Kapitel 2

Algebraische Gleichungen

Das Wort „Algebra“ wird auf eine Aufgabensammlung aus dem 9. Jahrhundert zurückgeführt; es entstand aus ihrem Titel „Hisâb al-jabr w'al-muqâbalah“ („Wissenschaft der Reduktion und des gegenseitigen Aufhebens“). Verfasst wurde dieses Buch von Muhammad ibn Musa al Hwârizmí, aus dessen Namen im Laufe der Zeit auch das Wort „Algorithmus“ entstanden sein soll.
Algebra in ihrem ursprünglichen Sinn ist so als die Lehre der Auflösung von Gleichungen zu verstehen. Damit beschäftigten sich bereits Mathematiker früher Kulturen, etwa im Zusammenhang mit Problemen geometrischer Art, wie sie in der Landvermessung auftraten. Es gibt Keilschrifttafeln aus dem 2. Jahrtausend v.u.Z., auf denen lineare Gleichungssysteme mit mehreren Unbekannten und sogar Systeme höheren Grades gelöst werden.

Wir haben bereits im 1. Kapitel gesehen, dass die Frage nach der Auflösung von Gleichungen immer wieder Anlass zur Erweiterung des Zahlbegriffs gab. Die ganzen Zahlen erhalten wir als Lösung des Problems, wie zu gegebenen natürlichen Zahlen a und b eine Zahl x gefunden werden kann, für die $a + x = b$ ist. Das ist allgemein möglich, wenn anstelle der natürlichen die ganzen Zahlen betrachtet werden.
Eine ähnliche Situation ergibt sich für die Multiplikation.
Die Gleichung $a \cdot x = b$ mit $a, b \in \mathbb{Z}$ und $a \neq 0$ besitzt erst nach Übergang zum Körper $\mathbb{Q}$ der rationalen Zahlen stets eine Lösung $x \in \mathbb{Q}$.
Wie schon früher erwähnt, entsteht durch die Konstruktion des Körpers $\mathbb{C}$ der komplexen Zahlen ein Zahlbereich, in dem jedes nichtkonstante Polynom mindestens eine Nullstelle besitzt. Wir wollen allerdings nicht übersehen, dass es vom Wissen über die Existenz einer Nullstelle bis zu ihrem Auffinden ein weiter Weg sein kann. Es gibt sogar Gleichungen, für die es prinzipiell unmöglich ist, eine Lösung im Sinne einer Formel anzugeben, in der außer den Grundrechenarten nur Wurzelausdrücke vorkommen, so wie wir dies z.B. von quadratischen Gleichungen kennen.
Ein Gegenbeispiel (wir geben hier keinen Beweis an) ist die recht einfach anmutende Gleichung $x^5 - 10x - 2 = 0$, die nach dem Zwischenwertsatz der Analysis sogar eine reelle Lösung besitzt. Dieses Phänomen werden wir erst recht zu beachten haben, wenn wir Systeme von Gleichungen höheren Grades mit mehreren Variablen lösen.
Der Verzicht auf Exaktheit beim Rechnen mit Näherungen wirft dagegen neue Probleme auf.

Die Naturwissenschaften und die Technik stellen gerade in der Gegenwart allerhöchste Anforderungen an die Mathematik hinsichtlich der Auflösung von Gleichungssystemen. Dies ist keine einseitige Entwicklung. Die Nutzung von Computern hatte zweifellos einen entscheidenden Einfluß auf die Entwicklung der letzten Jahrzehnte des 20. Jahrhunderts, wovon auch die „reine“ Mathematik nicht unberührt blieb: Die Auflösung polynomialer Gleichungen konnte in gewisser Weise automatisiert werden. Das symbolische Rechnen (auch *Computeralgebra* genannt) wurde nicht nur zu einer Schlüsseltechno-

logie der heutigen Informationsgesellschaft, es eröffnet der mathematischen Forschung den Zugang zur Nutzung von Algorithmen, die vergangenen Generationen von Mathematikern zwar in Ansätzen bekannt waren, wegen ihrer Komplexität aber ohne die aktuellen technischen Hilfsmittel nicht genutzt werden konnten.
Wir sollten jedoch nicht erwarten, dass eines Tages Maschinen unsere Arbeit erledigen, sondern müssen uns im Gegenteil bewusst sein, dass wir vor Herausforderungen stehen, wie es sie in der Geschichte der Mathematik noch nicht gegeben hat. Bruno Buchberger, der für die Computeralgebra fundamentale Arbeit geleistet hat, bemerkte dazu, wer heute Mathematik studiere, befinde sich „... im ‚Auge des Hurricans' der modernen Entwicklung und nicht irgendwo in einem Hinterzimmer" ... „Je algorithmischer und dann je effizienter man mathematische Probleme lösen will, umso mehr mathematische Theorie und umso schwierigere Beweise sind nötig und nicht umgekehrt" (vgl. [DMV][1]).

Das vorliegende Kapitel kann nicht mehr sein als ein Einstieg in die Frage nach den Lösungen polynomialer Gleichungssysteme. Am Schluss wird klar, dass die Struktur der Lösungsmengen sehr viel subtiler ist, als es auf den ersten Blick vermutet werden mag. Die mathematische Disziplin, die sich insbesondere den qualitativen Aspekten des Studiums der Lösungsmengen widmet, ist die algebraische Geometrie. Die numerische Mathematik befasst sich dagegen mit dem Auffinden von Näherungslösungen; auch dazu können wir hier nur Andeutungen machen.

2.5 Allgemeine polynomiale Gleichungssysteme

Nachfolgend werden lineare Ordnungsrelationen auf $\mathcal{M}_n$ und gleich bedeutend auf $\mathbb{N}^n$ betrachtet, die mit der jeweiligen Operation $\cdot$ bzw. $+$ sowie mit der Teilbarkeit bzw. der natürlichen Ordnung verträglich sind; auf beiden Monoiden erhalten sie dieselben Namen. Solche Ordnungen heißen *Monomordnungen* (auch *Termordnungen*). 2/5/8

Definition. (*Monomordnung*)
Eine *Monomordnung* für $K[\boldsymbol{X}]$ ist eine lineare Ordnung $\leq$ auf der Menge $\mathcal{M}_n$ der Monome in $K[\boldsymbol{X}]$, die folgende Eigenschaften erfüllt.

(1) Aus $\boldsymbol{m}, \boldsymbol{m}_1, \boldsymbol{m}_2 \in \mathcal{M}_n$ und $\boldsymbol{m}_1 \leq \boldsymbol{m}_2$ folgt $\boldsymbol{m}\boldsymbol{m}_1 \leq \boldsymbol{m}\boldsymbol{m}_2$
(Verträglichkeit mit der Struktur von $\mathcal{M}_n$ als Monoid).
(2) $\leq$ ist eine Wohlordnung
(d.h. jede nichtleere Teilmenge besitzt ein kleinstes Element).

Wie üblich wird das Symbol $\boldsymbol{m}_1 < \boldsymbol{m}_2$ verwendet um auszudrücken, dass $\boldsymbol{m}_1 \leq \boldsymbol{m}_2$ und $\boldsymbol{m}_1 \neq \boldsymbol{m}_2$ gilt.

Bevor wir uns den Begriff an Beispielen veranschaulichen, wird zunächst eine äquivalente Charakterisierung angegeben.

Satz. *Eine lineare Ordnung $\leq$ auf $\mathcal{M}_n$ mit der obigen Eigenschaft* (1) *ist genau dann eine Monomordnung, wenn sie die folgende Bedingung erfüllt.* 2/5/9
(2′) $1 \in \mathcal{M}_n$ *ist minimal bezüglich* $\leq$.

[1] *Mitteilungen der Deutschen Mathematiker-Vereinigung*, 2/2000

Beweis. Ist auf $\mathcal{M}_n$ eine Monomordnung gegeben, so existiert ein kleinstes Element $\boldsymbol{m} \in \mathcal{M}_n$. Dann ist $\boldsymbol{m} \leq 1$, und falls keine Gleichheit besteht, muss nach (1) sogar $\boldsymbol{m}^2 < \boldsymbol{m}$ sein, was wegen $\boldsymbol{m}^2 \neq \boldsymbol{m}$ der Minimalität von $\boldsymbol{m}$ widerspricht.
Wir zeigen umgekehrt, dass eine lineare Ordnung $\leq$ mit den Eigenschaften (1), (2′) Monomordnung ist. Sind $\boldsymbol{m}, \boldsymbol{m}' \in \mathcal{M}_n$ mit $\boldsymbol{m}'|\boldsymbol{m}$, so gilt $\boldsymbol{m}' \leq \boldsymbol{m}$ (aus $\boldsymbol{m}' \cdot \boldsymbol{q} = \boldsymbol{m}$ folgt wegen $1 \leq \boldsymbol{q}$ offensichtlich $\boldsymbol{m}' \leq \boldsymbol{m}' \cdot \boldsymbol{q} = \boldsymbol{m}$). Nun wählen wir eine beliebige nichtleere Teilmenge $M \subseteq \mathcal{M}_n$. Ist $\boldsymbol{a} = (M)$ das von ihr erzeugte Ideal, so existiert nach dem Korollar zu Dicksons Lemma (vgl. 2/5/7) eine endliche Teilmenge $S = \{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_r\} \subseteq M$ mit $\boldsymbol{a} = (S)$, für die o.B.d.A. $\boldsymbol{m}_1 < \ldots < \boldsymbol{m}_r$ ist. Da jedes Monom $\boldsymbol{m} \in \boldsymbol{a}$ Vielfaches eines der $\boldsymbol{m}_i$ ist, folgt $\boldsymbol{m}_1 \leq \boldsymbol{m}_i \leq \boldsymbol{m}$ insbesondere für Monome $\boldsymbol{m} \in M$, d.h. $\boldsymbol{m}_1$ ist kleinstes Element in M. ❏

Es zeigt sich, dass eine Monomordnung die durch Teilbarkeit gegebene Ordnung auf $\mathcal{M}^n$ verfeinert, d.h. $\boldsymbol{m}'|\boldsymbol{m} \Rightarrow \boldsymbol{m}' \leq \boldsymbol{m}$. Mit den entsprechenden Notationen für $\mathbb{N}^n$ heißt das $\mu \preceq \nu \Rightarrow \mu \leq \nu$. Die Eigenschaft (1) besagt $\mu_1 \leq \mu_2 \Rightarrow \mu + \mu_1 \leq \mu + \mu_2$ für $\mu, \mu_1, \mu_2 \in \mathbb{N}^n$.

Einige Monomordnungen

2/5/10

Die folgenden Ordnungen werden zur Vereinfachung der Bezeichnungen auf der Menge $\mathbb{N}^n$ der Exponenten angegeben. Unter 4. werden wir sehen, dass durch die ersten beiden Beispiele Monomordnungen gegeben sind.

1. *lexikographische Ordnung*
   Für $\mu, \nu \in \mathbb{N}^n$ wird $\mu <_{\text{lex}} \nu$ gesetzt, wenn ein $j \in \{1, \ldots, n\}$ existiert mit $\mu_i = \nu_i$ für $i < j$ und $\mu_j < \nu_j$.

   Diese Bedingung lässt sich äquivalent auch folgendermaßen ausdrücken: Der erste von 0 verschiedene Eintrag des n-Tupels $\mu - \nu \in \mathbb{Z}^n$ ist negativ.

2. *graduiert invers-lexikographische Ordnung*
   Wir verwenden wieder die Bezeichnung $|(\nu_1, \ldots, \nu_n)| = \nu_1 + \ldots + \nu_n$.
   Für $\mu, \nu \in \mathbb{N}^n$ wird $\mu <_{\text{d}} \nu$ gesetzt, wenn $|\mu| < |\nu|$ ist oder $|\mu| = |\nu|$ und ein $j \in \{1, \ldots, n\}$ existiert mit $\mu_i = \nu_i$ für $i > j$ sowie $\mu_j > \nu_j$.

   Die zweite Bedingung lässt sich (im Fall $|\mu| = |\nu|$) äquivalent auch folgendermaßen ausdrücken: Der letzte von 0 verschiedene Eintrag des n-Tupels $\mu - \nu \in \mathbb{Z}^n$ ist positiv.

3. *Blockordnungen (Produktordnungen)*
   Ist $<_1$ eine Ordnung auf $\mathbb{N}^{n_1}$ und $<_2$ eine Ordnung auf $\mathbb{N}^{n_2}$, so heißt die nachfolgend definierte Ordnung $<$ die *durch $<_1$ und $<_2$ gegebene Blockordnung* auf $\mathbb{N}^{n_1+n_2}$:
   Für $\mu, \mu' \in \mathbb{N}^{n_1}$ und $\nu, \nu' \in \mathbb{N}^{n_2}$ wird $(\mu, \nu) < (\mu', \nu')$ gesetzt, falls $\mu <_1 \mu'$ ist oder $\mu = \mu'$ und $\nu <_2 \nu'$.
   Sind $<_1$ und $<_2$ Monomordnungen, so ist auch $<$ eine Monomordnung.

4. *Matrixordnungen*
   $A \in \mathrm{GL}(n; \mathbb{R})$ sei eine reguläre Matrix. Für $\mu, \nu \in \mathbb{N}^n$ wird die *Matrixordnung* $<_A$ durch folgende Bedingung definiert:

   $$\mu <_A \nu \iff \begin{array}{l}\textit{Der erste von } 0 \textit{ verschiedene Eintrag} \\ \textit{in } A \cdot {}^{\text{t}}(\mu - \nu) \textit{ ist negativ.}\end{array}$$

   Wir geben noch eine äquivalente Bedingung an:

   $$\mu <_A \nu \iff \begin{array}{l}A \cdot {}^{\text{t}}\mu <_{\text{lex}} A \cdot {}^{\text{t}}\nu \textit{ in der lexikographischen} \\ \textit{Ordnung } <_{\text{lex}} \textit{ von } \mathrm{M}(n, 1; \mathbb{R}).\end{array}$$

   Beispielsweise ist die lexikographische Ordnung unter 1. die Matrixordnung $<_{\mathrm{E}_n}$, und unter 2. steht die durch

$$A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & & -1 \\ \dots\dots\dots & & \ddots & & \dots \\ 0 & 0 & -1 & & 0 \\ 0 & -1 & 0 & \dots & 0 \end{pmatrix}$$

gegebene Matrixordnung $<_A$.
Sind $A_1 \in \mathrm{M}(n_1;\mathbb{R})$ und $A_2 \in \mathrm{M}(n_2;\mathbb{R})$ reguläre Matrizen, so stimmt die durch $<_{A_1}$ und $<_{A_2}$ definierte Blockordnung mit der durch die Blockmatrix $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ definierten überein.

Nun wird nicht behauptet, dass jede Matrixordnung eine Monomordnung ist, was durch Gegenbeispiele leicht widerlegt werden kann. *Eine Matrixordnung $<_A$ ist genau dann eine Monomordnung, wenn in jeder Spalte der Matrix A der erste von 0 verschiedene Eintrag positiv ist.*
Das sehen wir folgendermaßen:
Um zu prüfen, dass eine lineare Ordnung vorliegt, muss nur gezeigt werden, dass für $\mu \neq \mu'$ stets $A \cdot {}^{\mathrm{t}}\mu \neq A \cdot {}^{\mathrm{t}}\mu'$ gilt. Anderenfalls wäre allerdings $A \cdot {}^{\mathrm{t}}(\mu - \mu') = 0$, d.h. wegen der Regularität von A auch $\mu - \mu' = \mathbf{0}$, was unmöglich ist.
Die Verträglichkeit der Addition auf $\mathbb{N}^n$ mit der Ordnung $<_A$ folgt aus dem Distributivgesetz der Matrizenrechnung.
Weiter ist $\mathbf{0} \in \mathbb{N}^n$ genau dann minimal für $<_A$, wenn der erste nichtverschwindende Eintrag jeder Spalte von A positiv ist (vgl. $(2')$ aus dem vorigen Satz 2/5/9), denn dies bedeutet $\boldsymbol{e}_i >_A \mathbf{0}$ für alle i.

Bemerkung.

(1) Für $n = 1$ gibt es nur eine einzige Monomordnung, sie ist durch
$$1 < X < X^2 < \ldots < X^i < X^{i+1} < \ldots$$
gegeben, denn 1 ist minimal in $\mathcal{M}$, und aus $1 < X$ folgt nach Multiplikation mit X^p auch $X^p = X^p \cdot 1 < X^p \cdot X = X^{p+1}$.

(2) Für $n = 2$ gibt es bereits unendlich viele Monomordnungen.

Wählen Sie z.B. die Monomordnung $<_n$, die durch die Matrix $A_n := \begin{pmatrix} 2^n & 1 \\ 0 & 1 \end{pmatrix}$ gegeben ist.
Es gilt $(0, 2^n) <_n (2, 0)$ sowie $(0, 2^n) \geq_k (2, 0)$ für $k < n$.

(3) Als Beispiel betrachten wir die graduiert invers-lexikographische Ordnung $<$ auf $K[X_1, X_2, X_3]$.
$$1 < X_3 < X_2 < X_1 < X_3^2 < X_2X_3 < X_1X_3 < X_2^2 < X_1X_2 < X_1^2 < X_3^3$$
sind die 11 kleinsten Monome.

Leitmonome und Leitkoeffizienten

2/5/11

Von nun an bezeichnet $<$ eine fest gewählte Monomordnung. Für $f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu \in K[\boldsymbol{X}]$ mit $a_\nu \in K$ wird die Menge

$$\mathrm{Supp}(f) := \{\nu \in \mathbb{N}^n \mid a_\nu \neq 0\}$$

der Träger von f genannt. Ist $\mathrm{Supp}(f) \neq \emptyset$, so heißen

$$\mathrm{LM}_<(f) := X^\mu \text{ bzw. } \mathrm{LC}_<(f) := a_\mu \text{ mit } \mu := \max\nolimits_<\big(\mathrm{Supp}(f)\big)$$

Leitmonom bzw. *Leitkoeffizient* von f;

$$\mathrm{LT}_<(f) := \mathrm{LC}_<(f) \cdot \mathrm{LM}_<(f)$$

wird der *Leitterm* von f genannt. Diese Notation knüpft an die schon in 1/2/16 (2) eingeführte Sprechweise an; offenbar ist $f \in K[\boldsymbol{X}] \setminus \{0\}$ genau dann ein Term, wenn $f = \mathrm{LT}_<(f)$ ist. Das n-Tupel

$$\mathrm{mdeg}_<(f) := \log\big(\mathrm{LM}_<(f)\big) \in \mathbb{N}^n$$

wird als Multigrad von f bezeichnet. Jedes von 0 verschiedene Polynom ist auf eindeutige Weise Summe von Termen mit paarweise verschiedenem Multigrad, und es ist zweckmäßig, beim Rechnen die Terme nach absteigendem Multigrad anzuordnen – so wie das in den Beispielen geschehen wird. Zur Vereinfachung verzichten wir in den Bezeichnungen meist auf die Angabe der (hier fixierten) Monomordnung.

Beispiel. $f = 3X_1^2X_2^2 + 4X_1X_2^2 - 1 \in \mathbb{R}[X_1, X_2, X_3]$ hat bezüglich der lexikographischen Ordnung das Leitmonom $\mathrm{LM}(f) = X_1^2X_2^2$ und den Leitkoeffizienten $\mathrm{LC}(f) = 3$. Damit ist $\mathrm{LT}(f) = 3X_1^2X_2^2$, und der Multigrad von f ist $\mathrm{mdeg}(f) = (2, 2)$.

Bemerkung. Sind $f, g \in K[\boldsymbol{X}] \setminus \{0\}$ Polynome, so gilt: 2/5/12

(1) $\mathrm{mdeg}(f \cdot g) = \mathrm{mdeg}(f) + \mathrm{mdeg}(g)$, d.h.
$\mathrm{LM}(f \cdot g) = \mathrm{LM}(f) \cdot \mathrm{LM}(g)$.

(2) Für $f + g \neq 0$ ist $\mathrm{mdeg}(f + g) \leq \max\{\mathrm{mdeg}(f), \mathrm{mdeg}(g)\}$,
und im Fall $\mathrm{mdeg}(f) \neq \mathrm{mdeg}(g)$ besteht Gleichheit.

Beide Eigenschaften sind schon bekannt, falls $n = 1$ und damit $\mathrm{mdeg}(f) = \deg_{\boldsymbol{X}}(f)$ der vollständige Grad ist. (1) ergibt sich durch Ausmultiplizieren von f und g nach den Eigenschaften einer Monomordnung.

Das folgende Lemma zeigt insbesondere, dass das kleinste gemeinsame Vielfache und der größte gemeinsame Teiler von Monomen existieren. Darüber hinaus gilt sogar der (hier weder benutzte noch bewiesene) Satz, dass im Ring $K[X_1, \ldots, X_n]$ eine eindeutige Zerlegung in irreduzible Faktoren existiert.

Lemma. *$\boldsymbol{m} \in \mathcal{M}_n$ sei ein Monom und $f \in K[\boldsymbol{X}]$ ein Teiler von $\boldsymbol{m}$. Dann ist f ein Term.*

Beweis. Wir fixieren die lexikographische Ordnung in $\mathcal{M}_n$. Ist $h \neq 0$ ein Polynom, so bezeichne $\mathrm{lm}(h)$ das Monom kleinsten Multigrades im Träger von h. Offensichtlich gilt

$$\mathrm{lm}(h_1 \cdot h_1) = \mathrm{lm}(h_1) \cdot \mathrm{lm}(h_2) \quad \text{für beliebige } h_1, h_2 \in K[\boldsymbol{X}] \setminus \{0\}.$$

Nun sei $\boldsymbol{m} = q \cdot f$ mit einem geeigneten Polynom q. Dann folgt

$$\mathrm{lm}(\boldsymbol{m}) = \mathrm{lm}(q) \cdot \mathrm{lm}(f) \leq \mathrm{LM}(q) \cdot \mathrm{LM}(f) = \mathrm{LM}(\boldsymbol{m}),$$

und wegen $\mathrm{lm}(\boldsymbol{m}) = \mathrm{LM}(\boldsymbol{m})$ kann keine der Beziehungen $\mathrm{lm}(q) \leq \mathrm{LM}(q)$, $\mathrm{lm}(f) \leq \mathrm{LM}(f)$ Ungleichheit sein. Daher sind q und f Terme. ❑

Mit nicht allzu großem Aufwand ergibt sich nun die folgende

Bemerkung. Wir betrachten Monome $\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau$ in $K[\boldsymbol{X}]$. 2/5/13

(1) $\mathrm{kgV}(\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau) := X_1^{\max\{\sigma_1,\tau_1\}} \cdot \ldots \cdot X_n^{\max\{\sigma_n,\tau_n\}}$
ist kleinstes gemeinsames Vielfaches von $\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau$.

(2) $\mathrm{ggT}(\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau) := X_1^{\min\{\sigma_1,\tau_1\}} \cdot \ldots \cdot X_n^{\min\{\sigma_n,\tau_n\}}$
ist größter gemeinsamer Teiler von $\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau$.

Für (2) verwenden wir das vorhergehende Lemma.

(3) Die Bedingung $\mathrm{ggT}(\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau) = 1$ besagt, dass $\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau$ als gemeinsame Teiler nur Polynome aus K^* besitzen; sie ist äquivalent zu
$\mathrm{kgV}(\boldsymbol{X}^\sigma, \boldsymbol{X}^\tau) = \boldsymbol{X}^{\sigma+\tau}$.

Division mit Rest 2/5/14

Für beliebige $f, g \in K[\boldsymbol{X}] - \{0\}$ setzen wir

$$\mathrm{S}(f,g) := \frac{\boldsymbol{X}^\nu}{\mathrm{LM}(f)} \cdot f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot \frac{\boldsymbol{X}^\nu}{\mathrm{LM}(g)} \cdot g \quad \text{mit}$$
$$\boldsymbol{X}^\nu := \mathrm{kgV}\big(\mathrm{LM}(f), \mathrm{LM}(g)\big).$$

$\mathrm{S}(f,g)$ heißt das S-Polynom von f und g.

Das S-Polynom haben wir in speziellen Situationen bereits kennen gelernt (vgl. 2/2/1 und 2/4/1). Sie können sich leicht davon überzeugen, dass die dort angegebenen Definitionen als Spezialfälle aus dieser hervorgehen.

Besonders einfache Gestalt hat $\mathrm{S}(f,g)$, wenn $\mathrm{LM}(g)$ Teiler von $\mathrm{LM}(f)$ ist; dann folgt $\mathrm{S}(f,g) = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} \cdot g$, und es ist $\mathrm{mdeg}\big(\mathrm{S}(f,g)\big) < \mathrm{mdeg}(f)$ oder $\mathrm{S}(f,g) = 0$.

Nun wird ein s-Tupel $F = (f_1, \ldots, f_m) \in K[\boldsymbol{X}]^m$ von 0 verschiedener Polynome fixiert.

(1) $g \in K[\boldsymbol{X}]$ heißt *speziell erzeugbar* durch F, falls entweder $g = 0$ ist oder Polynome $q_1, \ldots, q_s \in K[\boldsymbol{X}]$ existieren, so dass $g = \sum_{i=1}^m q_i f_i$ und für alle $i \in \{1, \ldots, s\}$ mit $q_i f_i \neq 0$ gilt $\mathrm{LM}(q_i f_i) \leq \mathrm{LM}(g)$.
Nach 2/5/12 ist für $g \neq 0$ diese Bedingung gleich bedeutend mit $g = \sum_{i=1}^m q_i f_i$ und $\mathrm{mdeg}(g) = \max\{\mathrm{mdeg}(q_i f_i) \mid 1 \leq i \leq s,\, q_i f_i \neq 0\}$.

(2) $r \in K[\boldsymbol{X}]$ heißt Rest bezüglich einer Menge $\{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_m\}$ von Monomen, falls für keinen Multiindex $\nu \in \mathrm{Supp}(r)$ das Monom $\boldsymbol{X}^\nu$ durch eines der Monome $\boldsymbol{m}_i$ teilbar ist.
Sinngemäß wird r Rest bezüglich F genannt, wenn r ein Rest bezüglich $\{\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\}$ ist, d.h. wenn für keinen Multiindex $\nu \in \mathrm{Supp}(r)$ das Monom $\boldsymbol{X}^\nu$ durch eines der Monome $\mathrm{LM}(f_i)$ teilbar ist.

Eigenschaft (1) besagt insbesondere, dass ein durch F speziell erzeugbares Element in dem von den Polynomen f_i erzeugten Ideal liegt. Bald wird klar sein, dass die Umkehrung im Allgemeinen nicht richtig ist.

Es gibt (viele!) Beispiele, in denen nicht jedes Element aus dem Ideal $(f_1, \ldots, f_m)$ durch die Polynome f_i speziell erzeugbar ist.

Wir stellen uns die Aufgabe, ein beliebiges Polynom als Summe eines speziell erzeugten und eines Rests darzustellen. 2/5/15

Bemerkung. (*Divisionsalgorithmus*)

$f \neq 0$ sei ein Polynom, so ersetzen wir schrittweise f durch ein Polynom $f^{(1)}$ mit $\mathrm{LM}(f^{(1)}) < \mathrm{LM}(f)$, für das $f - f^{(1)}$ Vielfaches eines der Polynome f_i oder ein Rest ist:

$$f^{(1)} := \begin{cases} f - \mathrm{LT}(f)\,, & \text{falls } \mathrm{LM}(f_i) \not| \mathrm{LM}(f),\ i = 1, \ldots, s \\ \mathrm{S}(f, f_i) & (= f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} \cdot f_i)\,, \\ & \text{falls } \ i = \min\{j \mid \mathrm{LM}(f_j) \text{ teilt } \mathrm{LM}(f)\}. \end{cases}$$

Im ersten Fall ist $f - f^{(1)} = \mathrm{LT}(f)$ ein Rest, im zweiten Fall folgt
$f - f^{(1)} = \frac{\mathrm{LT}(f)}{\mathrm{LT}(f_i)} \cdot f_i$.

Entsprechend ergibt sich induktiv aus $f^{(i)}$ ein Polynom $f^{(i+1)}$ und so eine Folge $f = f^{(0)}, f^{(1)}, \ldots, f^{(j)}, \ldots$ mit $\mathrm{LM}(f^{(j+1)}) < \mathrm{LM}(f^{(j)})$. Die gegebene Monomordnung ist eine Wohlordnung, daher muss nach endlich vielen Schritten das Verfahren mit $f^{(t)} = 0$ abbrechen.
Eine Summe von Resten ist wieder ein Rest, und schrittweises Einsetzen ergibt $f = \sum_{i=1}^m q_i f_i + r$ mit einem Rest r und $\mathrm{LM}(\sum_{i=1}^m q_i f_i) = \max\{\mathrm{LM}(q_i f_i) \mid q_i f_i \neq 0\}$, falls $r \neq f$. Das hier gefundene (und durch Kon-

Vorsicht, wenn Sie die Reihenfolge der Einträge $f_1, \ldots, f_m$ ignorieren.

struktion eindeutig bestimmte) Polynom r heißt Rest von f bei Division durch F. Analog zu der für $m = n = 1$ üblichen Schreibweise wird

$$f : (f_1, \ldots, f_m) = (q_1, \ldots, q_m) \text{ Rest } r.$$

als Notation für diesen Sachverhalt benutzt.

Beispiele. (*Division mit Rest*)

Hier wird die lexikographische Monomordnung gewählt.

Wir betrachten $F = (f_1, f_2) \in \mathbb{R}[X_1, X_2, X_3]^2$, $f_1 = X_1^2$, $f_2 = X_1X_2 + X_3^2$ und dividieren $f = X_1^2X_2^2 + X_1X_2^2 - 1$ mit Rest durch F.

$$\begin{array}{l|l} (X_1^2X_2^2 + X_1X_2^2 - 1) & (X_1^2, X_1X_2 + X_3^2) = (X_2^2, X_2) \text{ Rest } -X_2X_3^2 - 1 \\ \hline X_1^2X_2^2 & \\ \hline X_1X_2^2 - 1 & \\ X_1X_2^2 + X_2X_3^2 & \\ \hline -X_2X_3^2 - 1 & \end{array}$$

und damit $f = X_2^2 \cdot f_1 + X_2 f_2 + (-X_2X_3^2 - 1)$. Nun wird die Reihenfolge von f_1 und f_2 vertauscht und erneut dividiert.

$$\begin{array}{l|l} (X_1^2X_2^2 + X_1X_2^2 - 1) & (X_1X_2 + X_3^2, X_1^2) = (X_1X_2 + X_2 - X_3^2, 0) \\ X_1^2X_2^2 + X_1X_2X_3^2 & \text{Rest } -X_2X_3^2 + X_3^4 - 1 \\ \hline X_1X_2^2 - X_1X_2X_3^2 - 1 & \\ X_1X_2^2 + X_2X_3^2 & \\ \hline -X_1X_2X_3^2 - X_2X_3^2 - 1 & \\ -X_1X_2X_3^2 - X_3^4 & \\ \hline -X_2X_3^2 + X_3^4 - 1 & \end{array}$$

Wir erhalten $f = 0 \cdot f_1 + (X_1X_2 + X_2 - X_3^2) \cdot f_2 + (-X_2X_3^2 + X_3^4 - 1)$. Das Beispiel zeigt: Rest und Faktoren der f_i sind durch f nicht eindeutig bestimmt, der angegebene Algorithmus kann nach Permutation der f_i unterschiedliche Resultate ergeben.

Nachfolgend verdeutlichen wir noch das Vorgehen, wenn Reste in den Zwischenschritten auftreten.

$$\begin{array}{l|l} (X_1^3 + X_1 + X_2^2) & : (X_1^2 + X_2, X_2^2 + 1) = (X_1, 1) \quad \text{Rest } -X_1X_2 + X_1 - 1 \\ X_1^3 + X_1X_2 & \\ \hline -X_1X_2 + X_1 + X_2^2 & \\ X_2^2 + 1 & \\ \hline -X_1X_2 + X_1 - 1 & \end{array}$$

Satz. *Ist $F = (f_1, \ldots, f_m) \in (K[\boldsymbol{X}] \setminus \{0\})^m$, so existieren für jedes Polynom $f \in K[\boldsymbol{X}]$ bezüglich F ein Rest r und ein speziell erzeugbares Polynom g mit $f = g + r$.* 2/5/16

Dabei ist $g = 0$ oder es existieren Polynome q_i, so dass $f = \sum_{i=1}^m q_i f_i + r$ und $\operatorname{mdeg}(q_i f_i) \leq \operatorname{mdeg}(f)$ für alle i mit $q_i f_i \neq 0$.

Beweis. Der Divisionsalgorithmus zeigt die Existenz einer Zerlegung von f in eine Summe $f = g + r$, r ein Rest sowie $g = 0$ oder

$$g = \sum_{i=1}^m q_i f_i, \quad \operatorname{LM}(g) = \max\{\operatorname{LM}(q_i f_i) \mid 1 \leq i \leq m,\, q_i \neq 0\}$$

mit geeigneten Polynomen q_i. Es bleibt der zweite Teil der Behauptung zu prüfen, d.h. es genügt zu zeigen, dass $\operatorname{LM}(g) \leq \operatorname{LM}(f)$ gilt. Da eine

Monomordnung linear ist, muss anderenfalls $\mathrm{LM}(f) < \mathrm{LM}(f-r)$ sein. Dann ist insbesondere $r \neq 0$. Wegen $f = (f-r)+r$ gilt

$$\mathrm{LM}(f) \leq \max\{\mathrm{LM}(f-r), \mathrm{LM}(r)\},$$

und Gleichheit steht im Widerspruch zu $\mathrm{LM}(f) < \mathrm{LM}(f-r)$. Als einzige Möglichkeit bleibt Übereinstimmung der Leitmonome von $f-r$ und r, d.h. $\mathrm{LM}(r) = \mathrm{LM}(f-r) = \mathrm{LM}(g) = \mathrm{LM}(q_i f_i) = \mathrm{LM}(q_i) \cdot \mathrm{LM}(f_i)$ für einen geeigneten Index i. Wir haben damit gezeigt, dass $\mathrm{LM}(f_i)$ ein Teiler von $\mathrm{LM}(r)$ und deshalb r kein Rest bezüglich F ist, ↯. ❏

Reduzierte Gröbnerbasen

2/5/28

Für konsistente lineare Gleichungssysteme haben wir eine eindeutig bestimmte reduzierte Form kennen gelernt. Ebenso ist im Polynomring einer Unbestimmten der größte gemeinsame Teiler (wenn er – wie vereinbart – als normiertes Polynom gewählt wird) eindeutig bestimmt. Nachfolgend konstruieren wir zu einer gegebenen Monomordnung unter allen Gröbnerbasen eines Ideals eine eindeutig bestimmte *reduzierte* Gröbnerbasis.

Lemma. $\boldsymbol{a} \neq 0$ *sei ein Ideal im Polynomring* $K[X_1, \ldots X_n]$.

(1) *Ist* $\{f_1, \ldots, f_m\}$ *eine Gröbnerbasis von* $\boldsymbol{a}$*, so entsteht durch schrittweises Weglassen derjenigen* f_i*, für die* $\mathrm{LM}(f_i)$ *durch eines der Monome* $\mathrm{LM}(f_j)$ *mit* $j \neq i$ *teilbar ist, eine Gröbnerbasis* $\{g_1, \ldots, g_t\} \subseteq \{f_1, \ldots, f_m\}$ *von* $\boldsymbol{a}$*, für die* $\mathrm{LM}(g_i) \nmid \mathrm{LM}(g_j)$ *falls* $i \neq j$.

(2) *Unter* (1) *sind* $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)$ *die bezüglich der Teilbarkeitsrelation minimalen Elemente von* $\mathrm{L}(\boldsymbol{a}) \cap \mathcal{M}_n$ *und damit eindeutig bestimmt.*

Beweis. (1) Das Leitideal von $\boldsymbol{a}$ ist $\mathrm{L}(\boldsymbol{a}) = \big(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\big)$. Wird nun ein Monom $\mathrm{LM}(f_i)$ weggelassen, das Vielfaches eines der übrigen Monome $\mathrm{LM}(f_j)$ ist, so gilt

$$\big(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_m)\big) = \big(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_{i-1}), \mathrm{LM}(f_{i+1}), \ldots, \mathrm{LM}(f_m)\big),$$

daher ist $\{f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m\}$ ebenfalls Gröbnerbasis von $\boldsymbol{a}$. (2) ist ebenfalls offensichtlich. ❏

Definition. Eine Gröbnerbasis $\{g_1, \ldots, g_t\}$ heißt *reduziert,* falls für alle Indizes $i \in \{1, \ldots, t\}$ gilt: 2/5/29

(1) $\mathrm{LC}(g_i) = 1$.

(2) g_i ist ein Rest bezüglich $\{g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_t\}$, d.h. kein Term von g_i ist durch eines der Monome $\mathrm{LM}(g_j)$ mit $j \neq i$ teilbar.

Beispiele.

(1) Wählen wir eine Monomordnung mit $X_1 > \ldots > X_n$, so ist die reduzierte Form eines konsistenten linearen Gleichungssystems (vgl. 2/2/12) reduzierte Gröbnerbasis des von diesen linearen Polynomen erzeugten Ideals. Das System ist genau dann inkonsistent, wenn 1 in dem Ideal liegt, d.h. wenn $\{1\}$ reduzierte Gröbnerbasis ist.

(2) Die Gröbnerbasis $\{f_1, f_2, -f_3, f_4\}$ gemäß Beispiel 2/5/26 ist reduziert.

(3) In $\mathbb{R}[X_1, X_2, X_3, X_4]$ ist $\{f_1, f_2, f_3\}$ mit

$$f_1 = X_1^2 + X_2^2 X_3 + X_3^4 X_4^2$$
$$f_2 = X_2^3 + X_2 X_3 + X_3^2$$
$$f_3 = X_3^2 X_4 + X_4 + 1$$

eine Gröbnerbasis bezüglich der lexikographischen Ordnung (vgl. Lemma 2/5/27), jedoch offenbar nicht reduziert.
Wir suchen eine reduzierte Gröbnerbasis des von f_1, f_2, f_3 erzeugten Ideals. Zwischen den Leitmonomen bestehen keine Teilbarkeitsrelationen; wir bestimmen die Reste von $f_i - \mathrm{LT}(f_i)$ bei Division durch die übrigen f_j, die natürlich bis auf ein Element des von den Polynomen f_i erzeugten Ideals damit übereinstimmen. Für $i = 2, 3$ liegen bereits Reste vor, und $f_1 - \mathrm{LT}(f_1) = X_2^2 X_3 + X_3^4 X_4^2$ hat bei Division durch (f_2, f_3) den Rest $r = X_2^2 X_3 + X_4^2 + 2X_4 + 1$. Wir ersetzen f_1 durch $\mathrm{LM}(f_1) + r$ und erhalten für das von f_1, f_2, f_3 erzeugte Ideal

$$\{X_1^2 + X_2^2 X_3 + X_4^2 + 2X_4 + 1,\ X_2^3 + X_2 X_3 + X_3^2,\ X_3^2 X_4 + X_4 + 1\}$$

als reduzierte Gröbnerbasis.

Aus dem Beispiel (3) wird bereits deutlich, wie eine reduzierte Gröbnerbasis allgemein gefunden werden kann.

Satz. (*Existenz und Eindeutigkeit reduzierter Gröbnerbasen*) 2/5/30

Ist $\boldsymbol{a} \neq 0$ ein Ideal im Polynomring $K[X_1, \ldots X_n]$ mit der Monomordnung $<$, so besitzt dieses eine eindeutig bestimmte reduzierte Gröbnerbasis bezüglich $<$.

Beweis. Nach dem Lemma existiert zunächst eine Gröbnerbasis $\{g_1, \ldots, g_t\}$ von $\boldsymbol{a}$, für die $\mathrm{LM}(g_i)$ durch keines der Monome $\mathrm{LM}(g_j)$ $(j \neq i)$ teilbar ist. Induktiv wird g_i durch $g_i' \in \boldsymbol{a}$ ersetzt, so dass $\mathrm{LM}(g_i) = \mathrm{LM}(g_i')$ sowie jeder Term von g_i' ein Rest bezüglich der Leitmonome der übrigen $\mathrm{LM}(g_j)$ ist: $\mathrm{LT}(g_i)$ erfüllt bereits die letztere Bedingung. Nun wird für $g_i - \mathrm{LT}(g_i)$ die Division mit Rest ausgeführt, so dass $g_i - \mathrm{LT}(g_i) = \sum_{j, j \neq i} q_j g_j + h_i$ mit dem Rest h_i ist. Wir setzen $g_i' := \mathrm{LT}(g_i) + h_i$ und erhalten wegen $g_i - g_i' = \sum_{j, j \neq i} q_j g_j$ ein Polynom $g_i' \in \boldsymbol{a}$, das die behauptete Eigenschaft besitzt. Durch wiederholte Anwendung und ggf. Multiplikation mit Konstanten ergibt sich eine reduzierte Gröbnerbasis für $\boldsymbol{a}$.
Die Eindeutigkeit folgt nun so: Wir betrachten zwei reduzierte Gröbnerbasen $\{g_1, \ldots, g_t\}$ und $\{\tilde{g}_1, \ldots, \tilde{g}_{\tilde{t}}\}$ von $\boldsymbol{a}$. Nach Lemma 2/5/28 (2) sind die Leitmonome eindeutig bestimmt, daher $t = \tilde{t}$ und bei geeigneter Anordnung $\mathrm{LM}(g_i) = \mathrm{LM}(\tilde{g}_i)$ für $i = 1, \ldots, t$ sowie $\mathrm{LC}(g_i) = \mathrm{LC}(\tilde{g}_i) = 1$. Nun ist $g_i - \tilde{g}_i \in \boldsymbol{a}$, und da sich die Leitterme aufheben, ist dieses Polynom ein Rest bezüglich $\{\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)\} = \{\mathrm{LM}(\tilde{g}_1), \ldots, \mathrm{LM}(\tilde{g}_t)\}$. In $\boldsymbol{a}$ ist aber nur das Nullpolynom ein Rest, d.h. es folgt $g_i = \tilde{g}_i$. ❏

Der im Beweis angegebene Algorithmus zur Bestimmung reduzierter Gröbnerbasen ermöglicht eine konstruktive Überprüfung der Gleichheit von Idealen, die durch Erzeugende gegeben sind.

Korollar. *Ist $<$ eine Monomordnung für $K[X_1, \ldots, X_n]$, so gilt: Zwei Ideale in $K[X_1, \ldots X_n]$ stimmen genau dann überein, wenn ihre bezüglich der Ordnung $<$ gebildeten reduzierten Gröbnerbasen übereinstimmen.* 2/5/31

Aufgaben zum Kapitel 2

Aufgabe 2/5/010 (S: Varianten)
Matrixordnungen (1)

Index: Monomordnung, Matrixordnung

Stoffeinheiten: 2/5/8 - 2/5/16 Monomordnungen und Division mit Rest

Wir betrachten die Matrixordnungen $<_A$ und $<_B$ für Monome in $\mathbb{R}[X_1, X_2, X_3]$, die durch

$$(1)\quad A = \begin{pmatrix} 7 & 2 & 2 \\ 1 & 6 & -7 \\ -7 & -6 & 5 \end{pmatrix},$$

$$(2)\quad B = \begin{pmatrix} 1 & 6 & -7 \\ 7 & 2 & 2 \\ -7 & -6 & 5 \end{pmatrix}.$$

gegeben sind. Welche dieser Matrixordnungen ist keine Monomordnung? Finden Sie in diesem Fall ein Monom kleiner als 1.

Lösung. Offensichtlich ist $<_B$ keine Monomordnung und $X_3 <_B 1$.
Im anderen Fall liegt eine Monomordnung vor, denn die Matrix A hat den Rang 3 und enthält als ersten (von 0 verschiedenen) Eintrag in jeder Spalte eine positive Zahl.

Aufgabe 2/5/020 (S: Varianten)
Matrixordnungen (2)

Index: Monomordnung, Matrixordnung

Stoffeinheiten: 2/5/8 - 2/5/16 Monomordnungen und Division mit Rest

Wir betrachten die Monomordnung $<_A$ für $\mathbb{R}[X_1, X_2, X_3]$, die durch die Matrix

$$A = \begin{pmatrix} 1 & 6 & 6 \\ 1 & 4 & 5 \\ 0 & 0 & 2 \end{pmatrix}$$

gegeben ist. Ordnen Sie die Menge

$$M = \{X_1^2, X_1X_2, X_1X_3, X_2^2, X_2X_3, X_3^2\}$$

bezüglich $<_A$.

Lösung. Offensichtlich ist A regulär und enthält insbesondere in der ersten Zeile nur positive Einträge; daher wird durch diese Matrix tatsächlich eine Monomordnung definiert.
Für ein beliebiges Monom $q = X_1^{u_1}X_2^{u_2}X_3^{u_3}$ bilden wir $p = X_1^{v_1}X_2^{v_2}X_3^{v_3}$, wobei v_1, v_2, v_3 durch

$$(\, v_1 \; v_2 \; v_3 \,) = A \cdot \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

gegeben sind. f sei die Abbildung $q \mapsto p$ der Menge der Monome aus $\mathbb{R}[X_1, X_2, X_3]$ in sich. Sie ist bijektiv, da A regulär ist. Wir bestimmen nun die lexikographische Ordnung der Menge $N := f(M)$,

$N = \{X_1^2X_2^2, X_1^7X_2^5, X_1^{12}X_2^8, X_1^7X_2^6X_3^2, X_1^{12}X_2^9X_3^2, X_1^{12}X_2^{10}X_3^4\}$.
Das größte Monom in N ist $X_1^{12}X_2^{10}X_3^4$.

Das bedeutet, dass $X_3^2 = f^{-1}(X_1^{12}X_2^{10}X_3^4)$ das größte Monom von M bezüglich $<_A$ ist. Entsprechend erhalten wir die Anordnung aller Monome bezüglich $<_A$; es ergibt sich

$$X_3^2 > X_2X_3 > X_2^2 > X_1X_3 > X_1X_2 > X_1^2.$$

Aufgabe 2/5/040 (S: Varianten)
Gröbnerbasen (1)

Index: reduzierte Gröbnerbasis, lexikographische Ordnung, Ideal

Stoffeinheiten: 2/5/28 - 2/5/31 Reduzierte Gröbnerbasen

Bestimmen Sie (bezüglich der lexikographischen Ordnung) die reduzierte Gröbnerbasis für das Ideal in $\mathbb{R}[X_1, X_2, X_3]$, das durch die folgenden Polynome f und g,

$$f = X_1^2 + X_2^{24}X_3, \quad g = X_1X_2^3 + X_2^7X_3^{10}$$

erzeugt wird.

Lösung. Wir gehen im Wesentlichen so vor wie beim Buchberger-Algorithmus und bestimmen

$$\mathrm{S}(f,g) = X_2^3 \cdot f - X_1 \cdot g = -X_1X_2^7X_3^{10} + X_2^{27}X_3.$$

Nun ergibt sich der Rest von $\mathrm{S}(f,g)$ bei Division durch (f,g) als

$$q := X_2^{27}X_3 + X_2^{11}X_3^{20}.$$

$\mathrm{S}(f,q)$ ist bezüglich (f,q) speziell erzeugbar (vgl. Lemma 2/5/27).
Wir berechnen $\mathrm{S}(g,q)$ wie oben und sehen, dass bei Division durch (g,q) der Rest 0 auftritt, denn

$$\begin{aligned}\mathrm{S}(g,q) &= X_2^{24}X_3 \cdot g - X_1 \cdot q = -X_1X_2^{11}X_3^{20} + X_2^{31}X_3^{11} \\ &= -X_2^8X_3^{20} \cdot g + X_2^4X_3^{10} \cdot q.\end{aligned}$$

Dann ist

$$(f,g,q) = (X_1^2 + X_2^{24}X_3, X_1X_2^3 + X_2^7X_3^{10}, X_2^{27}X_3 + X_2^{11}X_3^{20})$$

eine Gröbnerbasis des von f,g erzeugten Ideals. Wir überzeugen uns leicht davon, dass diese sogar reduziert ist.

Schwerpunkte zum gewählten Stoff

- Begriff der Monomordnung, Charakterisierung und Beispiele [2/5/8 – 2/5/10]
- Leitmonome und Leitkoeffizienten bezüglich einer Monomordnung [2/5/11 – 2/5/13]
- Division mit Rest für Polynome in mehreren Unbestimmten [2/5/14 – 2/5/16]
- Existenz und Eindeutigkeit reduzierter Gröbnerbasen, Beispiele [2/5/28 – 2/5/31]

Sachverzeichnis