stets $\langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$. □

6. Konstruktion von reduzierten Gröbnerbasen

In dieser Sektion stellen wir einige Resultate zusammen, die es uns erlauben, die Zwischenergebnisse beim Berechnen einer Gröbnerbasis zu vereinfachen. Als Resultate erhalten wir "reduzierte Gröbnerbasen".

LEMMA 6.36. *Seien $f_1, \ldots, f_s$ paarweise verschiedene Elemente von $k[x_1, \ldots, x_n]$, und sei $F := \{f_1, \ldots, f_s\}$. Sei $i \in \{1, \ldots, s\}$, und sei $r_i \in k[x_1, \ldots, x_n]$ ein möglicher Rest von f_i bei einer Standarddarstellung durch $F \setminus \{f_i\}$. Sei $G := (F \setminus \{f_i\}) \cup \{r_i\}$. Dann gilt:*

(1) $\langle G \rangle_{k[\boldsymbol{x}]} = \langle F \rangle_{k[\boldsymbol{x}]}$,
(2) $\langle \mathrm{LT}(F) \rangle_{k[\boldsymbol{x}]} \subseteq \langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$,
(3) *Wenn $r_i \neq 0$ und $\mathrm{LM}(r_i) \neq \mathrm{LM}(f_i)$, so gilt $\mathrm{LT}(r_i) \notin \langle \mathrm{LT}(F) \rangle_{k[\boldsymbol{x}]}$.*
(4) *Für alle $q \in k[\boldsymbol{x}]$ gilt: Wenn 0 ein möglicher Rest von q bei einer Standarddarstellung durch F ist, so ist 0 auch ein möglicher Rest von q bei einer Standarddarstellung durch G.*

Beweis: (1) Für $\subseteq$ beobachten wir, dass r_i in $\langle F \rangle_{k[\boldsymbol{x}]}$ liegt. Somit gilt $G \subseteq \langle F \rangle_{k[\boldsymbol{x}]}$. Für $\supseteq$ zeigen wir, $f_i \in \langle G \rangle_{k[\boldsymbol{x}]}$. Wir wissen, dass es $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_s \in k[\boldsymbol{x}]$ gibt, sodass

$$f_i = \sum_{\substack{j=1 \\ j \neq i}}^{s} a_j f_j + r_i.$$

Da $r_i \in G$, gilt $f_i \in \langle G \rangle_{k[\boldsymbol{x}]}$.

(2) Es reicht zu zeigen, dass im Fall $f_i \neq 0$ gilt, dass $\text{LT}(f_i) \in \text{LT}(G)$ liegt. Wir wissen, dass f_i eine Standarddarstellung durch $F \setminus \{f_i\}$ mit Rest r_i besitzt. Somit gibt es $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_s \in k[\boldsymbol{x}]$, sodass

$$f_i = \sum_{\substack{j=1 \\ j \neq i}}^{s} a_j f_j + r_i,$$

und alle Summanden auf der rechten Seite Multigrad $\leq \text{DEG}(f_i)$ haben. Einer der Summanden muss daher Multigrad $\text{DEG}(f_i)$ haben. Ist das $a_j f_j$ für ein $j \neq i$, so gilt $\text{LT}(f_j)|\text{LT}(f_i)$, und somit $\text{LT}(f_i) \in \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Wenn $\text{DEG}(r_i) = \text{DEG}(f_i)$, so gilt $\text{LT}(r_i)|\text{LT}(f_i)$, und folglich $\text{LT}(f_i) \in \langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$.

(3) Wir nehmen an, dass $r_i \neq 0$. Wenn nun $\text{LT}(r_i) \in \langle \text{LT}(F) \rangle_{k[\boldsymbol{x}]}$, so gibt es ein $k \in \{1, \ldots, s\}$, sodass $\text{LT}(f_k)|\text{LT}(r_i)$. Da r_i ein möglicher Rest einer Standarddarstellung durch $F \setminus \{f_i\}$ ist, muss $k = i$ sein. Es gilt also $\text{LT}(f_i)|\text{LT}(r_i)$, und folglich $\text{DEG}(f_i) \leq \text{DEG}(r_i)$. Da r_i Rest einer Standarddarstellung von f_i ist, gilt aber auch $\text{DEG}(r_i) \leq \text{DEG}(f_i)$. Somit gilt $\text{DEG}(r_i) = \text{DEG}(f_i)$, und somit $\text{LM}(r_i) = \text{LM}(f_i)$.

(4) Wir nehmen an, dass q eine Standarddarstellung

$$q = \sum_{j=1}^{s} a_j f_j + 0$$

durch F mit Rest 0 besitzt. Weiters besitzt f_i eine Standarddarstellung durch $F \setminus \{f_i\}$ mit Rest r_i; es gibt also $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_s$, sodass

$$f_i = \sum_{\substack{l=1 \\ l \neq i}}^{s} b_l f_l + r_i.$$

Insgesamt gilt also

$$q = \sum_{j=1}^{s} a_j f_j + a_i \Big(\sum_{\substack{l=1 \\ l \neq i}}^{s} b_l f_l + r_i \Big),$$

also

$$q = \sum_{\substack{j=1 \\ j\neq i}}^{s} (a_j + a_i b_j) f_j + a_i r_i. \tag{6.1}$$

Es gilt $\text{DEG}(b_j f_j) \leq \text{DEG}(f_i)$, also auch $\text{DEG}(a_i b_j f_j) \leq \text{DEG}(a_i f_i) \leq \text{DEG}(q)$. Wegen $\text{DEG}(r_i) \leq \text{DEG}(f_i)$ gilt auch $\text{DEG}(a_i r_i) \leq \text{DEG}(a_i f_i) \leq \text{DEG}(q)$. Also ist die Darstellung von q in (6.1) eine Standarddastellung von q durch G. □

DEFINITION 6.37. Sei F eine endliche Teilmenge von $k[x_1, \ldots, x_n] \setminus \{0\}$, und sei $f \in F$. Dann ist f *reduziert in* F, wenn kein Monom in f durch ein $\text{LT}(g)$ mit $g \in F \setminus \{f\}$ teilbar ist.

Das Polynom f ist also reduziert in F, wenn

$$f = \sum_{\substack{g\in F \\ g\neq f}} 0 \cdot g + f$$

eine Standarddarstellung von f durch $F \setminus \{f\}$ mit Rest f ist.

DEFINITION 6.38. Sei F eine endliche Teilmenge von $k[x_1, \ldots, x_n] \setminus \{0\}$. F ist *reduziert*, wenn alle $f \in F$ reduziert in F sind.

Wir betrachten nun folgende Prozedur zur Erzeugung einer Gröbnerbasis.

ALGORITHMUS 6.39 (Erzeugen einer Gröbnerbasis mit Vereinfachung).
Eingabe: $f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \setminus \{0\}$.
Ausgabe: $g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ so, dass $G := \{g_1, \ldots, g_t\}$ eine Gröbnerbasis für $\langle \{f_1, \ldots, f_s\} \rangle_{k[\boldsymbol{x}]}$ ist.

```
1   G ← {f_1, ..., f_s}
2   P ← ∅
3   while ∃ f, g ∈ G : f ≠ g und {f, g} ∉ P
4       do P ← P ∪ {{f, g}}
5          r ← { Ein möglicher Rest von S(f, g)
               { bei Standarddarstellung durch G
6          if r ≠ 0
7             then G ← (G, r)
8          while G ist nicht reduziert und wir wollen G reduzieren
```

```
 9        do f_1 ← Ein Element von G, das in G nicht reduziert ist
10           r_1 ← { Ein möglicher Rest von f_1
                   { bei Standarddarstellung durch G \ {f_1}
11           if r_1 = 0
12              then G ← G \ {f_1}
13              else   G ← (G \ {f_1}) ∪ {r_1}
```

SATZ 6.40. *Unabhängig davon, wie oft wir im Ablauf des Algorithmus reduzieren wollen, terminiert der Algorithmus 6.39 und liefert eine Gröbnerbasis von* $I := \langle f_1, \ldots, f_s \rangle_{k[\boldsymbol{x}]}$.

Beweis: Am Beginn jedes Durchlaufs der äußeren *while*-Schleife gilt für alle $\{f, g\} \in P$, dass $S(f, g)$ eine Standarddarstellung durch G mit Rest 0 besitzt, und dass $\langle G \rangle_{k[\boldsymbol{x}]} = I$ ist: klarerweise gilt das beim ersten Betreten der *while*-Schleife. Wegen Lemma 6.33 bleiben diese Bedingungen auch durch das Hinzufügen des Restes r des S-Polynoms $S(f, g)$ erhalten. Nun bleibt diese Bedingung auch bei jedem Durchlauf der inneren *while*-Schleife erhalten: Lemma 6.36 (1) liefert, dass $\langle G \rangle_{k[\boldsymbol{x}]}$ immer gleich dem Ideal I ist. Lemma 6.36 (4) garantiert, dass die S-Polynome aller Paare aus P auch nach dem Reduzieren 0 als möglichen Rest haben. Wenn der Algorithmus terminiert, so wurde die äußere *while*-Schleife verlassen: für alle $\{f, g\} \in \binom{G}{2}$ gilt also $\{f, g\} \in P$; somit hat $S(f, g)$ eine Standarddarstellung durch G mit Rest 0. Nach Satz 6.32 ist G also eine Gröbnerbasis von $\langle G \rangle_{k[\boldsymbol{x}]} = I$.

Wir zeigen nun, dass der Algorithmus für jede Eingabe terminiert. Sei dazu $F = (f_1, \ldots, f_s)$ eine Eingabe, und seien unsere möglichen Wahlen während des Ablaufs des Algorithmus so, dass der Algorithmus nicht hält. Nun betrachten wir zunächst nach jedem Betreten einer der *while*-Schleifen das Ideal $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Wegen Lemma 6.36 (2) wird dieses Ideal von einem Betreten zum nächsten echt größer, oder es bleibt gleich. Da $k[\boldsymbol{x}]$ die (ACC) für Ideale erfüllt, bleibt dieses Ideal ab irgendwann stets konstant.

Ab diesem Punkt betrachten wir die Anzahl der Elemente von G, die in G nicht reduziert sind. Wir behaupten, dass ab diesem Durchlauf we die Anzahl der nicht reduzierten Elemente in G nicht mehr größer wird. Zunächst kann ab diesem Durchlauf der Schleife der Fall $r \neq 0$ nicht mehr eintreten. Wenn nämlich r ein möglicher Rest von $S(f, g)$ bei einer Standarddarstellung durch G ist, und $r \neq 0$, so liegt $\mathrm{LT}(r)$ nicht in $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Dann gilt aber $\langle \mathrm{LT}(G) \rangle_{k[\boldsymbol{x}]} \neq \langle \mathrm{LT}(G \cup \{r\}) \rangle_{k[\boldsymbol{x}]}$. Nun

überlegen wir uns, warum auch die Anweisungen in der inneren *while*-Schleife die Anzahl der nicht reduzierten Elemente von G nicht erhöhen: Alle in G reduzierten Elemente von $G \setminus \{f_1\}$ sind auch reduziert in $G \setminus \{f_1\}$. Also könnte nur die Anweisung $G \leftarrow (G \setminus \{f_1\}) \cup \{r_1\}$ die Anzahl der nicht reduzierten Elemente von G erhöhen. In diesem Fall gilt $r_1 \neq 0$. Da ja $\text{LT}(G)$ konstant bleibt, bleibt wegen Lemma 6.36 (3) nur mehr der Fall $\text{LM}(r_1) = \text{LM}(f_1)$ übrig. Dann ist aber jedes Element von $(G \setminus \{f_1\}) \cup \{r_1\}$, das in $G \setminus \{f_1\} \cup \{r_1\}$ nicht reduziert ist, auch in G nicht reduziert. Keine Anweisung kann also die Anzahl der in G nicht reduzierten Elemente von G mehr erhöhen. Ab irgendeinem Durchlauf bleibt also auch die Anzahl der in G nicht reduzierten Elemente von G konstant.

Ab diesem Durchlauf betrachten wir $|G| + |\binom{G}{2} \setminus P|$. Von den Zuweisungen an G kann nun einzig die Zuweisung $G \leftarrow G \setminus \{f_1\}$ noch ausgeführt werden, da die Zuweisung $G \leftarrow (G \setminus \{f_1\}) \cup \{r_1\}$ ja bewirkt, dass die Anzahl der nicht reduzierten Elemente von G wegen $\text{LM}(r_1) = \text{LM}(f_1)$ um 1 kleiner wird, im Widerspruch dazu, dass die Anzahl der in G nicht reduzierten Elemente konstant bleibt. Jede der Zuweisungen $G \leftarrow G \setminus \{f_1\}$ und $P \leftarrow P \cup \{\{f, g\}\}$ bewirkt aber, dass $|G| + |\binom{G}{2} \setminus P|$ echt kleiner wird. Das kann aber nur endlich oft passieren.

Also hält der Algorithmus nach diesen endlichen vielen Schritten. □

Wenn wir immer reduzieren wollen, und die führenden Koeffizienten des Ergebnisses auf 1 normieren, so erhalten wir als Ergebnis des Algorithmus 6.39 eine "reduzierte Gröbnerbasis".

DEFINITION 6.41. Sei k ein Körper, und sei G eine endliche Teilmenge von $k[x_1, \ldots, x_n] \setminus \{0\}$. G ist eine *reduzierte Gröbnerbasis* von $\langle G \rangle_{k[\boldsymbol{x}]}$, wenn:

(1) G ist eine Gröbnerbasis von $\langle G \rangle_{k[\boldsymbol{x}]}$,
(2) G ist reduziert,
(3) Alle Polynome $g \in G$ erfüllen $\text{LC}(g) = 1$.

Als Konsequenz aus der Termination und Korrektheit des Algorithmus 6.39 erhalten wir:

SATZ 6.42. *Jedes Ideal von $k[x_1, \ldots, x_n]$ besitzt eine reduzierte Gröbnerbasis.*

Diese reduzierte Gröbnerbasis eines Ideals ist, ähnlich der Zeilenstaffelnormalform eines Unterraums, durch das Ideal eindeutig bestimmt.

SATZ 6.43. *Sei I ein Ideal von $k[x_1, \ldots, x_n]$, sei $\leq$ eine zulässige Ordnung auf $\mathbb{N}_0{}^n$, und seien G, H reduzierte Gröbnerbasen von I bezüglich $\leq$. Dann gilt $G = H$.*

Beweis: Wir nehmen an, dass $I \neq 0$. Als erstes zeigen wir

$$\text{LT}(G) = \text{LT}(H).$$

Sei $G = \{g_1, \ldots, g_r\}$ und $H = \{h_1, \ldots, h_s\}$. Sei nun $g \in G$. Da g eine Standarddarstellung durch H mit Rest 0 besitzt, gibt es $a_1, \ldots, a_s \in k[\boldsymbol{x}]$, sodass $g = \sum_{i=1}^{s} a_i h_i$, und für alle i gilt $\text{DEG}(a_i h_i) \leq \text{DEG}(g)$. Für zumindest einen Summanden muss $\text{DEG}(a_j h_j) = \text{DEG}(g)$ sein. Da h_j eine Standarddarstellung durch G mit Rest 0 besitzt, gibt es $b_1, \ldots, b_r \in k[\boldsymbol{x}]$, sodass $h_j = \sum_{l=1}^{r} b_l g_l$, und für alle l gilt $\text{DEG}(b_l g_l) \leq \text{DEG}(h_j)$. Sei l so, dass $\text{DEG}(h_j) = \text{DEG}(b_l g_l)$. Dann gilt $\text{LT}(g_l) | \text{LT}(h_j)$ und $\text{LT}(h_j) | \text{LT}(g)$. Es gilt also $\text{LT}(g_l) | \text{LT}(g)$. Da G reduziert ist, gilt $g = g_l$. Nun gilt $\text{LM}(g_l) | \text{LM}(h_j)$ und $\text{LM}(h_j) | \text{LM}(g)$. Wegen $g_l = g$ gilt also $\text{LM}(g) = \text{LM}(h_j)$. Folglich gilt $\text{LT}(g) \in \text{LT}(H)$. Damit haben wir $\text{LT}(G) \subseteq \text{LT}(H)$ bewiesen.

Ebenso gilt $\text{LT}(H) \subseteq \text{LT}(G)$. Insgesamt gilt also $\text{LT}(G) = \text{LT}(H)$.

Wir zeigen nun $G \subseteq H$. Sei dazu $g \in G$. Es gibt nun ein Polynom $h \in H$, sodass $\text{LT}(g) = \text{LT}(h)$. Da G reduziert ist, enthält $g - \text{LT}(g)$ kein Monom, das in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$ liegt. Da H reduziert ist, enthält $h - \text{LT}(h)$ kein Monom, das in $\langle \text{LT}(H) \rangle_{k[\boldsymbol{x}]}$ liegt. Wegen $\text{LT}(G) = \text{LT}(H)$ liegt also auch kein Monom von $h - \text{LT}(h)$ in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Somit liegt wegen $\text{LT}(g) = \text{LT}(h)$ kein Monom von $g - h = (g - \text{LT}(g)) - (h - \text{LT}(h))$ in $\langle \text{LT}(G) \rangle_{k[\boldsymbol{x}]}$. Somit ist $g - h = \sum_{i=1}^{r} 0 \cdot g_r + (g - h)$ eine Standarddarstellung von $g - h$ durch G mit Rest $g - h$. Da G eine Gröbnerbasis von I ist, und da $g - h \in I$, gilt wegen Korollar 6.25 die Gleichheit $g = h$. Somit gilt $g \in H$.

Ebenso zeigt man $H \subseteq G$. □

Das folgende Kriterium erspart die Überprüfung der S-Polynome jener Paare, deren führende Monome keine gemeinsamen Variablen enthalten.

LEMMA 6.44. *Sei k ein Körper, sei F eine endliche Teilmenge von $k[x_1, \ldots, x_n]$, und seien $f, g \in F \setminus \{0\}$ so, dass $\text{LCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g)$. Dann ist 0 ein möglicher Rest von $S(f, g)$ bei Standarddarstellung durch F.*

Beweis: Sei $p := f - \text{LT}(f)$ und $q := g - \text{LT}(g)$. Dann gilt

$$\begin{aligned} S(f,g) &= \frac{\text{LM}(g)}{\text{LC}(f)} f - \frac{\text{LM}(f)}{\text{LC}(g)} g \\ &= \frac{\text{LT}(g)}{\text{LC}(f)\text{LC}(g)} f - \frac{\text{LT}(f)}{\text{LC}(f)\text{LC}(g)} g \\ &= \frac{1}{\text{LC}(f)\text{LC}(g)} (\text{LT}(g) f - \text{LT}(f) g). \end{aligned}$$

Es gilt

$$\begin{aligned} \text{LT}(g) f - \text{LT}(f) g &= (g - q) f - (f - p) g \\ &= qf + pg. \end{aligned}$$

Wir behaupten nun, dass $qf + pg$ eine Standarddastellung von $\text{LT}(g) f - \text{LT}(f) g$ durch (f, g) ist. Wenn $p = q = 0$, ist das offensichtlich.

Wir nehmen nun an, dass $p \neq 0$ und betrachten zuerst den Fall, dass $\text{DEG}(qf) = \text{DEG}(pg)$. Dann gilt $\text{LM}(f) | \text{LM}(p)\text{LM}(g)$. Da $\text{LM}(f)$ und $\text{LM}(g)$ keine gemeinsamen Variablen enthalten, gilt $\text{LM}(f) | \text{LM}(p)$. Das steht aber im Widerspruch zu $\text{DEG}(p) < \text{DEG}(f)$. Somit gilt $\text{DEG}(qf) \neq \text{DEG}(pg)$. Damit gilt aber $\text{DEG}(qf + pg) = \max(\text{DEG}(qf), \text{DEG}(pg))$. Somit gilt also $\text{DEG}(qf) < \text{DEG}(qf + pg)$ und $\text{DEG}(pg) < \text{DEG}(qf + pg)$. Damit ist aber $qf + pg$ eine Standarddarstellung von $qf + pg$ durch (f, g) mit Rest 0.

Der Fall $q \neq 0$ lässt sich genauso behandeln. □

7. Die Eliminationseigenschaft von Gröbnerbasen

SATZ 6.45. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$. Sei $\leq$ eine zulässige Ordnung auf ${\mathbb{N}_0}^{m+n}$, sodass für alle $\alpha \in {\mathbb{N}_0}^m$ und $\beta \in {\mathbb{N}_0}^n$ mit $\alpha \neq (0, \ldots, 0)$ gilt: $\boldsymbol{x}^\alpha > \boldsymbol{y}^\beta$. Sei G eine Gröbnerbasis von I bezüglich dieser Ordnung. Dann ist $G \cap k[\boldsymbol{y}]$ eine Gröbnerbasis des Ideals $I \cap k[\boldsymbol{y}]$ von $k[\boldsymbol{y}]$.*

Beweis: Sei $G_{\boldsymbol{y}} := G \cap k[\boldsymbol{y}]$. Wir zeigen nun, dass für alle $f \in I \cap k[\boldsymbol{y}]$ mit $f \neq 0$ auch dass $\text{LT}(f) \in \langle \text{LT}(G_{\boldsymbol{y}}) \rangle_{k[\boldsymbol{y}]}$ gilt. $f = \sum_{i=1}^{t} a_i g_i$ eine Standarddarstellung von f durch G. Da für alle i mit $a_i g_i \neq 0$ gilt, dass $\text{DEG}(a_i g_i) \leq \text{DEG}(f)$, und da in f keine der Variablen $x_1, \ldots, x_m$ vorkommt, kommt wegen der Eigenschaft der

Ordnung auch in $a_i g_i$ keine der Variablen $x_1, \ldots, x_m$ vor. Es gilt also

$$f = \sum_{\substack{i=1 \\ a_i g_i \neq 0}}^{t} a_i g_i,$$

wobei alle in dieser Summe auftretenden a_i und g_i in $k[\boldsymbol{y}]$ liegen.

Für zumindest einen der Summanden muss $\text{DEG}(a_j g_j) = \text{DEG}(f)$ gelten. Dann gilt $\text{LT}(g_j) | \text{LT}(f)$ in $k[\boldsymbol{y}]$, und somit liegt $\text{LT}(f)$ in $\langle \text{LT}(G_{\boldsymbol{y}}) \rangle_{k[\boldsymbol{y}]}$. □

Wir geben hier eine erste Anwendung dieser Eigenschaft an: wir zeigen, wie wir die Generatoren des Schnitts zweier Ideale von $k[x_1, \ldots, x_n]$ berechnen.

SATZ 6.46 (Schnitt von Idealen). *Sei R ein kommutativer Ring mit Eins, und seien I, J Ideale von R. Seien (x) und $(x-1)$ die von x beziehungsweise $x-1$ erzeugten Hauptideale von $R[x]$. Dann gilt*

$$I \cap J = \{ r \in R \mid r\, x^0 \in I[x] \cdot (x) + J[x] \cdot (x-1) \}.$$

Beweis: Für $\subseteq$ sei $i \in I \cap J$. Es gilt dann $i\, x^0 = ix - i(x-1)$. Für $\supseteq$ sei $rx^0 = x \cdot \sum_{l=0}^{m} i_l x^l + (x-1) \cdot \sum_{l=0}^{n} j_l x^l$ mit $i_1, \ldots, i_m \in I$ und $j_1, \ldots, j_n \in J$. Wenn wir für $x := 0$ einsetzen, erhalten wir $r = -1 j_0$, also $r \in J$. Wenn wir für $x = 1$ einsetzen, so erhalten wir $r = \sum_{l=0}^{m} i_l$, also $r \in I$. □

KOROLLAR 6.47. *Sei k ein Körper, und seien I, J Ideale von $k[t_1, \ldots, t_n]$. Seien $a_1, \ldots, a_r, b_1, \ldots, b_s \in k[\boldsymbol{t}]$ so, dass $I = \langle a_1, \ldots, a_r \rangle_{k[\boldsymbol{t}]}$ und $J = \langle b_1, \ldots, b_s \rangle_{k[\boldsymbol{t}]}$. Sei $H := \langle a_1 y, \ldots, a_r y, b_1(y-1), \ldots, b_s(y-1) \rangle_{k[\boldsymbol{t}, y]}$. Dann gilt $H \cap k[\boldsymbol{t}] = I \cap J$.*

Beweis: Wir verwenden Satz 6.46 für $R := k[\boldsymbol{t}]$. □

8. Finden algebraischer Abhängigkeiten

Die folgenden Sätze bieten Möglichkeiten, zu bestimmen, ob gegebene Elemente eines Rings algebraisch abhängig sind. Als Vorbereitung beweisen wir folgendes Lemma:

LEMMA 6.48. *Sei k ein Körper, sei $\in \mathbb{N}$, sei R ein kommutativer Ring mit Eins mit $k \leq R$, und sei I ein Ideal von R. Sei $f \in k[t_1, \ldots, t_l]$, und seien $\boldsymbol{y}, \boldsymbol{z} \in R^l$ so, dass für alle $i \in \{1, \ldots, l\}$ gilt: $y_i - z_i \in I$. Dann gilt auch $\overline{f}(y_1, \ldots, y_l) - \overline{f}(z_1, \ldots, z_l) \in I$.*

Beweis: Offensichtlich erfüllt jedes konstante Polynom und jedes Polynom der Form $f = t_j$ diese Aussage. Wir zeigen nun, dass die Menge der Polynome, die diese Aussage erfüllen, abgeschlossen unter Addition und Multiplikation ist. Da man alle Polynome als Summen von Produkten von konstanten Polynomen und Variablen erhalten kann, beweist das das Lemma. Sei also $g = f_1 + f_2$. Dann gilt $g(\boldsymbol{y}) - g(\boldsymbol{z}) = f_1(\boldsymbol{y}) - f_1(\boldsymbol{z}) + f_2(\boldsymbol{y}) - f_2(\boldsymbol{z})$. Nach Voraussetzung liegen beide $f_i(\boldsymbol{y}) - f_i(\boldsymbol{z})$ in I. Wenn $g = f_1 \cdot f_2$, so gilt $g(\boldsymbol{y}) - g(\boldsymbol{z}) = f_1(\boldsymbol{y})f_2(\boldsymbol{y}) - f_1(\boldsymbol{z})f_2(\boldsymbol{z}) = f_1(\boldsymbol{y})f_2(\boldsymbol{y}) - f_1(\boldsymbol{y})f_2(\boldsymbol{z}) + f_1(\boldsymbol{y})f_2(\boldsymbol{z}) - f_1(\boldsymbol{z})f_2(\boldsymbol{z}) = f_1(\boldsymbol{y})(f_2(\boldsymbol{y}) - f_2(\boldsymbol{z})) + f_2(\boldsymbol{z})(f_1(\boldsymbol{y}) - f_1(\boldsymbol{z}))$. Beide Summanden liegen in I. □

SATZ 6.49 (Algebraische Abhängigkeit in $k[x_1, \ldots, x_n]/I$). *Sei k ein Körper, seien $r \in \mathbb{N}_0$, $n, s \in \mathbb{N}$, sei $I = \langle g_1, \ldots, g_r \rangle_{k[\boldsymbol{x}]}$, und seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Sei $p \in k[t_1, \ldots, t_s]$, und sei $J := \langle g_1, \ldots, g_r, t_1 - f_1, \ldots, t_s - f_s \rangle_{k[\boldsymbol{t},\boldsymbol{x}]}$. Dann sind äquivalent:*

(1) $p(f_1, \ldots, f_s) \in I$.
(2) $p \in J \cap k[t_1, \ldots, t_s]$.

Beweis: (1)⇒(2): Da für alle $i \in \{1, \ldots, s\}$ gilt: $f_1 \equiv t_1 \pmod{J}$, gilt wegen Lemma 6.48 auch

$$p(f_1, \ldots, f_s) \equiv p(t_1, \ldots, t_s) \pmod{J}.$$

Da $I \subseteq J$, gilt nach (1) auch $p(f_1, \ldots, f_s) \in J$, und somit $p(t_1, \ldots, t_s) \in J$. Da $p(t_1, \ldots, t_s)$ auch in $k[t_1, \ldots, t_s]$ liegt, gilt (2).

(2)⇒(1): Wenn $p \in J$, so gibt es Polynome $a_1, \ldots, a_r, b_1, \ldots, b_s \in k[\boldsymbol{t}, \boldsymbol{x}]$, sodass

$$p(\boldsymbol{t}) = \sum_{i=1}^{r} a_i(\boldsymbol{t}, \boldsymbol{x}) g_i(\boldsymbol{x}) + \sum_{i=1}^{s} b_i(\boldsymbol{t}, \boldsymbol{x})(t_i - f_i).$$

Diese Gleichheit gilt auch, wenn man für die Variable t_i das Polynom f_i einsetzt. Wir erhalten dann

$$p(f_1, \ldots, f_s) = \sum_{i=1}^{r} a_i(f_1, \ldots, f_s, \boldsymbol{x}) g_i(\boldsymbol{x}).$$

Daher gilt $p(f_1, \ldots, f_s) \in I$. □

KOROLLAR 6.50 (Algebraische Abhängigkeit in $k[x_1, \ldots, x_n]$). *Sei k ein Körper, seien $r \in \mathbb{N}_0$, $n, s \in \mathbb{N}$, und seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Sei $p \in k[t_1, \ldots, t_s]$, und sei $J := \langle t_1 - f_1, \ldots, t_s - f_s \rangle_{k[\boldsymbol{t},\boldsymbol{x}]}$. Dann sind äquivalent:*

(1) $p(f_1, \ldots, f_s) = 0$.
(2) $p \in J \cap k[t_1, \ldots, t_s]$.

SATZ 6.51 (Algebraische Abhängigkeit im Quotientenkörper). *Sei k ein Körper, und sei R ein Integritätsbereich mit $k \leq R$. Seien $f_1, \ldots, f_s \in R$, und seien $g_1, \ldots, g_s \in R \setminus \{0\}$. Sei $p \in k[t_1, \ldots, t_s]$, und sei*

$$J := \left\langle f_1 - t_1 g_1,\ \ldots,\ f_s - t_s g_s,\ y \prod_{i=1}^{s} g_i - 1 \right\rangle_{R[\boldsymbol{t}, y]}.$$

Dann sind äquivalent:

(1) $p(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}) = 0$. *Dabei wird im Quotientenkörper $Q(R)$ von R gerechnet.*
(2) $p \in J \cap k[t_1, \ldots, t_s]$.

Beweis: (1)⇒(2): Sei $m := \max\{\deg_{t_i}(p) \mid i \in \{1, \ldots, s\}\}$. Wir definieren ein Polynom $q \in k[a_1, \ldots, a_s, b_1, \ldots, b_s]$ durch

$$q(\boldsymbol{a}, \boldsymbol{b}) := \overline{p}(\frac{a_1}{b_1}, \ldots, \frac{a_s}{b_s}) \cdot (b_1 \cdots b_s)^m.$$

Wegen $p(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}) = 0$ gilt dann $\overline{q}(f_1, \ldots, f_s,\ g_1, \ldots, g_s) = p(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}) \cdot (g_1 \cdots g_s)^m = 0$. Da $q \in k[\boldsymbol{a}, \boldsymbol{b}]$, gilt wegen $t_i g_i \equiv f_i \pmod{J}$ auch

$$\overline{q}(t_1 g_1, \ldots, t_s g_s,\ g_1, \ldots, g_s) \in J.$$

Das bedeutet

$$p(t_1, \ldots, t_s) \cdot (g_1, \ldots, g_s)^m \in J.$$

Durch Multiplikation mit y^m erhalten wir

$$p(t_1, \ldots, t_s) \cdot (g_1, \ldots, g_s)^m \cdot y^m \in J.$$

Wegen Lemma 6.48 gilt $(g_1, \ldots, g_s)^m \cdot y^m - 1^m \in J$. Also gilt auch $p(t_1, \ldots, t_s) \cdot (g_1, \ldots, g_s)^m \cdot y^m - p(t_1, \ldots, t_s) \in J$. Insgesamt gilt also $p(t_1, \ldots, t_s) \in J$. Somit gilt $p \in J$.

(2)⇒(1): Seien $a_1, \ldots, a_s, b_1, \ldots, b_s \in R[\boldsymbol{t}, y]$ so, dass

$$p(\boldsymbol{t}) = \sum_{i=1}^{s} a_i(\boldsymbol{t}, y)(f_i - t_i g_i)) + \sum_{i=1}^{s} b_i(\boldsymbol{t}, y)(y \prod_{j=1}^{s} g_i - 1).$$

Diese gilt auch, wenn man in $Q(R)$ für $t_i := \frac{f_i}{g_i}$ und für $y_i := \frac{1}{g_1 \cdots g_s}$ einsetzt. Es gilt dann $p(\boldsymbol{t}) = 0$, also (1). □

KOROLLAR 6.52 (Algebraische Abhängigkeit in $k(x_1, \ldots, x_n)$). *Sei k ein Körper, seien $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, $g_1, \ldots, g_s \in k[x_1, \ldots, x_n] \backslash \{0\}$. Sei $p \in k[t_1, \ldots, t_s]$. Sei*

$$J := \left\langle f_1 - t_1 g_1, \ldots, f_s - t_s g_s, y \prod_{i=1}^{s} g_i - 1 \right\rangle_{k[\boldsymbol{t}, y, \boldsymbol{x}]}.$$

Dann sind äquivalent:

(1) $p(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}) = 0$. *Dabei wird im Körper der rationalen Funktionen, also in $Q(k[x_1, \ldots, x_n]) = k(x_1, \ldots, x_n)$ gerechnet.*
(2) $p \in J \cap k[t_1, \ldots, t_s]$.

Beweis: Wir verwenden Satz 6.51 für $R := k[x_1, \ldots, x_n]$. □

9. Zugehörigkeit zu Ring- und Körpererweiterungen

Wir werden uns in dieser Sektion überlegen, wie wir bestimmen können, ob eine rationale Funktion $\frac{a}{b} \in k(t_1, \ldots, t_n)$ in einer gegebenen Körpererweiterung $k(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s})$ liegt.

Zunächst beobachten wir, dass wir aus Satz 6.51 und dem Homomorphiesatz ein Ideal I von $k[x_1, \ldots, x_{s+1}]$ finden können, sodass $k[\![\frac{a}{b}, \frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}]\!]$ isomorph zu $k[x_1, \ldots, x_{s+1}]/I$ ist. Nun werden wir uns überlegen, wie wir im Restklassenring eines Polynomrings rechnen,

DEFINITION 6.53. Sei k ein Körper, seien $n \in \mathbb{N}$, $m \in \mathbb{N}_0$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Das Polynom $p = \sum_{i=0}^{m} p_i(x_2, \ldots, x_n) x_1^i \in k[x_1, \ldots, x_n]$ ist ein *kritisches Polynom für x_1 in I*, wenn

(1) $p \in I$, und
(2) es gibt $j \in \{0, \ldots, m\}$, sodass $p_j(x_2, \ldots, x_n) \notin I$.

DEFINITION 6.54. Sei k ein Körper, seien $n \in \mathbb{N}$, $m \in \mathbb{N}_0$, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Das Polynom $p = \sum_{i=0}^{m} p_i(x_2, \ldots, x_n) x_1^i \in k[x_1, \ldots, x_n]$ ist ist ein *kritisches Polynom minimalen Grades für x_1 in I*, wenn

(1) p ist kritisch für x_1 in I, und
(2) Für alle q, die kritisch für x_1 in I sind, gilt $\deg_{x_1}(q) \leq \deg_{x_1}(p)$.

Wenn es ein kritisches Polynom gibt, so finden wir ein kritisches Polynom minimalen Grades mithilfe der Berechnung einer Gröbnerbasis.

SATZ 6.55. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Wir nehmen an, dass es ein kritisches Polynom für x_1 in I gibt. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine Gröbnerbasis von I bezüglich $\leq$. Dann enthält G ein kritisches Polynom minimalen Grades für x_1 in I.*

Beweis: Sei f ein kritisches Polynom für x_1 in I, für das $\text{DEG}(f)$ minimal ist. Da $f \in I$, gilt $\text{LT}(f) \in \text{LT}(I)$. Also gibt es ein $g \in G$, sodass $\text{LT}(g)|\text{LT}(f)$. Sei $f_1 = f - \frac{\text{LT}(f)}{\text{LT}(g)} g$. Nun hat f_1 kleineren Multigrad als f. Wegen der Minimalität von f ist f_1 also nicht kritisch. Es gibt also $m \in \mathbb{N}_0$ und $a_0, \ldots, a_m \in I \cap k[x_2, \ldots, x_n]$, sodass $f_1 = \sum_{i=0}^m a_i(x_2, \ldots, x_n) x_1^i$.

Nehmen wir nun an, g ist nicht kritisch. Dann gibt es $l \in \mathbb{N}_0$ und $b_0, \ldots, b_l \in I \cap k[x_2, \ldots, x_n]$, sodass $g = \sum_{i=0}^l b_i(x_2, \ldots, x_n) x_1^i$. Dann lässt sich auch $\frac{\text{LT}(f)}{\text{LT}(g)} g$ als Summe $\sum_i c_i(x_2, \ldots, x_n) x_1^i$ schreiben, wobei alle $c_i \in I \cap k[x_2, \ldots, x_n]$ liegen. Dann ist $f = f_1 + \frac{\text{LT}(f)}{\text{LT}(g)} g$ nicht kritisch für x_1, im Widerspruch zur Wahl von f.

Also ist g kritisch. Wir zeigen nun, dass g ein kritisches Polynom minimalen Grades ist. Sei dazu p ein kritisches Polynom. Es gilt $\text{DEG}(g) \leq \text{DEG}(f)$ und $\text{DEG}(f) \leq \text{DEG}(p)$, insgesamt also $\text{DEG}(g) \leq \text{DEG}(p)$. Da die Monomordnung zuerst nach dem Grad in x_1 ordnet, gilt also $\deg_{x_1}(g) \leq \deg_{x_1}(p)$. □

Wir finden also in jeder Gröbnerbasis bezüglich einer geeigneten Monomordnung ein kritischen Polynoms von minimalem Grad in x_1.

LEMMA 6.56. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine Gröbnerbasis von I bezüglich $\leq$. Wenn G reduziert ist, so ist jedes Polynom in G mit $\deg_{x_1}(p) \geq 1$ kritisch für x_1 in I.*

Beweis: Sei $p = \sum_{i=0}^n p_i(x_2, \ldots, x_n) x_1^i \in G$ mit $n := \deg_{x_1}(p) \geq 1$.

Wenn $p_n \in I$, so gibt es ein $g \in G$ mit $\text{LT}(g)|\text{LT}(p_n)$. Wegen der Eigenschaft der Ordnung gilt $\text{LT}(p) = \text{LT}(p_n) \cdot x_1^n$. Also gilt $\text{LT}(g)|\text{LT}(p)$. Da G reduziert ist, gilt also $g = p$. Dann gilt aber $\deg_{x_1}(p) = 0$, im Widerpruch zu den Voraussetzungen an p.

Es gilt also $p_n \notin I$. Somit ist p kritisch für x_1 in I. □

DEFINITION 6.57. Seien A, B kommutative Ringe mit Eins, und sei $b \in B$. Wir nehmen an, dass b algebraisch über A ist. Ein *Minimalpolynom von b über A* ist ein Polynom p minimalen Grades in $A[t]$, das $p \neq 0$ und $\overline{p}(b) = 0$ erfüllt.

LEMMA 6.58. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $p = \sum_{i=1}^{m} p_i(x_2, \ldots, x_m)x_1^i \in k[x_1, \ldots, x_n]$. Äquivalent sind:*

(1) *$q(t) := \sum_{i=1}^{m} \overline{p_i}(x_2 + I, \ldots, x_n + I) \cdot t^i$ ist ein Minimalpolynom von $x_1 + I$ über $k[\![x_2 + I, \ldots, x_n + I]\!]$.*
(2) *p ist ein kritisches Polynom minimalen Grades für x_1 in I.*

Beweis: Sei $\Phi : k[x_1, \ldots, x_n] \to k[\![x_2 + I, \ldots, x_n + I]\!][t]$, $\Phi(\sum_{i=1}^{m} p_i(x_2, \ldots, x_n)x_1^i) := \sum_{i=1}^{m} \overline{p_i}(x_2 + I, \ldots, x_n + I)\, t^i$.

Zunächst gilt $p \in I$ genau dann, wenn $\overline{\Phi(p)}(x_1 + I) = 0$. Für $p \in I$ gilt $\Phi(p) = 0$ genau dann, wenn p nicht kritisch für x_1 in I ist.

Somit ist p genau dann ein kritisches Polynom minimalen Grades für x_1 in I, wenn $\Phi(p)$ ein Minimalpolynom für $x_1 + I$ über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist. □

Wir lösen nun als Anwendung dieser Sätze einige Beispiele.

BEISPIEL 6.59. Bestimmen Sie, ob x^3 im Unterkörper $\mathbb{Q}\big(x^2 + 2, x^5 + x + 1\big)$ liegt. Finden Sie gegebenenfalls Polynome $f_1, f_2 \in \mathbb{Q}[t_1, t_2]$, sodass $\frac{f_1(x^2+2, x^5+x+1)}{f_2(x^2+2, x^5+x+1)} = x^3$.

Lösung: Wir betrachten den Ring $R := k[\![x^3, x^2 + 2, x^5 + x + 1]\!]$. Sei

$$\begin{array}{rccl} \varphi & : & k[x_1, x_2, x_3] & \longrightarrow & k[x] \\ & & p & \longmapsto & p(x^3, x^2 + 2, x^5 + x + 2) \end{array}.$$

Die Abbildung φ ist ein Ringhomomorphismus mit $\varphi(x_1) = x^3$, $\varphi(x_2) = x^2 + 2$, und $\varphi(x_3) = x^5 + x + 2$. Den Kern dieser Abbildung kann man mithilfe von Korollar 6.50 finden. Wir berechnen dazu eine reduzierte Gröbnerbasis von

$$J = \big\langle x_1 - x^3, x_2 - (x^2 + 2), x_3 - (x^5 + x + 1) \big\rangle_{k[x, x_1, x_2, x_3]}$$

bezüglich der lexikographischen Ordnung mit $x > x_1 > x_2 > x_3$. Mathematica liefert diese Gröbnerbasis als

$$\begin{array}{l} x_2^5 - 10x_2^4 + 42x_2^3 - 92x_2^2 + 105x_2 - x_3^2 + 2x_3 - 51 \\ x_1x_3 - x_1 - x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20 \\ x_1x_2^2 - 4x_1x_2 + 5x_1 - x_2x_3 + x_2 + 2x_3 - 2 \\ x_1^2 - x_2^3 + 6x_2^2 - 12x_2 + 8 \\ x + x_1x_2 - 2x_1 - x_3 + 1 \end{array}$$

Das Ideal $I = J \cap k[x_1, x_2, x_3]$ wird also wegen der Eliminationseigenschaft, Satz 6.45, von den ersten 4 Polynomen dieser Basis erzeugt. Das Polynom

$$p = x_1x_3 - x_1 - x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20$$

ist aufgrund von Lemma 6.56 ein kritisches Polynom für x_1 in $J \cap k[x_1, x_2, x_3]$. Aufgrund von Satz 6.55 (oder weil p linear in x_1 ist), ist p auch kritisch minimalen Grades. Also ist wegen Lemma 6.58

$$(-x_2^4 + 8x_2^3 - 25x_2^2 + 36x_2 - 20 + I)\ t^0 + (x_3 - 1 + I)\ t$$

ein MinimalPolyom von $x_1 + I$ über $k[\![x_2 + I, x_3 + I]\!]$. Wenn wir das in den isomorphen Ring $k[\![x, x^2 + 2, x^5 + x + 1]\!]$ übertragen, so ist mit $y_2 := x^2 + 2$ und $y_3 := x^5 + x + 1$ das Polynom

$$(-y_2^4 + 8y_2^3 - 25y_2^2 + 36y_2 - 20)t^0 + (y_3 - 1)t$$

ein Minimalpolynom von x^3 über $k[\![x^2 + 2, x^5 + x + 1]\!] = k[\![y_2, y_3]\!]$. Es gilt also

$$x^3 = \frac{y_2^4 - 8y_2^3 + 25y_2^2 - 36y_2 + 20}{y_3 - 1}.$$

Also liegt x^3 in $k\big(x^2 + 2, x^5 + x + 1\big)$, und $r(t_1, t_2) := \frac{t_1^4 - 8t_1^3 + 25t_1^2 - 36t_1 + 20}{t_2 - 1}$ erfüllt $r(x^2 + 2, x^5 + x + 1) = x^3$. □

Mit diesen Sätzen haben wir also Algorithmen, für $a, f_1, \ldots, f_s \in k[\boldsymbol{x}]$ und $b, g_1, \ldots, g_s \in k[\boldsymbol{x}]$ folgende Fragen beantworten:

(1) Gilt $\frac{a}{b} \in k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$?
(2) Ist die Körpererweiterung $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)\big(\frac{a}{b}\big)$ algebraisch über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$?
(3) Wenn diese Körpererweiterung algebraisch ist, was ist ihr Grad?

Wir finden dazu mithilfe von Satz 6.51 ein Ideal I des Polynomrings $k[x_1, \ldots, x_{s+1}]$, sodass $k[x_1, \ldots, x_{s+1}]/I$ durch φ isomorph zu $k[\![\frac{a}{b}, \frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}]\!]$ ist, und $\varphi(x_1 + I) = \frac{a}{b}$, $\varphi(x_{i+1} + I) = \frac{f_i}{g_i}$ für $i \in \{1, \ldots, s\}$. Dann bestimmen wir ein Minimalpolynom für $x_1 + I$ über $k[\![x_2 + I, \ldots, x_{s+1} + I]\!]$, indem wir ein kritisches Polynom p minimalen Grades für x_1 in I bestimmen. Wenn es kein kritisches Polynom für x_1 in I gibt, ist $\frac{a}{b}$ nicht algebraisch über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$. Ansonsten erhalten wir aus p ein Minimalpolynom von $\frac{a}{b}$ über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$. Wenn $\deg_{x_1}(p) = 1$, so liegt $\frac{a}{b} \in k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$. Wenn $\deg_{x_1}(p) > 1$, so ist $\frac{a}{b}$ algebraisch über $k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)$, und $\deg_{x_1}(p)$ ist der Grad der Körpererweiterung $[k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)\big(\frac{a}{b}\big) : k\big(\frac{f_1}{g_1}, \ldots, \frac{f_s}{g_s}\big)]$.

Als letztes fragen wir uns noch, ob $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist, und, wenn ja, wie ein Polynom kleinsten Grades mit führendem Koeffizienten 1 aussieht, dass das belegt.

SATZ 6.60. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Wir nehmen an, dass $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist, und dass m der minimale Grad eines Polynoms mit führendem Koeffizienten 1 ist, das das belegt. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine Gröbnerbasis von I bezüglich $\leq$. Dann gibt es ein Polynom $g \in G$ mit $\mathrm{LM}(g) = x_1^m$.*

Beweis: Sei $f \in k[\![x_2 + I, \ldots, x_n + I]\!][t]$ ein Polynom minimalen Grades, das belegt, dass $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist. Wir schreiben f als $\sum_{i=0}^{m-1} \overline{f_i}(x_2 + I, \ldots, x_n + I)\, t^i + t^m$. Wegen $\overline{f}(x_1 + I) = 0$ liegt das Polynom $p = \sum_{i=0}^{m-1} f_i(x_2, \ldots, x_n)\, x_1^i$ in I.

Da G eine Gröbnerbasis ist, gibt ein $g \in G$, sodass $\mathrm{LT}(g) \mid \mathrm{LT}(p)$. Dann gibt es ein $m_1 \in \mathbb{N}_0$, sodass $\mathrm{LT}(g) = x_1^{m_1}$. Nun ist $g(t, x_2 + I, \ldots, x_n + I)$ ein Polynom vom Grad m_1, das belegt, dass $x_1 + I$ ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$ ist. Wegen der Minimalität von m gilt $m_1 = m$. □

Wir beobachten, dass wir in unseren Beispielen ein Ideal I immer so konstruiert haben, dass $k[x_1, \ldots, x_n]/I$ isomorph zu einem Integritätsbereich ist. In diesem Fall ist das Ideal I prim.

SATZ 6.61. *Sei k ein Körper, und sei I ein Ideal von $k[x_1, \ldots, x_n]$. Sei $\leq$ eine zulässige Ordnung der Monome, die $x_1^\alpha \geq x_2^{\beta_2} \cdots x_n^{\beta_n}$ für alle $\alpha \in \mathbb{N}$ und $\beta_2, \ldots, \beta_n \in \mathbb{N}_0$ erfüllt. Sei G eine reduzierte Gröbnerbasis von I bezüglich $\leq$. Dann gilt:*

(1) *$x_1 + I$ liegt genau dann in $k[\![x_2 + I, \ldots, x_n + I]\!]$, wenn G ein Polynom p mit $\mathrm{LM}(p) = x_1$ enthält.*
(2) *$x_1 + I$ ist genau dann ganz über $k[\![x_2 + I, \ldots, x_n + I]\!]$, wenn es ein $m \in \mathbb{N}$ gibt, sodass G ein Polynom p mit $\mathrm{LM}(p) = x_1^m$ enthält.*
(3) *$x_1 + I$ ist genau dann algebraisch über $k[\![x_2 + I, \ldots, x_n + I]\!]$, wenn G ein Polynom p mit $\deg_{x_1}(p) \neq 0$ enthält. Der Grad des Minimalpolynoms von $x_1 + I$ ist $\min\{\deg_{x_1}(p) \mid p \in G, \deg_{x_1}(p) \neq 0\}$.*
(4) *Wir nehmen an, dass I prim ist. Dann ist $k[\![x_1 + I, \ldots, x_n + I]\!]$ ein Integritätsbereich. Sei K sein Quotientenkörper. Dann liegt $x_1 + I$ genau*

dann in $k(x_2+I,\ldots,x_n+I)$*, wenn* G *ein Polynom* p *mit* $\deg_{x_1}(p)=1$ *enthält.*

Beweis: (1) Wenn $x_1+p_0(x_2,\ldots,x_n)\in I$, so gilt $x_1+I=-\overline{p_0}(x_2+I,\ldots,x_n+I)$, also $x_1+I\in k[\![x_2+I,\ldots,x_n+I]\!]$. Wenn $x_1+I\in k[\![x_2+I,\ldots,x_n+I]\!]$, so ist x_1+I ganz über $k[\![x_2+I,\ldots,x_n+I]\!]$, und $t-(x_1+I)$ ist ein Polynom vom Grad 1, das das belegt. Somit gibt es nach Satz 6.60 ein Polynom in G mit $\mathrm{LM}(g)=x_1$.

(2) Dieser Teil ergibt sich genauso aus Satz 6.60.

(3) Ergibt sich aus Satz 6.55, Lemma 6.56 und Lemma 6.58.

(4) Wir nehmen an, es gibt ein Polynom $r=q(x_2,\ldots,x_n)\,x_1+p(x_2,\ldots,x_n)$ mit $\deg_{x_1}(r)=1$, das in G liegt. Nach Lemma 6.56 ist dieses Polynom auch kritisch. Da $\overline{q}(x_2+I,\ldots,x_n+I)\neq 0+I$, gilt dann $x_1+I=\frac{\overline{p}(x_2+I,\ldots,x_n+I)}{\overline{q}(x_2+I,\ldots,x_n+I)}$. Wir nehmen nun an x_1+I liegt im Quotientenkörper. Dann ist x_1+I algebraisch über $k[\![x_2+I,\ldots,x_n+I]\!]$ mit einem Minimalpolynom vom Grad 1. Dann gibt es ein kritisches Polynom p mit $\deg_{x_1}(p)=1$ in I, und wegen Satz 6.55 auch in G. □

10. Existenz universeller Gröbnerbasen

Wir zeigen in dieser Sektion den folgenden Satz.

Satz 6.62. *Sei* k *ein Körper, sei* $n\in\mathbb{N}$*, und sei* I *ein Ideal von* $k[x_1,\ldots,x_n]$*. Dann gibt es eine endliche Teilmenge* G *von* $k[x_1,\ldots,x_n]$*, sodass* G *bezüglich jeder zulässigen Ordnung von* ${\mathbb{N}_0}^n$ *eine Gröbnerbasis ist.*

Dazu brauchen wir zunächst einen Satz über die Ordnungsfilter auf $\mathbb{N}_0^m$. Aus Satz 6.6 wissen wir bereits, dass es keine undendliche aufsteigende Kette $U_1\subset U_2\subset\cdots$ von Ordnungsfiltern auf ${\mathbb{N}_0}^m$ gibt. Wir zeigen nun, dass es auch keine unendlichen Antiketten von Ordnungsfiltern auf ${\mathbb{N}_0}^m$ gibt.

Satz 6.63 (cf. [**Mac01**, Theorem 1.2]). *Sei* $m\in\mathbb{N}$*, und sei* $\mathcal{L}$ *die Menge der Ordnungsfilter von* $\mathbb{N}_0^m$*. Dann hat* $(\mathcal{L},\subseteq)$ *keine unendliche Antikette.*

Beweis: Wenn $m=1$, so ist die Menge der Ordnungsfilter linear geordnet; Antiketten haben höchstens ein Element.

Sei nun $m \geq 2$. Für jedes Ordnungsfilter F of $\mathbb{N}_0^m$ definieren wir eine Funktion $\Phi_F : \mathbb{N}_0^{m-1} \to \mathbb{N}_0 \cup \{\infty\}$ durch

$$\Phi_F(\boldsymbol{a}) := \begin{cases} \min\{c \in \mathbb{N}_0 \mid (\boldsymbol{a}, c) \in F\} & \text{wenn es ein } c' \in \mathbb{N} \text{ mit } (\boldsymbol{a}, c') \in F \text{ gibt ,} \\ \infty & \text{sonst.} \end{cases}$$

für $\boldsymbol{a} \in \mathbb{N}_0^{m-1}$. Wir zeigen zuerst, dass für alle $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}_0^{m-1}$ mit $\boldsymbol{a} \leq \boldsymbol{b}$ auch $\Phi_F(\boldsymbol{a}) \geq \Phi_F(\boldsymbol{b})$ gilt. Sei dazu $c := \Phi_F(\boldsymbol{a})$. Wir nehmen an, dass $c \neq \infty$. Es gilt $(\boldsymbol{a}, c) \in F$. Da F ein Ordnungsfilter ist, gilt auch $(\boldsymbol{b}, c) \in F$, und folglich $\Phi_F(\boldsymbol{b}) \leq c = \Phi_F(\boldsymbol{a})$. Außerdem gilt für Ordnungsfilter F, G of $\mathbb{N}_0^m$ die Inklusion $F \subseteq G$ genau dann, wenn $\Phi_F(\boldsymbol{a}) \geq \Phi_G(\boldsymbol{a})$ für alle $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}_0^{m-1}$.

Sei nun $\langle F_i \mid i \in \mathbb{N} \rangle$ eine unendliche Antikette in $\mathcal{L}$. Für $i, j \in \mathbb{N}$ mit $i < j$ gilt daher $F_j \not\subseteq F_i$. Daher gibt es ein $\boldsymbol{a}^{(i,j)} \in \mathbb{N}_0^{m-1}$, sodass

$$\Phi_{F_j}(\boldsymbol{a}^{(i,j)}) < \Phi_{F_i}(\boldsymbol{a}^{(i,j)}).$$

Für $i, j, k \in \mathbb{N}$ mit $i < j < k$ färben wir nun die 3-elementige Menge $\{i, j, k\}$ mit einer von 2^{m-1} Farben. Als Farben wählen wir die Funktionen von $\{1, \ldots, m-1\}$ nach $\{\mathbf{1}, \mathbf{2}\}$. Für $l \in \{1, \ldots, m-1\}$ bezeichnen wir die l-te Komponente von $\boldsymbol{a}^{(i,j)}$ mit $\boldsymbol{a}_l^{(i,j)}$. Wir definieren jetzt die Farbe von $\{i, j, k\}$ durch

$$C(\{i, j, k\})(l) := \begin{cases} \mathbf{1} & \text{, wenn } \boldsymbol{a}_l^{(i,j)} \leq \boldsymbol{a}_l^{(j,k)}, \\ \mathbf{2} & \text{, wenn } \boldsymbol{a}_l^{(i,j)} > \boldsymbol{a}_l^{(j,k)}. \end{cases}$$

Nach dem Satz von Ramsey (Satz 6.1 hat $\mathbb{N}$ eine unendliche Teilmenge T, sodass alle 3-elementigen Teilmengen von T die gleiche Farbe C haben. Wir zeigen nun, dass $C(l) = \mathbf{1}$ für alle $l \in \{1, \ldots, m-1\}$ gilt.

Im Widerspruch dazu nehmen wir an, dass es ein l mit $C(l) = \mathbf{2}$ gibt. Seien $t_1 < t_2 < t_3 \ldots$ die Elemente von T. Wenn $C(l) = \mathbf{2}$, so gilt

$$\boldsymbol{a}_l^{(t_1,t_2)} > \boldsymbol{a}_l^{(t_2,t_3)} > \boldsymbol{a}_l^{(t_3,t_4)} > \cdots .$$

Damit haben wir eine unendliche absteigende Kette natürlicher Zahlen konstruiert, was unmöglich ist.

Es gilt also für alle $r \in \mathbb{N}$ die Ungleichung $\boldsymbol{a}^{(t_r,t_{r+1})} \leq \boldsymbol{a}^{(t_{r+1},t_{r+2})}$. Sei nun $r \in \mathbb{N}$. Wegen der Wahl von $\boldsymbol{a}^{(t_r,t_{r+1})}$ gilt nun

$$\Phi_{F_{t_r}}(\boldsymbol{a}^{(t_r,t_{r+1})}) > \Phi_{F_{t_{r+1}}}(\boldsymbol{a}^{(t_r,t_{r+1})}).$$

Da $\boldsymbol{a}^{(t_r,t_{r+1})} \leq \boldsymbol{a}^{(t_{r+1},t_{r+2})}$, gilt auch

$$\Phi_{F_{t_{r+1}}}(\boldsymbol{a}^{(t_r,t_{r+1})}) \geq \Phi_{F_{t_{r+1}}}(\boldsymbol{a}^{(t_{r+1},t_{r+2})}).$$

Damit ist die Folge $\langle \Phi_{F_{t_i}}(\boldsymbol{a}^{(t_i,t_{i+1})}) \mid i \in \mathbb{N}\rangle$ eine unendliche absteigende Kette $\mathbb{N}_0 \cup \{\infty\}$, was unmöglich ist.

Folglich kann es keine unendliche Antikette $\langle F_i \mid i \in \mathbb{N}\rangle$ von Ordnungsfiltern von $\mathbb{N}_0^m$ geben. □

KOROLLAR 6.64. *Sei k ein Körper. Dann besitzt die Menge der monomialen Ideale von $k[x_1, \ldots, x_n]$ keine unendliche Antikette.*

Beweis: Wir ordnen jedem monomialen Ideal I von $k[x_1, \ldots, x_n]$ das Ordnungsfilter $F(I) := \{\alpha \in {\mathbb{N}_0}^n \mid \boldsymbol{x}^\alpha \in I\}$ zu.

Für monomiale Ideale mit $F(I) \subseteq F(J)$ gilt auch auch $I \subseteq J$: Sei dazu $p \in I$. Wegen Lemma 6.19 liegt jedes Monom von p in I. Also liegt der Exponent jedes Monoms in $F(I)$. Wegen $F(I) \subseteq F(J)$ liegt der Exponent eines jeden Monoms von p auch in $F(J)$. Also liegt jedes Monom von p in J, also gilt auch $p \in J$.

Aufgrund dieser Eigenschaft ist F injektiv. Einer unendlichen Antikette in $k[x_1, \ldots, x_n]$ wird also durch F eine unendliche Antikette von Ordnungsfiltern auf ${\mathbb{N}_0}^n$ zugeordnet. Eine solche unendliche Antikette gibt es aber wegen Satz 6.63 nicht. □

Beweis von Satz 6.62: Wir bilden für jede zulässige Ordnung $\leq$ auf ${\mathbb{N}_0}^n$ die Menge

$$F(\leq) := \langle \mathrm{LT}_{\leq}(I)\rangle_{k[\boldsymbol{x}]}\,.$$

Die Menge

$$\mathcal{F} = \{F(\leq) \mid \leq \text{ ist zulässig }\}$$

ist eine Menge von monomialen Idealen. Sei $\mathcal{F}_{\max}$ die Menge der maximalen Elemente von $\mathcal{F}$. Wegen Korollar 6.64 ist $\mathcal{F}_{\max}$ endlich.

Seien nun $\leq_1, \ldots, \leq_m$ zulässige Ordnungen, sodass $\mathcal{F}_{\max} = \{F(\leq_1), \ldots, F(\leq_m)\}$. Nach Satz 6.42 besitzt I nun bezüglich jeder dieser Ordnungen $\leq_i$ eine reduzierte Gröbnerbasis G_i. Sei nun $G = G_1 \cup \ldots \cup G_m$.

Es bleibt zu zeigen, dass G bezüglich jeder zulässigen Ordnung auf ${\mathbb{N}_0}^n$ eine Gröbnerbasis von I ist. Sei also $\leq$ eine zulässige Ordnung. Wir zeigen, dass für alle $f \in I$ mit $f \neq 0$ gilt, dass $\mathrm{LT}_{\leq}(f)$ in $\langle \mathrm{LT}(G)\rangle_{k[\boldsymbol{x}]}$ liegt. Sei also $f\ in I$. Da $\mathcal{F}$ die (ACC) erfüllt, ist $F(\leq)$ in einem maximalen Element von $\mathcal{F}$ als Teilmenge enthalten. Es gibt also ein $i \in \{1, \ldots, m\}$, sodass $F(\leq) \subseteq F(\leq_i)$ Klarerweise gilt $\mathrm{LT}_{\leq}(f) \in \mathrm{LT}_{\leq}(I)$, also auch $\mathrm{LT}_{\leq}(f) \in \langle \mathrm{LT}_{\leq}(I)\rangle_{k[\boldsymbol{x}]}$. Da $\langle \mathrm{LT}_{\leq}(I)\rangle_{k[\boldsymbol{x}]} \subseteq$

$\langle \mathrm{LT}_{\leq_i}(I)\rangle_{k[\boldsymbol{x}]}$, gilt $\mathrm{LT}_{\leq}(f) \in \langle \mathrm{LT}_{\leq_i}(I)\rangle_{k[\boldsymbol{x}]}$. Nun ist G_i eine Gröbnerbasis bezüglich $\leq_i$. Somit liegt $\mathrm{LT}_{\leq}(f)$ in $\langle \mathrm{LT}_{\leq_i}(G_i)\rangle_{k[\boldsymbol{x}]}$. Es gibt also ein $g \in G_i$, sodass

$$\mathrm{LT}_{\leq_i}(g) | \mathrm{LT}_{\leq}(f).$$

Wir betrachten nun $\mathrm{LT}_{\leq}(g)$. Da $g \in I$, gilt $\mathrm{LT}_{\leq}(g) \in \mathrm{LT}_{\leq}(I)$. Da $\langle \mathrm{LT}_{\leq}(I)\rangle_{k[\boldsymbol{x}]} \subseteq \langle \mathrm{LT}_{\leq_i}(I)\rangle_{k[\boldsymbol{x}]}$, gilt somit auch

$$\mathrm{LT}_{\leq}(g) \in \langle \mathrm{LT}_{\leq_i}(I)\rangle.$$

Da G_i eine Gröbnerbasis von I bezüglich $\leq_i$ ist, gibt es ein $h \in G_i$, sodass $\mathrm{LT}_{\leq_i}(h) | \mathrm{LT}_{\leq}(g)$. Nun ist G_i eine reduzierte Gröbnerbasis. Daher ist kein Monom in g durch ein $\mathrm{LT}_{\leq_i}(g')$ mit $g' \in G_i \setminus \{g\}$ teilbar. Also gilt $g = h$. Dann gilt aber $\mathrm{LT}_{\leq_i}(g) | \mathrm{LT}_{\leq}(g)$. Da $\mathrm{LT}_{\leq_i}(g)$ maximal bezüglich Teilbarkeit unter den in g auftretenden Monomen ist, gilt $\mathrm{LT}_{\leq_i}(g) = \mathrm{LT}_{\leq}(g)$. Also gilt auch $\mathrm{LT}_{\leq}(g) | \mathrm{LT}_{\leq}(f)$, und somit $\mathrm{LT}_{\leq}(f) \in \langle \mathrm{LT}_{\leq}(G)\rangle_{k[\boldsymbol{x}]}$. □

Literaturverzeichnis

[Buc70] B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.

[Dic13] L. E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, American Journal of Mathematics **35** (1913), no. 4, 413–422.

[Hal76] P. R. Halmos, *Naive Mengenlehre*, Vandenhoeck & Ruprecht, Göttingen, 1976, Vierte Auflage, Aus dem Englischen übersetzt von Manfred Armbrust und Fritz Ostermann, Moderne Mathematik in elementarer Darstellung, No. 6.

[Mac01] D. Maclagan, *Antichains of monomial ideals are finite*, Proc. Amer. Math. Soc. **129** (2001), no. 6, 1609–1615 (electronic).

[Ram29] F. P. Ramsey, *On a problem of formal logic*, Proceedings London Mathematical Society (2) **30** (1929), 264–286.

[vdW67] B. L. van der Waerden, *Algebra. Teil II*, Unter Benutzung von Vorlesungen von E. Artin und E. Noether. Fünfte Auflage. Heidelberger Taschenbücher, Band 23, Springer-Verlag, Berlin, 1967.