Der Divisionsalgorithmus

Alexandre Wolf

Seminar: Computeralgebra

Fachbereich Mathematik der Universität Dortmund

Dortmund, November 2006

Inhaltsverzeichnis

Einleitung

Ziel dieses Vortrags ist es, einen Algorithmus für die Division von Polynomen in mehreren Veränderlichen zu konstruieren.
Zu Beginn werden gewisse Eigenschaften dieser Division anhand von konkreten Beispielen aufgezeigt. Darauf aufbauend wird dann der Algorithmus formuliert und bewiesen, anschließend an einem Beispiel ausgeführt.
Mit einer wichtigen Definition für den Buchberger Algorithmus schließt der Abschnitt ab.

1 Einführende Beispiele

Beispiel 1.1

Zunächst betrachten wir über dem Körper $\mathbb{Q}$ *und dem Polynomring* $P = \mathbb{Q}[x]$ *die Polynome*

$$\begin{aligned} & f(x) &:=& \ x^3 + 2x^2 + x + 1 \\ \textit{und} \quad & g(x) &:=& \ 2x + 1 \end{aligned}$$

Division mit Rest liefert

$$
\begin{array}{rcl}
(x^3+2x^2+x+1):(2x+1) & = & \frac{1}{2}x^2+\frac{3}{4}x+\frac{1}{8} \quad Rest \quad \frac{7}{8} \\
\underline{-(x^3+\frac{1}{2}x^2)} & & \\
\frac{3}{2}x^2+x & & \\
\underline{-(\frac{3}{2}x^2+\frac{3}{4}x)} & & \\
\frac{1}{4}x+1 & & \\
\underline{-(\frac{1}{4}x+\frac{1}{8})} & & \\
\frac{7}{8} & &
\end{array}
$$

Man erhält also eine eindeutige Darstellung

$$
\begin{array}{rrcl}
 & f & = & qg+p \\
mit & q(x) & := & \frac{1}{2}x^2+\frac{3}{4}x+\frac{1}{8} \\
 & p(x) & := & \frac{7}{8}
\end{array}
$$

Offenbar gilt : $deg(p) = 0 \ < \ 1 = deg(g)$.

Beispiel 1.2

(*i*) *Über dem Polynomring* $\mathbb{Q}[x_1, x_2]$ *seien folgende Polynome definiert*

$$
\begin{array}{rcl}
f(x_1,x_2) & := & x_1^2x_2+x_1x_2^2+x_2^2 \\
g_1(x_1,x_2) & := & x_1x_2-1 \\
g_2(x_1,x_2) & := & x_2^2-1
\end{array}
$$

Ziel: *finde eine Darstellung der Form* $f = q_1g_1+q_2g_2+p$ *,wobei* q_1, q_2 *und* p *mit* $deg(p) < 2$ *Polynome sind. Dazu werden die in den jeweiligen Einzelschritten auftretenden lexikographischen Leitterme von* f *nacheinander soweit wie möglich mittels* g_1 *und* g_2 *eliminiert.*

Zunächst ergibt die Division mit g_1 *:*

$$
\begin{array}{rcl}
(x_1^2x_2+x_1x_2^2+x_2^2):(x_1x_2-1) & = & x_1+x_2 \quad Rest \quad x_1+x_2^2+x_2 \\
\underline{-(x_1^2x_2-x_1)} & & \\
x_1x_2^2+x_1+x_2^2 & & \\
\underline{-(x_1x_2^2-x_2)} & & \\
x_1+x_2^2+x_2 & &
\end{array}
$$

dann die Division des Restes durch g_2 *:*

$$
\begin{array}{rcl}
(x_1+x_2^2+x_2):(x_2^2-1) & = & 1 \quad Rest \quad x_1+x_2+1 \\
\underline{-(x_2^2-1)} & & \\
x_1+x_2+1 & &
\end{array}
$$

Dies erbringt die erwünschte Darstellung :

$$\begin{aligned} & & f &= q_1 g_1 + q_2 g_2 + p \\ \textit{mit} & & q_1(x_1, x_2) &:= x_1 + x_2 \\ & & q_2(x_1, x_2) &:= 1 \\ & & p(x_1, x_2) &:= x_1 + x_2 + 1 \end{aligned}$$

Dabei gilt erneut: $\quad deg(p) = 1 \ < \ 2 = deg(g_1) = deg(g_2)$.

(*ii*) *Ändert man die Reihenfolge der Divisionsschritte, so bekommt man zunächst wieder bei Division durch* g_1 *:*

$$\begin{array}{rl} (x_1^2 x_2 + x_1 x_2^2 + x_2^2) : (x_1 x_2 - 1) & = \ x_1 \quad Rest \quad x_1 x_2^2 + x_1 + x_2^2 \\ \underline{-(x_1^2 x_2 - x_1)} & \\ x_1 x_2^2 + x_1 + x_2^2 & \end{array}$$

Division des Restes durch g_2 *:*

$$\begin{array}{rl} (x_1 x_2^2 + x_1 + x_2^2) : (x_2^2 - 1) & = \ x_1 + 1 \quad Rest \quad 2x_1 + 1 \\ \underline{-(x_1 x_2^2 - x_1)} & \\ 2x_1 + x_2^2 & \\ \underline{-(-1 + x_2^2)} & \\ 2x_1 + 1 & \end{array}$$

Es entsteht also eine alternative Darstellung der Form:

$$\begin{aligned} & & f &= \tilde{q}_1 g_1 + \tilde{q}_2 g_2 + \tilde{p} \\ \textit{mit} & & \tilde{q}_1(x_1, x_2) &:= x_1 \\ & & \tilde{q}_2(x_1, x_2) &:= x_1 + 1 \\ & & \tilde{p}(x_1, x_2) &:= 2x_1 + 1 \end{aligned}$$

Auch hier gilt: $\quad deg(\tilde{p}) = 1 \ < \ 2 = deg(g_1) = deg(g_2)$.

Die Polynomdivision in mehreren Veränderlichen ist also nicht eindeutig bestimmt. Desweiteren bleibt festzustellen, dass der Grad des Restpolynoms p *stets kleiner als derjenige der einzelnen Divisoren* g_1 *und* g_2 *ist.*

Die Division von Polynomen in mehreren Unbestimmten aus Beispiel 1.2 *wird nun verallgemeinert.*

2 Divisionsalgorithmus

Theorem 2.1

Es seien $s \in \mathbb{N}$, $P = K[x_1, ..., x_n]$ *ein Polynomring in n Unbestimmten,* m, $g_j \in P^r \setminus \{0\}$ *für* $j \in \mathbb{N}_s := \{1, ..., s\}$ *und* σ *eine Modultermordnung auf* $\mathbb{T}^n\langle e_1, ..., e_r\rangle$. *Die Polynomdivision in mehreren Veränderlichen gelingt wie folgt:*

(*i*) *Seien* $q_j = 0$, $p = 0$ $(= 0_r)$ *und* $v = m$.

(*ii*) *Finde kleinstes* $j \in \mathbb{N}_s$, *so dass* $LT_\sigma(v)$ *ein Vielfaches von* $LT_\sigma(g_j)$ *ist.*
Existiert ein solches j, *dann ersetze* q_j *durch* $q_j + \frac{LM_\sigma(v)}{LM_\sigma(g_j)}$ *und*
v *durch* $v - \frac{LM_\sigma(v)}{LM_\sigma(g_j)} g_j$.

(*iii*) *Wiederhole Schritt* (*ii*) *solange, bis es kein derartiges* j *mehr gibt.*
Dann ersetze das Restpolynom p *durch* $p + LM_\sigma(v)$ *und* v *durch* $v - LM_\sigma(v)$.

(*iv*) *Gilt* $v \neq 0$, *dann starte wieder mit Schritt* (*ii*).
Falls $v = 0$ *ist , so gib die Vektoren* $(q_1, ..., q_s) \in P^s$ *und* $p \in P^r$ *aus, die der Gleichung*

$$m \;=\; \sum_{j=1}^{s} q_j g_j + p$$

genügen, so dass folgende Eigenschaften erfüllt sind:

(*a*) *Für alle* $t \in supp(p)$ *gilt :* $\quad t \notin \langle LT_\sigma(g_1), ..., LT_\sigma(g_s)\rangle$.

(*b*) *Ist* $q_j \neq 0$ *für* $j \in \mathbb{N}_s$, *dann gilt:* $\quad LT_\sigma(q_j g_j) \leq_\sigma LT_\sigma(m)$.

(*c*) *Für alle* $j \in \mathbb{N}_s$ *und alle Terme* $t \in supp(q_j)$ *gilt:*

$$t \cdot LT_\sigma(g_j) \notin \langle LT_\sigma(g_1), ..., LT_\sigma(g_{j-1})\rangle.$$

Erfüllen $(q_1, ..., q_s) \in P^s$ *und* $p \in P^r$ *die Bedingungen* (*a*), (*b*) *und* (*c*) , *so sind sie durch die Vektoren* m, $g_j \in P^r$ *eindeutig bestimmt.*

Beweis:
In den Schritten (i) bis (iv) gilt stets die Gleichung

$$m = \sum_{j=1}^{s} q_j g_j + p + v \qquad\qquad (*)\ .$$

Sind die entsprechenden Größen in $(*)$ gemäß (i) null, so folgt direkt $v = m$.
In den beiden darauffolgenden Schritten wird lediglich eine Ergänzung vorgenommen, denn man hat

$$q_j g_j + v = (q_j + \tfrac{LM_\sigma(v)}{LM_\sigma(g_j)}) g_j + (v - \tfrac{LM_\sigma(v)}{LM_\sigma(g_j)} g_j)$$

sowie

$$p + v = (p + LM_\sigma(v)) + (v - LM_\sigma(v))\ .$$

Für $v = 0$ ergibt sich die in (iv) angezeigte Form von m.

Bei Anwendung von Schritt (ii) und (iii) wird der Leitterm von v stets kleiner. In (ii) wird durch das Vielfache von g_j das Leitmonom von v eliminiert, was in (iii) offensichtlich auch der Fall ist. Da σ als Modultermordnung auch eine Wohlordnung darstellt, muss es nach Theorem $A.1$ (siehe Anhang) einen kleinsten Leitterm von v geben. Für diesen gilt $v = 0$. Mit (iv) bricht dann der Algorithmus ab.
Wegen $v = m$ zu Beginn des Algorithmus und aufgrund der Monotonie gilt in jedem Schritt

$$LT_\sigma(v) \;\leq\; LT_\sigma(m)\,.$$

Nach Beendigung des Algorithmus bekommt man die Darstellung:

$$m = \sum_{j=1}^{s} q_j g_j + p\ .$$

p genügt Eigenschaft (a), da nach Schritt (iii) nur dann ein skalares Vielfaches eines Terms p hinzugefügt wird, falls dieser kein Vielfaches der Leitterme der g_j ist.
Nun wird mit Induktion nach der Anzahl der durchgeführten Schritte Eigenschaft (b) nachgewiesen.
Induktionsanfang: da in Schritt (i) stets $q_j = 0$ gilt, gibt es nichts zu zeigen.
Induktionsvoraussetzung:

$$LT_\sigma(q_j g_j) \;\leq\; LT_\sigma(m) \qquad \text{für} \quad q_j \neq 0 \quad .$$

Induktionsschritt: unter der Voraussetzung, dass der alte und neue Wert von q_j nicht trivial sind, gelten bei Anwendung von Schritt (ii) immer die Ungleichungen:

$$\begin{aligned} LT_\sigma((q_j + \tfrac{LM_\sigma(v)}{LM_\sigma(g_j)})g_j) \;&\leq_\sigma\; max_\sigma\{LT_\sigma(q_j g_j), LT_\sigma(v)\} \\ &\leq_\sigma\; LT_\sigma(m) \quad . \end{aligned}$$

Der Beweis dazu erfolgt mit Satz $A.1$ (i) (siehe Anhang), so dass

$$LT_\sigma(q_j g_j + \tfrac{LM_\sigma(v)}{LM_\sigma(g_j)}\, g_j) \;\leq_\sigma\; \max_\sigma\{LT_\sigma(q_j g_j), LT_\sigma(\tfrac{LM_\sigma(v)}{LM_\sigma(g_j)}\, g_j)\} \quad .$$

Desweiteren gilt mit:

$$\begin{aligned} v \;&=\; \sum_{i=1}^{m} c_i t_i e_{\gamma_i} \qquad \text{mit} \quad t_1 e_{\gamma_1} >_\sigma \ldots >_\sigma t_m e_{\gamma_m} \\ g_j \;&=\; \sum_{i=1}^{l} \tilde{c}_i \tilde{t}_i e_{\delta_i} \qquad \text{mit} \quad \tilde{t}_1 e_{\delta_1} >_\sigma \ldots >_\sigma \tilde{t}_l e_{\delta_l} \end{aligned}$$

$$\begin{aligned} \tfrac{LM_\sigma(v)}{LM_\sigma(g_j)}\, g_j \;&=\; \tfrac{c_1 t_1 e_{\gamma_1}}{\tilde{c}_1 \tilde{t}_1 e_{\gamma_1}}\, g_j \\ &=\; \tfrac{c_1 t_1 e_{\gamma_1}}{\tilde{c}_1 \tilde{t}_1 e_{\gamma_1}}\, (\tilde{c}_1 \tilde{t}_1 e_{\gamma_1} + \tilde{c}_2 \tilde{t}_2 e_{\delta_2} + (Rest)\,) \\ &=\; c_1 t_1 e_{\gamma_1} + \,(Rest) \quad . \end{aligned}$$

Also

$$LT_\sigma(\tfrac{LM_\sigma(v)}{LM_\sigma(g_j)}\, g_j) \;=\; LT_\sigma(v)$$

und damit auch

$$\begin{aligned} max_\sigma\{LT_\sigma(q_j g_j), LT_\sigma(\tfrac{LM_\sigma(v)}{LM_\sigma(g_j)}\, g_j)\} &= max_\sigma\{LT_\sigma(q_j g_j), LT_\sigma(v)\} \\ &\leq_\sigma LT_\sigma(m) \quad . \end{aligned}$$

Die letzte Abschätzung beruht auf der Induktionsannahme.

In Schritt (ii) wird immer das minimale $j \in \mathbb{N}_s$ bestimmt, für das gilt:

$$LT_\sigma(v) = t \cdot LT_\sigma(g_j) \quad \text{für } t \in \mathbb{T}^n\langle e_1, ..., e_r\rangle.$$

Annahme, es gäbe eine Darstellung $\quad t \cdot LT_\sigma(g_j) = \sum_{k=1}^{j-1} s_k \cdot LT_\sigma(g_k).$

Dies ist nach Schritt (ii) aber nicht möglich, da gerade dieses j minimal ist, so dass $LT_\sigma(v)$ sich als Vielfaches von $LT_\sigma(g_j)$ ausdrücken lässt. Die rechte Seite der Gleichung, nach der es ein kleinstes $\tilde{j} \in \{1, ..., j-1\}$ geben würde, widerspricht also der Minimalität von j.
Demnach kann $t \cdot LT_\sigma(g_j)$ nicht im Erzeugnis der Terme $LT_\sigma(g_1), ..., LT_\sigma(g_{j-1})$ liegen.

Eindeutigkeit: Annahme, es gäbe zwei Darstellungen für m gegeben durch:

$$m \;=\; \sum_{j=1}^{s} q_j g_j + p \;=\; \sum_{j=1}^{s} \tilde{q}_j g_j + \tilde{p}\ ,$$

so dass die Bedingungen (a), (b) und (c) erfüllt sind. Die Differenz beider Gleichungen liefert:

$$\tilde{p} - p \;=\; \sum_{j=1}^{s} (q_j - \tilde{q}_j) g_j \qquad\qquad (\bullet).$$

Nach (a) gilt $\quad LT_\sigma(\tilde{p} - p) \;\notin\; \langle LT_\sigma(g_1), ..., LT_\sigma(g_s)\rangle$ für $p \neq \tilde{p}$, da offensichtlich $LT_\sigma(\tilde{p} - p) \in supp(p)$ gilt.

Ferner folgt mit (c) sowie Satz $A.1$ (iii) (siehe Anhang) für $q_j \neq \tilde{q}_j$:

$$LT_\sigma((q_j - \tilde{q}_j) g_j) \;=\; LT_\sigma(q_j - \tilde{q}_j) \cdot LT_\sigma(g_j) \;\notin\; \langle LT_\sigma(g_1), ..., LT_\sigma(g_{j-1})\rangle.$$

Also sind die Leitterme $LT_\sigma((q_j - \tilde{q}_j) g_j)$ in $(\bullet)$ paarweise verschieden.

Wegen Satz $A.1$ (ii) (siehe Anhang) folgt wegen

$$LT_\sigma(\tilde{p} - p) \;=\; \underbrace{max_\sigma\{LT_\sigma((q_j - \tilde{q}_j) g_j)\}}_{\in\, \langle LT_\sigma(g_1), ..., LT_\sigma(g_s)\rangle}$$

der Widerspruch zu (a) und damit zunächst

$$q_j - \tilde{q}_j \;=\; 0$$

und dann auch

$$\tilde{p} - p \;=\; 0.$$

Es kann aber dennoch $q_j - \tilde{q}_j$ geben, die ungleich null sind. In diesem Fall bringt man das maximale $q_j - \tilde{q}_j \neq 0$ auf die linke Seite von Gleichung $(\bullet)$ und vollzieht für dieses analog die vorangegangene Beweiskette. $\square$

Beispiel 2.1

Es seien $n = 2$, $r = 1$ *und* $P = \mathbb{Q}[x_1, x_2]$.
Betrachte das Polynom $m = x_1x_2^2 - x_1$ *sowie die Divisoren* $g_1 = x_1x_2 + 1$ *und* $g_2 = x_2^2 - 1$.
Ferner lege die lexikographische Termordnung zugrunde, d. h. $\sigma = Lex$ *(siehe Anhang Definition A.4).*

Das kleinste $j \in \{1, 2\}$, *für das* $LT_\sigma(m) = LT_\sigma(v)$ *ein Vielfaches von* $LT_\sigma(g_j)$ *bildet, ist* $j = 1$, *denn*

$$LT_\sigma(m) = x_1x_2^2 = x_2LT_\sigma(g_1) .$$

Man hat dann

$$q_1 = \frac{LM_\sigma(v)}{LM_\sigma(g_1)} = \frac{x_1x_2^2}{x_1x_2} = x_2$$

und

$$v = x_1x_2^2 - x_1 - x_2g_1 = x_1x_2^2 - x_1 - x_1x_2^2 - x_2 = -x_1 - x_2 \neq 0 .$$

Es gibt kein weiteres j *, d. h.* $q_2 = 0$ *, und weiter* $p = -x_1$
sowie $v = -x_1 - x_2 - (-x_1) = -x_2$.

Da $v \neq 0$ *und erneute Anwendung von* (ii) *nicht möglich ist, befolge wieder Schritt* (iii) *, so dass dann* $p = -x_1 - x_2$ *und* $v = -x_2 - (-x_2) = 0$.
Man bekommt also

$$m = q_1g_1 + q_2g_2 + p .$$

Offensichtlich ist $m = x_1g_2$ *im Ideal* $\langle g_1, g_2\rangle \subseteq P$ *enthalten und somit Element des Untermoduls* $\langle g_1, g_2\rangle$.

Bemerkung 2.1

Mit dem Divisionsalgorithmus kann die Restklasse eines Elements m *modulo dem Untermodul, das durch* $\{g_1, ..., g_s\}$ *erzeugt wird, als Linearkombination von Termen geschrieben werden, die kein Vielfaches von* $LT_\sigma(g_1), ..., LT_\sigma(g_s)$ *sind.*

Beispiel 2.2

In Beispiel 1.2 (i) *und* (ii) *gibt es keine eindeutige Zerlegung von* f *:*

$$\begin{aligned} f &= (x_1 + x_2)g_1 + g_2 + (x_1 + x_2 + 1) \\ &= x_1 g_1 + (x_1 + 1)g_2 + (2x_1 + 1) \quad . \end{aligned}$$

Es ist

$$\begin{aligned} x_1 - x_2 &= (2x_1 + 1) - (x_1 + x_2 + 1) \\ &= x_2(x_1 x_2 - 1) - x_1(x_2^2 - 1) \end{aligned}$$

ein Element des Ideals $\langle g_1, g_2 \rangle \subseteq \mathbb{Q}[x_1, x_2]$.
Demzufolge haben x_1 *und* x_2 *dieselbe Restklasse in* $P/\langle g_1, g_2 \rangle$.

Definition 2.1

Es seien $s \in \mathbb{N}$, m, $g_1, ..., g_s \in P^r \setminus \{0\}$ *und* $\mathcal{G} := (g_1, ..., g_s)$. *Anwendung des Divisionsalgorithmus liefert*

$$m = \sum_{j=1}^{s} q_j g_j + p \quad , \; q_j \in P, \; p \in P^r \; .$$

Dann heißt p *der* ***normale Rest*** *von* m *bezüglich* $\mathcal{G}$.
Notation: $NR_{\sigma,\mathcal{G}}(m) := p$, *kurz* $NR_{\mathcal{G}}(m)$.
Im Fall $m = 0$ *setzt man* $NR_{\mathcal{G}}(m) = 0$.

Ausblick

A Anhang

Definition A.1

(a) *Ein Tripel* $(R, +, \cdot)$ *bestehend aus einer Menge* R *und zwei Operationen*

$$\begin{aligned} + &: R \times R \longrightarrow R \quad mit \quad (a,b) \longmapsto a+b \\ \cdot &: R \times R \longrightarrow R \quad mit \quad (a,b) \longmapsto a \cdot b \end{aligned}$$

heißt ***Ring*** *, falls gilt:*

(i) $(R, +)$ *ist eine abelsche Gruppe.*

(ii) *Die Operation* $\cdot$ *ist assoziativ.*

(iii) *Es gelten die Distributivgesetze.*

(b) *Ist die Operation* $\cdot$ *kommutativ und existiert für letztere ein neutrales Element (Einselement), so wird* $(R, +, \cdot)$ *ein* ***kommutativer Ring mit Eins*** *genannt.*

(In der zugrundeliegenden Ausarbeitung sprechen wir der Kürze wegen von einem Ring.)

Definition A.2

(i) *Die Menge aller Polynome in einer Veränderlichen über* R *wird mit* $R[x]$ *bezeichnet.*

Jedes Element von $R[x]$ *hat eine eindeutige Darstellung der Form*

$$p(x) = \sum_{j \in \mathbb{N}_0} r_j x_j \qquad , r_j \in R \,,\, r_j \neq 0 \text{ nur für endlich viele Indizes } j.$$

(ii) *Allgemein definiert man durch* $R[x_1, ..., x_n]$ *die Menge aller Polynome in* n *Unbestimmten über* R.

Definition A.3

(i) *Ein Element* $t \in R[x_1, ..., x_n]$ *der Form* $t = \prod_{j=1}^{n} x_j^{\alpha_j}$ *mit* $\alpha_j \in \mathbb{N}_0$ *heißt* ***Term*** *oder auch* ***Potenzprodukt****.*

(ii) *Die Menge aller Terme sei* $\mathbb{T}^n := \mathbb{T}(x_1, ..., x_n)$.

(iii) *Der* ***Grad*** *von* $t \in \mathbb{T}^n$ *ist gegeben durch* $deg(t) := \sum_{j=1}^{n} \alpha_j$.

(iv) *Die durch* $\prod_{j=1}^{n} x_j^{\alpha_j} \mapsto (\alpha_1, ..., \alpha_n)$ *definierte Abbildung* $log : \mathbb{T}^n \to \mathbb{N}_0^n$ *heißt der* ***Logarithmus****.*

Definition A.4

Für $t_1, t_2 \in \mathbb{T}^n$ *gilt* $t_1 \geq_{Lex} t_2$ *genau dann, wenn die erste nichttriviale Komponente von* $log(t_1) - log(t_2)$ *positiv ist oder* $t_1 = t_2$ *gilt.*
Die Termordnung ***Lex*** *wird* ***lexikographische Termordnung*** *genannt.*

Definition A.5

Es sei $(\Gamma, \circ)$ *ein Monoid und* $(\Sigma, *)$ *ein* Γ*-Monomodul. Eine vollständige Relation* σ *auf* Σ *heißt* ***Modul-Ordnung*** *, wenn für alle* $s_1, s_2, s_3 \in \Sigma$ *und* $\gamma \in \Gamma$ *gilt:*

(*i*) *Reflexivität:* $s_1 \geq_\sigma s_1$.

(*ii*) *Antisymmetrie:* $s_1 \geq_\sigma s_2 \wedge s_2 \geq_\sigma s_1 \Rightarrow s_1 = s_2$.

(*iii*) *Transitivität:* $s_1 \geq_\sigma s_2 \wedge s_2 \geq_\sigma s_3 \Rightarrow s_1 \geq_\sigma s_3$.

(Die Definitionen der Begriffe Monomodul und vollständige Relation sind aus [1] (Seite 41 bzw. 50) zu entnehmen.)

Definition und Bemerkung A.1

Es seien R *ein Ring ,* $P := R[x_1, .., x_n]$ *ein Polynomring,* σ *eine Modulordnung auf der Menge aller Terme* $\mathbb{T}^n\langle e_1, ..., e_r\rangle$ *von* P^r.
Die Elemente von P^r *haben die Form* $t \cdot e_j$ *für* $t \in \mathbb{T}^n$.
Jedes Element $m \in P^r \backslash \{0\}$ *hat eine eindeutige Darstellung als Linearkombination von Termen:*

$$m = \sum_{j=1}^{s} c_j t_j e_{\gamma_j} \qquad , c_j \in R\backslash\{0\} \, , \, t_j \in \mathbb{T}^n \, , \, \gamma_j \in \mathbb{N}_r \, , \, t_1 e_{\gamma_1} >_\sigma ... >_\sigma t_s e_{\gamma_s}.$$

Definition A.6

Für obiges m *definiert man:*

(*i*) *Der Term* $LT_\sigma(m) := t_1 e_{\gamma_1} \in \mathbb{T}^n\langle e_1, ..., e_r\rangle$ *heißt der* ***Leitterm*** *von* m *bezüglich* σ .

(*ii*) *Das Element* $LC_\sigma(m) := c_1 \in R\backslash\{0\}$ *heißt der* ***Leitkoeffizient*** *von* m *bezüglich* σ .

(*iii*) *Der Term* $LM_\sigma(m) := LC_\sigma(m) \cdot LT_\sigma(m)$ *heißt das* ***Leitmonom*** *von* m *bezüglich* σ .

Satz A.1

Es seien P *ein Polynomring über* R *,* σ *eine Modulordnung auf* $\mathbb{T}^n\langle e_1, ..., e_r\rangle$.
Dann gelten die folgenden Rechenregeln:

(*i*) *Man hat* $supp(m_1 + m_2) \subseteq supp(m_1) \cup supp(m_2)$.

Ist überdies $m_1 + m_2 \neq 0$ *, so folgt die Abschätzung:*

$$LT_\sigma(m_1 + m_2) \leq_\sigma max_\sigma\{LT_\sigma(m_1), LT_\sigma(m_2)\} \ .$$

(*ii*) *Gelten die Beziehungen* $m_1 + m_2 \neq 0$ *sowie* $LT_\sigma(m_1) \neq LT_\sigma(m_2)$ *(bzw.* $LC_\sigma(m_1) + LC_\sigma(m_2) \neq 0$*) , dann ist:*

$$LT_\sigma(m_1 + m_2) = max_\sigma\{LT_\sigma(m_1), LT_\sigma(m_2)\} \ .$$

(*iii*) *Ist* R *ein Integritätsring und* τ *eine Monoidordnung auf* $\mathbb{T}^n$ *, so dass* σ *mit* τ *verträglich ist, dann gilt für* $g \in P$ *:*

$$LT_\sigma(gm) = LT_\sigma(g) \cdot LT_\sigma(m).$$

Beweis: Siehe in [1] auf Seite 61.

Definition A.7

Für $n \in \mathbb{N}$ *seien der Vektor* $m = \sum_{j=1}^{r} \sum_{\alpha \in \mathbb{N}_0^n} c_{\alpha,j} t_\alpha e_j \in P^r$ *und das Polynom* $f := \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha t_\alpha \in P$ *gegeben.*

(*i*) *Das Element* $c_{\alpha,j} \in R$ *heißt der* ***Koeffizient*** *des Terms* $t_\alpha e_j$ *vom* m*.*

(*ii*) *Der* ***Träger*** *von* m *ist gegeben durch:*

$$supp(m) := \{t_\alpha e_j \in \mathbb{T}^n\langle e_1, ..., e_r\rangle |\ c_{\alpha,j} \neq 0\}.$$

(*iii*) *Der* ***Grad*** *von* f*,* $f \neq 0$*, ist definiert durch:*

$$deg(f) := max\{deg(t_\alpha) |\ t_\alpha \in supp(f)\}.$$

Definition A.8

Eine Modulordnung σ *auf einer Menge* M *heißt* ***Wohlordnung****, falls jede nichtleere Teilmenge* $S \subseteq M$ *ein kleinstes Element* $m \in S$ *enthält, d. h. es gilt:*

$$m \leq_\sigma \tilde{m} \qquad \forall\ \tilde{m} \in S.$$

Theorem A.1

Eine Modulordnung σ *ist genau dann eine Wohlordnung auf* $\mathbb{T}^n\langle e_1, ..., e_r\rangle$*, falls jede monoton fallende Folge* $(m_j)_{j \in \mathbb{N}}$ *in* M *eine konstante Teilfolge besitzt.*

Beweis: Siehe in [1] auf Seite 56.

Definition A.9

Es sei R *ein Ring. Eine Teilmenge* $I \subseteq R$ *heißt genau dann ein* ***Ideal*** *von* R*, wenn folgende Bedingungen erfüllt sind:*

(*i*) $(I, +)$ *ist eine Untergruppe von* $(R, +)$*.*

(*ii*) $R \cdot I \subseteq I \quad \Leftrightarrow \quad (p \in I, r \in R \Rightarrow pr \in I \wedge rp \in I)$*.*

Literatur

[1] M. Kreuzer und L. Rabbiano , *Computational Commutative Algebra 1.* Springer Verlag, 2000.