Skript zur Vorlesung

Gröbnerbasen

Birgit Reinert

Wintersemester 1996/97

Dieses Skript entstand als Begleitmaterial für die Vorlesung „Gröbnerbasen“, die im Wintersemester 1996/97 von der Autorin an der Universität Kaiserslautern angeboten wurde.

Gröbnerbasen, entwickelt von Bruno Buchberger für kommutative Polynomringe, finden immer häufiger Anwendung bei der Lösung algorithmischer Probleme in der Computer Algebra. Ziel der Vorlesung war es, eine Einführung in die Theorie der Gröbnerbasen zu geben. Dabei wurde sowohl die algebraische und geometrische Sicht, als auch eine Interpretation als Rewriting-Methode vorgestellt, da gerade eine Kombination dieser verschiedenen Facetten der Gröbnerbasen ihre Bedeutung für verschiedene Bereiche in Theorie und Praxis motiviert. Neben Algorithmen zur Berechnung von Gröbnerbasen wurde auf ausgewählte Anwendungen eingegangen.

Die Vorlesung wandte sich an Studenten der Informatik, Mathematik und Ingenieurwissenschaften, die sich insbesondere für Probleme in Polynomringen als Teilbereich der Computer Algebra interessieren.

Es sei darauf hingewiesen, daß dieses Skript nur „Appetit” auf das inzwischen sehr große Gebiet der Gröbnerbasen machen kann. Es stellt exemplarisch wesentliche Charakterisierungen und Anwendungen vor und soll zu eigenen weiteren Studien anregen. Weiterführende Literatur findet sich in der Bibliographie. Wesentliche Grundlage des Skriptes waren die Bücher von Cox, Little, O'Shea und Adams, Loustaunau.

Mein besonderer Dank gilt Professor Dr. Klaus Madlener, der es mir ermöglicht hat, diese Vorlesung anzubieten, für das in mich gesetzte Vertrauen. Christoph Kögl möchte ich für das geduldige Korrekturlesen danken. Weiterhin danke ich der Deutschen Forschungsgemeinschaft, deren finanzielle Unterstützung mir die Freiheit gab, mich intensiv der Forschung zu widmen und diese Vorlesung vorzubereiten. Zuletzt möchte ich auch meinen Hörern danken, deren gute Mitarbeit und genaues Lesen wesentlich zu einer Verbesserung und Abrundung des Skriptes beigetragen haben.

Dieses Skript enthält auch eine Reihe von Übungsaufgaben, die helfen sollen, den Stoff zu vertiefen. Diese Aufgaben sind am Rand mit kleinen Symbolen versehen.

◷	kennzeichnet Rechenaufgaben, die von Hand ausgeführt helfen sollen, die vorgestellten Verfahren zu vertiefen.
✓	kennzeichnet Aufgaben, in denen Beweismethoden und vorgestellte Ideen vertieft werden sollen.
☼	kennzeichnet Aufgaben, die den Horizont erweitern sollen. Solche Aufgaben verlangen bisweilen auch eigene Ideen.

Inhaltsverzeichnis

Kapitel 1

Einleitung

Wer vieles bringt, wird manchem etwas bringen.

GOETHE

Die Theorie der Gröbnerbasen wurde 1965 von Bruno Buchberger in seiner Dissertation entwickelt. Er zeichnete endliche algorithmisch bestimmbare Idealbasen in Polynomringen über Körpern aus, welche es erlauben, Fragen über die von ihnen erzeugten Ideale algorithmisch zu beantworten und insbesondere den dazugehörigen Quotientenring zu studieren. Diese Basen benannte er nach seinem Doktorvater Wolfgang Gröbner. Der Algorithmus zur Berechnung solcher Basen heißt Buchbergers Algorithmus.

1.1 Algebraische und geometrische Motivation

Im Folgenden sei $\mathbf{K}$ immer ein berechenbarer Körper[1], z.B. die rationalen Zahlen $\mathbf{Q}$ oder die reellen Zahlen $\mathbf{R}$. Mit $\mathbf{K}[x_1, \ldots, x_n]$ bezeichnen wir den (kommutativen) Polynomring über den Unbestimmten (Variablen) $x_1, \ldots, x_n$. Wenn wir in Beispielen nur eine kleine Anzahl von Variablen haben, werden wir diese auch mit x, y, z bezeichnen. Um die Elemente dieser Struktur näher zu beschreiben, benötigen wir den Begriff der **Terme** in den Unbestimmten $x_1, \ldots, x_n$

$$\mathsf{T}^n(\{x_1, \ldots, x_n\}) = \{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbf{N}\}.$$

Diese Menge werden wir, wenn die Bezeichner der zugrunde liegenden Menge der Variablen bekannt sind, auch mit T^n bezeichnen. Die Verknüpfung zweier Terme $s = x_1^{i_1} \ldots x_n^{i_n}$ und $t = x_1^{j_1} \ldots x_n^{j_n}$ aus T^n wird mit $\circ$ bezeichnet, und wir erhalten $s \circ t = x_1^{i_1+j_1} \ldots x_n^{i_n+j_n}$. Elemente aus $\mathbf{K}[x_1, \ldots, x_n]$ heißen **Polynome** und lassen sich formal als Summen der Form $f = \sum_{t \in \mathsf{T}^n} a_t \cdot t$ schreiben, wobei die Produkte $a_t \cdot t$ als

[1] Unter einem berechenbaren Körper verstehen wir einen Körper, der als Menge entscheidbar ist und für den die Addition, Subtraktion und Multiplikation aller Elemente und die Inversenbildung der Elemente ungleich der Null effektive Operationen sind.

Monome bezeichnet werden, die sogenannten Koeffizienten a_t in $\mathbf{K}$ liegen und nur endlich viele dieser Koeffizienten ungleich Null sind. In der Regel werden wir ein solches Polynom als endliche Summe $f = \sum_{i=1}^{k} a_i \cdot t_i$ schreiben. Mit der herkömmlichen formalen Addition und Multiplikation für Polynome ist $\mathbf{K}[x_1, \ldots, x_n]$ ein kommutativer Ring mit Eins. Dabei definieren wir für zwei Polynome $f = \sum_{t \in \mathsf{T}^n} a_t \cdot t$ und $g = \sum_{t \in \mathsf{T}^n} b_t \cdot t$ aus $\mathbf{K}[x_1, \ldots, x_n]$ als Addition $f + g = \sum_{t \in \mathsf{T}^n} (a_t + b_t) \cdot t$ und als Multiplikation $f * g = \sum_{t \in \mathsf{T}^n} c_t \cdot t$, mit $c_t = \sum_{s \circ r = t} a_s \cdot b_r$.

Warum sind nun Polynome eines Polynomringes von so großer Bedeutung? Um diese Frage zu beantworten, betrachten wir den affinen $\mathbf{K}$-Vektorraum der Dimension n zu unserem Körper $\mathbf{K}$, nämlich die Menge

$$\mathbf{K}^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbf{K}\}.$$

Wählt man als Körper die reellen Zahlen, so ist $\mathbf{K}^n = \mathbf{R}^n$ der herkömmliche euklidische n-dimensionale $\mathbf{K}$-Vektorraum. Wir wollen nun kurz aufzeigen, wie Polynome neben ihrer formalen Betrachtungsweise, die wir oben kennengelernt haben, als Abbildungen vom n-dimensionalen $\mathbf{K}$-Vektorraum $\mathbf{K}^n$ in den Körper $\mathbf{K}$ aufgefaßt werden können. Dazu definieren wir für ein Polynom f in $\mathbf{K}[x_1, \ldots, x_n]$ eine Auswertungsabbildung[2] $f : \mathbf{K}^n \longrightarrow \mathbf{K}$ durch

$$(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n)$$

für alle $(a_1, \ldots, a_n)$ aus $\mathbf{K}^n$. Diese zwei Facetten der Polynome, sie sowohl als formale Elemente eines Ringes in der Algebra aufzufassen, als auch als lineare Abbildungen eines $\mathbf{K}$-Vektorraumes zu interpretieren, bilden nun die Brücke zwischen algebraischen und geometrischen Fragestellungen und ermöglichen es, Lösungen von einer zur anderen Seite zu übertragen. Wir werden später noch eine weitere Sicht auf Polynome als „Regeln" zur algebraischen Simplifikation und somit eine Brücke zu Rewriting-Methoden und den dort exisiterenden Algorithmen schlagen. Verbleiben wir jedoch zunächst in der Algebra und Geometrie.

Die Fragestellung „Gilt $f = 0$?" hat nun zwei mögliche Bedeutungen. Faßt man f als formales Objekt aus $\mathbf{K}[x_1, \ldots, x_n]$ auf, so ist dies die Frage, ob f das Nullpolynom ist, also das Polynom, in dem alle Koeffizienten gleich Null sind. Interpretiert man f jedoch als Funktion, so ist dies die Frage, ob f eine Nullfunktion ist, ob also für alle Tupel $(a_1, \ldots, a_n)$ aus $\mathbf{K}^n$ $f(a_1, \ldots, a_n) = 0$ gilt. Überraschenderweise stimmen diese beiden Interpretationen der Fragestellung „Gilt $f = 0$?" im Allgemeinen nicht überein. Um dies zu sehen, nehmen wir an, $\mathbf{K}$ sei der endliche Körper bestehend aus den zwei Elementen 0 und 1. Dann ist $f = x^2 - x$ nicht das Nullpolynom in $\mathbf{K}[x]$, aber es gilt $f(0) = f(1) = 0$, d.h. f ist eine Nullfunktion.

Ist der Körper $\mathbf{K}$ hingegen unendlich, so haben wir dieses Problem nicht.

Satz 1.1.1 *Es sei $\mathbf{K}$ ein unendlicher Körper und f ein Polynom aus $\mathbf{K}[x_1, \ldots, x_n]$. Dann ist f das Nullpolynom genau dann, wenn es die Nullfunktion von $\mathbf{K}^n$ nach $\mathbf{K}$ ist.*

Beweis :
Das Nullpolynom ist sicherlich eine Nullfunktion von $\mathbf{K}^n$ nach $\mathbf{K}$. Gilt umgekehrt für

[2]Diese Abbildung ist sogar ein Homomorphismus.

alle $(a_1, \ldots, a_n)$ aus $\mathbf{K}^n$, daß $f(a_1, \ldots, a_n) = 0$, so zeigen wir unsere Behauptung durch Induktion nach der Anzahl der Variablen n. Für $n = 1$ wissen wir, daß für jedes Polynom f aus $\mathbf{K}[x]$ die Anzahl der Nullstellen durch den Grad, d.h. den größten Exponenten der Terme mit Koeffizienten ungleich Null, beschränkt ist. Da $\mathbf{K}$ unendlich ist, kann daher nicht für alle a aus $\mathbf{K}$ $f(a) = 0$ gelten, da dies einen Widerspruch ergäbe. Ist nun f aus $\mathbf{K}[x_1, \ldots, x_n]$, so können wir f auch als Objekt aus $\mathbf{K}[x_1, \ldots, x_{n-1}][x_n]$ auffassen, indem wir Polynome als Koeffizienten zulassen. Diese Polynome entstehen durch das „Aufsammeln" der jeweiligen Potenzen von x_n. Sei also $f = \sum_{i=1}^{k} g_i * x_n^i$ mit g_i aus $\mathbf{K}[x_1, \ldots, x_{n-1}]$. Indem wir nun zeigen, daß jedes g_i das Nullpolynom in $\mathbf{K}[x_1, \ldots, x_{n-1}]$ ist, erhalten wir, daß f selbst das Nullpolynom in $\mathbf{K}[x_1, \ldots, x_n]$ sein muß. Für festes $(a_1, \ldots, a_{n-1})$ aus $\mathbf{K}^{n-1}$ ist das Polynom f, ausgewertet in den Variablen $x_1, \ldots, x_n$, ein Polynom aus $\mathbf{K}[x_n]$, welches wir mit $f(a_1, \ldots, a_{n-1}, x_n)$ bezeichnen wollen. Da dieses Polynom nun für alle a_n aus $\mathbf{K}$ Null ist, muß nach der Induktionsvoraussetzung $f(a_1, \ldots, a_{n-1}, x_n)$ das Nullpolynom in $\mathbf{K}[x_n]$ sein. Weiter liefert nun

$$f(a_1, \ldots, a_{n-1}, x_n) = \sum_{i=1}^{k} g_i(a_1, \ldots, a_{n-1}) * x_n^i,$$

daß $g_i(a_1, \ldots, a_{n-1}) = 0$ für alle $1 \leq i \leq k$ und somit muß laut Induktionsvoraussetzung jedes g_i das Nullpolynom in $\mathbf{K}[x_1, \ldots, x_{n-1}]$ sein, da das Tupel $(a_1, \ldots, a_n)$ beliebig gewählt war. Also ist auch f das Nullpolynom in $\mathbf{K}[x_1, \ldots, x_n]$.

q.e.d.

Fassen wir nun ein Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$ als Funktion auf, so ist die Menge der Tupel aus $\mathbf{K}^n$, die von f auf die Null abgebildet wird, von besonderem Interesse[3]. Wir können nun zu f folgende Menge assoziieren

$$V_{\mathbf{K}}(f) = \{(a_1, \ldots, a_n) \in \mathbf{K}^n \mid f(a_1, \ldots, a_n) = 0\}$$

genannt die **Varietät** oder das **Nullstellengebilde** von f. Dieser Begriff kann wie folgt für beliebige Polynommengen F erweitert werden:

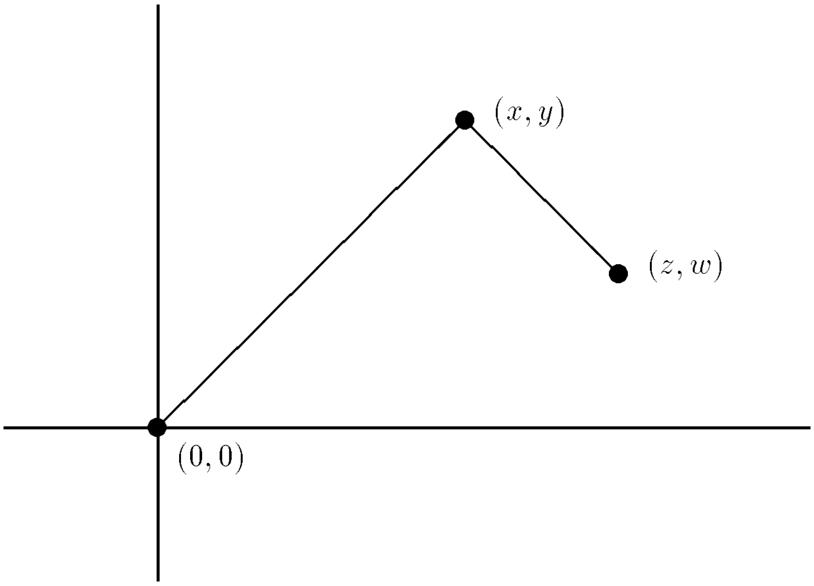
$$V_{\mathbf{K}}(F) = \{(a_1, \ldots, a_n) \in \mathbf{K}^n \mid f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in F\}.$$

Zum Beispiel beschreibt in der euklidischen Ebene die Varietät $V_{\mathbf{R}}(x^2+y^2-1, x-y^2) \subseteq \mathbf{R}^2$ gerade den Schnitt des Kreises $x^2 + y^2 = 1$ mit der Parabel $x = y^2$.

Die Bedeutung von Nullstellengebilden wird deutlich, wenn man sich folgende Anwendung überlegt:

Wir stellen uns einen Robotorarm in der Ebene vor bestehend aus zwei Teilstücken, von denen das erste doppelt so lang ist wie das zweite (vgl. Zeichnung).

[3] Diese Menge ist der Kern des von f definierten Auswertungshomomorphismus.



Der Zustand des Armes wird durch die Koordinaten (x, y) des Gelenks und (z, w) der Hand eindeutig beschrieben, und es stellt sich die Frage, welche Zustände möglich sind. Schaut man sich die Zeichnung genauer an, so können wir unsere Informationen in folgenden Gleichungen ausdrücken:

$$\begin{array}{rcl} x^2 + y^2 & = & 4 \\ (x - z)^2 + (y - w)^2 & = & 1 \end{array}$$

Dabei drückt die erste Gleichung aus, daß der Teil des Robotorarmes vom Urprung zum Gelenk zwei Einheiten lang ist und die zweite Gleichung drückt aus, daß der zweite Teil des Armes eine Einheit lang ist. Somit sind die möglichen Zustände dieses so beschriebenen Robotorarmes gerade die gemeinsamen Nullstellen dieser beiden Gleichungen (oder anders ausgedrückt der Polynome $x^2 + y^2 - 4$ und $(x - z)^2 + (y - w)^2 - 1$ aus $\mathbf{Q}[x, y, z, w]$) in $\mathbf{R}^4$.

Geometrisch gesehen beschreiben also Mengen von Polynomen Nullstellengebilde in Vektorräumen. In der Literatur finden sich zahlreiche Algorithmen, um Fragen bezüglich solcher Nullstellengebilde zu beantworten, z.B. um für ein gegebenes nichtlineares Gleichungssystem $f_1 = 0, \ldots, f_k = 0$ approximativ einzelne Lösungen zu berechnen. Wir werden später sehen, daß Gröbnerbasen nicht einzelne Lösungen bestimmen sondern vielmehr die Beschreibung des Nullstellengebildes derart „verändern", daß alle Lösungen „geschickt" bestimmt werden können. Dies passiert beispielweise auch bei der herkömmlichen Gauß-Elimination, bei der lineare Gleichungen als Einträge in einer Matrix aufgefaßt werden, die in „Dreiecksgestalt" gebracht wird. Diese neue Beschreibung erlaubt dann ein direktes „Ablesen" der Lösungen. Es geht im Wesentlichen also nun darum, eine „geeignete" Darstellung eines Nullstellengebildes zu finden. Dies wird uns mittels eines weiteren Begriffes aus der Algebra gelingen – dem des Ideals. Für eine (endliche) Menge von Polynomen $\{f_1, \ldots, f_k\}$ definieren wir

$$\langle f_1, \ldots, f_k \rangle = \{\sum_{i=1}^{k} f_i * g_i \mid g_1, \ldots, g_k \in \mathbf{K}[x_1, \ldots, x_n]\}.$$

Diese Menge ist ein **Ideal**, denn sie erfüllt folgende Bedingungen:

1. Da $0 = \sum_{i=1}^{k} f_i * 0$, liegt 0 in $\langle f_1, \ldots, f_k \rangle$.
2. Für f und g aus $\langle f_1, \ldots, f_k \rangle$ liegt auch die Summe $f + g$ in $\langle f_1, \ldots, f_k \rangle$.
3. Für f aus $\langle f_1, \ldots, f_k \rangle$ und h aus $\mathbf{K}[x_1, \ldots, x_n]$ liegt auch das Produkt $f * h$ in $\langle f_1, \ldots, f_k \rangle$.

Die Menge $\{f_1, \ldots, f_k\}$ bezeichnet man als eine **Basis** des Ideals, und ein Ideal kann natürlich ganz verschiedene Arten von Basen haben. So gilt z.B. $\langle x + y, x \rangle = \langle x, y \rangle = \langle x + xy, x^2, y^2, y + xy \rangle$, und sicherlich ist es am einfachsten, alle Elemente dieses Ideals mit Hilfe der Basis $\{x, y\}$ zu bestimmen. Die Bedeutung einer Basis $\{f_1, \ldots, f_k\}$ für ein Ideal $\mathfrak{i}$ liegt in folgender Eigenschaft begründet:

$$V_{\mathbf{K}}(\mathfrak{i}) = V_{\mathbf{K}}(f_1, \ldots, f_k).$$

Da $f_1, \ldots, f_k$ Elemente von $\mathfrak{i}$ sind folgt sofort $V_{\mathbf{K}}(\mathfrak{i}) = \{(a_1, \ldots, a_n) \in \mathbf{K}^n \mid f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in \mathfrak{i}\} \subseteq V_{\mathbf{K}}(f_1, \ldots, f_k)$. Umgekehrt läßt sich jedes f aus $\mathfrak{i}$ als Linearkombination $f = \sum_{i=1}^{k} f_i * g_i$ mit g_i aus $\mathbf{K}[x_1, \ldots, x_n]$ darstellen. Somit ist jede Nullstelle aus $V_{\mathbf{K}}(f_1, \ldots, f_k)$ auch eine Nullstelle des Polynoms f und somit auch in $V_{\mathbf{K}}(\mathfrak{i})$. Nullstellengebilde werden also durch Ideale und diese wiederum durch ihre Basen bestimmt. Später werden wir sehen, in welchem Sinne die Gröbnerbasen besonders „gute" Basen für Ideale sind.

Bisher haben wir gesehen, wie eine Menge von Polynomen ein Nullstellengebilde in einem Vektorraum beschreibt, d.h. wir haben einer algebraische Beschreibung ein geometrisches Objekt zugeordnet:

$$\mathbf{K}[x_1, \ldots, x_n] \supseteq F \longmapsto V_{\mathbf{K}}(F) \subseteq \mathbf{K}^n.$$

Umgekehrt können wir einer Teilmenge $N \subseteq \mathbf{K}^n$ wiederum wie folgt eine Menge von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$ zuordnen:

$$I(N) = \{f \mid f \in \mathbf{K}[x_1, \ldots, x_n], f(a_1, \ldots, a_n) = 0 \text{ für alle } (a_1, \ldots, a_n) \in N\}.$$

Man sieht sofort, daß die Polynommenge $I(N)$ ein Ideal in $\mathbf{K}[x_1, \ldots, x_n]$ ist, da

1. das Nullpolynom in $I(N)$ liegt,
2. für f und g aus $I(N)$ auch $f + g$ in $I(N)$ liegt und
3. für f aus $I(N)$ und h aus $\mathbf{K}[x_1, \ldots, x_n]$ auch wieder $f * h$ in $I(N)$ ist.

Somit können wir nun auch jeder Teilmenge von $\mathbf{K}^n$ eine algebraische Beschreibung zuordnen, nämlich durch die Abbildung

$$\mathbf{K}^n \supseteq N \longmapsto I(N) \subseteq \mathbf{K}[x_1, \ldots, x_n].$$

Wie hängen nun diese beiden Übergänge zwischen algebraischen und geometrischen Problembeschreibungen zusammen? Wichtig ist hier zunächst Hilberts berühmter Basissatz.

Satz 1.1.2 (Hilberts Basissatz) *Jedes Ideal in* $\mathbf{K}[x_1,\dots,x_n]$ *hat eine endliche Basis.*

Dieser fundamentale Satz impliziert nun, daß das dem Nullstellengebilde N zugeordnete Ideal $I(N)$ in $\mathbf{K}[x_1,\dots,x_n]$ eine endliche Basis hat, d.h. es existieren Polynome $f_1,\dots,f_k$ so daß $I(N)=\langle f_1,\dots,f_k\rangle$. Nun haben wir den folgenden Übergang

$$\begin{array}{ccccc} \text{Polynome} & \longrightarrow & \text{Nullstellengebilde} & \longrightarrow & \text{Ideal} \\ f_1,\dots,f_k & \longmapsto & V_{\mathbf{K}}(f_1,\dots,f_k) & \longmapsto & I(V_{\mathbf{K}}(f_1,\dots,f_k)), \end{array}$$

und es stellt sich natürlich sofort die Frage, wie sich die Ideale $\langle f_1,\dots,f_k\rangle$ und $I(V_{\mathbf{K}}(f_1,\dots,f_k))$ zueinander verhalten. Offensichtlich gilt $\langle f_1,\dots,f_k\rangle \subseteq I(V_{\mathbf{K}}(f_1,\dots,f_k))$, da für jede Linearkombination $f=\sum_{i=1}^k f_i * g_i$, wobei $g_i \in \mathbf{K}[x_1,\dots,x_n]$, gilt, $f(a_1,\dots,a_n)=0$ für alle $(a_1,\dots,a_n)$ aus $V_{\mathbf{K}}(f_1,\dots,f_k)$, und somit liegt nach Definition f in $I(V_{\mathbf{K}}(f_1,\dots,f_k))$. Die Umkehrung gilt jedoch im Allgemeinen nicht mehr, wie folgendes Beispiel zeigt: Für das Ideal $\langle x^2,y^2\rangle$ gilt $V_{\mathbf{R}}(\langle x^2,y^2\rangle)=\{(0,0)\}$, und somit sind die Polynome x und y beide in $I(V_{\mathbf{R}}(\langle x^2,y^2\rangle))$, jedoch nicht in $\langle x^2,y^2\rangle$. Wir werden später sehen, für welche Ideale $\mathfrak{i}$ dennoch $I(V_{\mathbf{K}}(\mathfrak{i}))=\mathfrak{i}$ gilt. Zum Abschluß wollen wir nun einige Probleme auflisten, für die „geeignete" Idealbasen algorithmische Lösungen bieten werden.

Problem 1:
Gegeben Polynome $f_1,\dots f_k$ und f aus $\mathbf{K}[x_1,\dots,x_n]$, entscheide, ob f in dem Ideal $\langle f_1,\dots,f_k\rangle$ liegt.

Problem 2:
Gegeben Polynome $f_1,\dots f_k$ aus $\mathbf{K}[x_1,\dots,x_n]$ und ein Polynom f aus $\langle f_1,\dots,f_k\rangle$, bestimme Polynome $g_1,\dots,g_k$ aus $\mathbf{K}[x_1,\dots,x_n]$, so daß $f=\sum_{i=1}^k f_i * g_i$ gilt.

Problem 3:
Gegeben zwei Polynome f und g aus $\mathbf{K}[x_1,\dots,x_n]$ und ein Ideal $\mathfrak{i}$. Sind die von f und g induzierten Auswertungsabbildungen eingeschränkt auf $V_{\mathbf{K}}(\mathfrak{i})$ gleich?

Es zeigt sich, daß die in Problem 3 gestellte Frage genau dann positiv zu beantworten ist, wenn die durch das Polynom $f-g$ gegebene Auswertungsabbildung eingeschränkt auf $V_{\mathbf{K}}(\mathfrak{i})$ identisch gleich Null ist, d.h. $f-g$ in $I(V_{\mathbf{K}}(\mathfrak{i}))$ liegt. Wir nennen die Polynome f und g dann auch kongruent modulo $I(V_{\mathbf{K}}(\mathfrak{i}))$.

Kongruenz modulo eines Ideales $\mathfrak{i}$ definiert eine Äquivalenzrelation auf $\mathbf{K}[x_1,\dots,x_n]$, und der Quotient $\mathbf{K}[x_1,\dots,x_n]/\mathfrak{i}$ enthält als Elemente die sogenannten Nebenklassen $f+\mathfrak{i}$. Überträgt man Addition und Multiplikation von $\mathbf{K}[x_1,\dots,x_n]$ auf $\mathbf{K}[x_1,\dots,x_n]/\mathfrak{i}$, so kann man zeigen, daß letzteres wiederum ein Ring ist, der sogenannte Quotientenring von $\mathbf{K}[x_1,\dots,x_n]$ modulo $\mathfrak{i}$. Für diesen Ring ergibt sich nun folgendes interessante Problem.

Problem 4:
Gegeben ein Ideal $\mathfrak{i}$, bestimme Repräsentanten für die Nebenklassen von $\mathbf{K}[x_1,\dots,x_n]/\mathfrak{i}$.

Ein effektives Verfahren, um eindeutige Repräsentanten zu bestimmen, ermöglicht es, im Quotientenring $\mathbf{K}[x_1,\dots,x_n]/\mathfrak{i}$ zu rechnen.

Im nächsten Abschnitt werden wir eine Methode kennenlernen, die genau das Bestimmen eindeutiger Nebenklassenrepräsentanten zum Ziel hat.

Übungen

1. Bestimmen Sie zu einem Tupel $(a_1, \ldots, a_n)$ aus $\mathbf{K}^n$ eine Polynommenge F so, daß gilt $V_{\mathbf{K}}(F) = \{(a_1, \ldots, a_n)\}$.

2. Es seien $N_1 = V_{\mathbf{K}}(\{f_1, \ldots, f_k\})$ und $N_2 = V_{\mathbf{K}}(\{g_1, \ldots, g_s\})$ zwei Nullstellengebilde in $\mathbf{K}^n$. Zeigen Sie:

   (a) $N_1 \cap N_2 = V_{\mathbf{K}}(\{f_1, \ldots, f_k, g_1, \ldots, g_s\})$.

   (b) $N_1 \cup N_2 = V_{\mathbf{K}}(\{f_i * g_j \mid 1 \leq i \leq k, 1 \leq j \leq s\})$.

   (c) $N_1 \subset N_2$ genau dann, wenn $I(N_2) \subset I(N_1)$.

   (d) $N_1 = N_2$ genau dann, wenn $I(N_1) = I(N_2)$.

3. Es sei $\mathfrak{i}$ ein Ideal und $f_1, \ldots, f_k$ eine Menge von Polynomen in $\mathbf{K}[x_1, \ldots, x_n]$. Zeigen Sie, daß folgende Aussagen äquivalent sind:

   (a) $f_1, \ldots, f_k \in \mathfrak{i}$.

   (b) $\langle f_1, \ldots, f_k \rangle \subseteq \mathfrak{i}$.

4. Der Begriff „Basis" wird in der Mathematik häufig mit verschiedenen Bedeutungen benutzt. Diese Aufgabe will den Unterschied zwischen einer „Basis eines Ideals " und einer „Basis eines Untervektorraumes" deutlich machen. Beide Begriffe werden in dieser Vorlesung benutzt werden.

   (a) Es sei $\mathfrak{i} = \langle x \rangle$ ein Ideal in $\mathbf{K}[x]$. Als Ideal hat $\mathfrak{i}$ eine Basis $\{x\}$. Faßt man $\mathfrak{i}$ als Untervektorraum von $\mathbf{K}[x]$ auf, wobei $\mathbf{K}[x]$ als $\mathbf{K}$-Vektorraum gesehen wird, so ist $\{x\}$ keine ($\mathbf{K}$-Vektorraum-) Basis[4] von $\mathfrak{i}$. Zeigen Sie, daß es keine endliche solche Basis geben kann. Hinweis: Es reicht, eine unendliche $\mathbf{K}$-Vektorraumbasis anzugeben. Es zeigt sich, daß die Möglichkeit, x mit Elementen aus $\mathbf{K}[x]$ statt nur mit Elementen aus $\mathbf{K}$ zu multiplizieren, die Existenz der endlichen Idealbasis ermöglicht.

   (b) In der linearen Algebra muß eine Basis den Unterraum erzeugen und zusätzlich linear unabhängig sein[5]. Von einer Idealbasis hingegen verlangt man nur, daß sie das Ideal erzeugt. Der Grund, warum hier keine Unabhängigkeitsbedingung mehr gefordert wird, liegt darin, daß das Zulassen von Polynomen zur Multiplikation eine solche Bedingung zunichte macht. Betrachten Sie das Ideal $\langle x, y \rangle$ in $\mathbf{K}[x, y]$. Zeigen Sie, daß man die Null als Linearkombination von x und y mit Koeffizienten ungleich Null darstellen kann.

---

[4] Z.B. läßt sich das Polynom $x^2 + x$ nicht als $\mathbf{K}$-Linearkombination $\sum_{i=1}^{n} a_i \cdot x$, $a_i \in \mathbf{K}$ schreiben.

[5] Eine Basis $b_1, \ldots, b_k$ eines $\mathbf{K}$-Vektorraumes heißt linear unabhängig, falls aus $\sum_{i=1}^{k} a_i \cdot b_i = 0$, $a_i \in \mathbf{K}$, $a_i = 0$ folgt für alle $1 \leq i \leq k$.

(c) Es sei $\{f_1, \ldots, f_k\}$ eine Basis eines Ideals $\mathfrak{i}$ in $\mathbf{K}[x_1, \ldots, x_n]$ mit $k \geq 2$ und $f_i \neq 0$, $1 \leq i \leq k$. Zeigen Sie, daß für beliebige Indizes $i \neq j$ die Null als Linearkombination der Polynome f_i, f_j mit Koeffizienten ungleich Null dargestellt werden kann.

(d) Eine Folge des Fehlens einer Unabhängigkeitsbedingung ist, daß in einer Darstellung eines Polynomes f aus $\langle f_1, \ldots, f_k \rangle$ als Linearkombination $f = \sum_{i=1}^{k} h_i * f_i$ die Elemente $h_i \in \mathbf{K}[x_1, \ldots, x_n]$ nicht mehr eindeutig sind. Betrachten Sie hierzu $f = x^2 + xy + y^2 \in \langle x, y \rangle$.

(e) Eine Basis eines Ideals heißt minimal, falls sie keine echte Teilmenge enthält, die bereits alleine das Ideal erzeugt. Zum Beispiel ist $\{x, x^2\}$ eine Idealbasis, welche nicht minimal ist, da bereits $\{x\}$ dasselbe Ideal erzeugt. Leider kann ein Ideal mehrere verschiedene minimale Basen haben. Betrachten Sie hierzu das von der Menge $\{x, x^2 + x, x^2\}$ erzeugte Ideal und zeigen Sie, daß die Mengen $\{x\}$ und $\{x^2 + x, x^2\}$ beides minimale Basen dieses Ideals sind.

1.2 Die Idee der algebraischen Simplifikation

Die Idee der algebraischen Simplifikation spielt eine zentrale Rolle in der Computer-Algebra. Ziel ist es, Objekte einer algebraischen Struktur in äquivalente, „einfachere" Elemente umzuformen und somit gewisse Elemente als Repräsentanten auszuzeichnen. Angestrebt wird dabei die effektive Berechnung eindeutiger Repräsentanten äquivalenter Objekte. Dieser Prozeß wird in der Literatur häufig mit kanonischer Simplifikation bezeichnet. Er spielt eine wichtige Rolle, da er eng verknüpft ist mit dem effektiven Rechnen in algebraischen Strukturen und der Entscheidung des Kongruenzproblems.

Erfolgreich eingesetzt wird die Technik der algebraischen Simplifikation z.B. bei der Darstellung von Monoiden und Gruppen durch sogenannte Wortersetzungssysteme oder Semi-Thue-Systeme. Solche Wortersetzungssyteme können durch den sogenannten Knuth-Bendix-Algorithmus „vervollständigt" werden.

In dieser Vorlesung wollen wir ein weiteres Feld aufzeigen, in dem die Idee algebraischer Simplifikationsmethoden Anwendung gefunden hat — Polynomringe über Körpern. In diesem Zusammenhang sind Gröbnerbasen gerade solche endlichen Idealbasen bezüglich derer ein kanonischer Simplifikationsprozeß möglich ist. Dabei wird ein Polynom p mit einem anderen Polynom f simplifiziert (oft auch reduziert genannt), falls ein geeignetes Monomvielfaches von f benutzt werden kann, um p durch Subtraktion zu verkleinern (bezüglich einer sogenannten zulässigen Ordnung). Benutzt man in diesem Simplifikationsprozeß nun Elemente einer Gröbnerbasis eines Ideals, so erhält man eindeutige Repräsentanten bezüglich der Idealkongruenz, und der Repräsentant der Idealelemente ist die Null. Kanonische Simplifikation mit Gröbnerbasen wird in der Praxis benutzt, um die idealtheoretischen Probleme, welche in vorherigen Abschnitt vorgestellt wurden, zu lösen.

Um für später das benötigte Vokabular zu haben, soll nun hier kurz eine Definition von Reduktionssystemen und ihrer Eigenschaften vorgestellt werden. Es sei $\mathcal{E}$ eine

Menge von Elementen und $\longrightarrow$ eine binäre Relation auf $\mathcal{E}$, die wir **Reduktion** nennen werden. Für Elemente a und b aus $\mathcal{E}$ schreiben wir $a \longrightarrow b$ genau dann, wenn das Paar (a, b) in der Relation $\longrightarrow$ enthalten ist. Ein Paar $(\mathcal{E}, \longrightarrow)$ heißt Reduktionssystem. Die binäre Relation $\longrightarrow$ kann nun wie folgt fortgesetzt werden:

$\xrightarrow{0}$		steht für die Identität auf $\mathcal{E}$,
$\longleftarrow$		steht für die inverse Relation von $\longrightarrow$,
$\xrightarrow{n+1}$:=	$\xrightarrow{n} \circ \longrightarrow$	wobei $\circ$ für die Komposition von Relationen steht, $n \in \mathbf{N}$,
$\xrightarrow{\leq n}$:=	$\bigcup_{0 \leq i \leq n} \xrightarrow{i}$,	
$\xrightarrow{+}$:=	$\bigcup_{n>0} \xrightarrow{n}$	steht für die transitive Hülle von $\longrightarrow$,
$\xrightarrow{*}$:=	$\xrightarrow{+} \cup \xrightarrow{0}$	steht für die reflexive transitive Hülle von $\longrightarrow$,
$\longleftrightarrow$:=	$\longleftarrow \cup \longrightarrow$	steht für die symmetrische Hülle von $\longrightarrow$,
$\xleftrightarrow{+}$		steht für die symmetrisch transitive Hülle von $\longrightarrow$,
$\xleftrightarrow{*}$		steht für die reflexive symmetrisch transitive Hülle von $\longrightarrow$.

Assoziiert zu solch einem Reduktionssytem ist das sogenannte **Wortproblem**, d.h. entscheide zu gegebenen Elementen a und b aus $\mathcal{E}$, ob sie „äquivalent" sind bezüglich $\xleftrightarrow{*}$, also ob $a \xleftrightarrow{*} b$ gilt. Es ist bekannt, daß dieses Problem für manche Reduktionssysteme unentscheidbar ist. Wichtig für unser weiteres Vorgehen sind jedoch Eigenschaften, die garantieren, daß ein Reduktionssystem entscheidbares Wortproblem hat, denn wir werden später sehen, daß das Kongruenzproblem für ein Ideal gerade solch einem Wortproblem entspricht.

Zuerst müssen wir ein paar weitere Begriffe einführen. Ein Element a aus $\mathcal{E}$ heißt **reduzibel** (bezüglich $\longrightarrow$), falls es ein b aus $\mathcal{E}$ gibt, so daß (a, b) in $\longrightarrow$ liegt, im folgenden geschrieben als $a \longrightarrow b$. Alle Elemente b, für die nun $a \xrightarrow{*} b$ gilt, heißen Nachfolger von a und, falls sogar $a \xrightarrow{+} b$ gilt, echte Nachfolger. Ein Element ohne echten Nachfolger nennen wir **irreduzibel**. Gilt nun $a \xrightarrow{*} b$ und b ist irreduzibel, so wird b als **Normalform** von a bezeichnet, wobei a keine, eine oder mehrere verschiedene Normalformen haben kann.

Definition 1.2.1 *Ein Reduktionssystem* $(\mathcal{E}, \longrightarrow)$ *heißt* **noethersch** *oder* **terminierend***, falls es keine unendlichen Ketten der Form* $a_0 \longrightarrow a_1 \longrightarrow a_2 \longrightarrow \ldots$ *mit* a_i *aus* $\mathcal{E}$*,* i *aus* $\mathbf{N}$ *gibt.*

Somit hat in einem noetherschen Reduktionssystem jedes Element mindestens eine Normalform, die jedoch noch nicht eindeutig sein muß.

Definition 1.2.2 *Ein Reduktionssystem* $(\mathcal{E}, \longrightarrow)$ *heißt* **konfluent***, falls für alle* a, a_1, a_2 *in* $\mathcal{E}$ $a \xrightarrow{*} a_1$ *und* $a \xrightarrow{*} a_2$ *die Existenz eines* a_3 *in* $\mathcal{E}$ *impliziert mit* $a_1 \xrightarrow{*} a_3$ *und* $a_2 \xrightarrow{*} a_3$.

In konfluenten Reduktionssystemen sind also Normalformen, falls sie existieren, eindeutig. Kombiniert man nun Konfluenz und Terminierung, so hat man eine hinreichende Bedingung für die Existenz eindeutiger Normalformen.

Definition 1.2.3 *Ein Reduktionssystem* $(\mathcal{E}, \longrightarrow)$ *heißt* **vollständig***, falls es konfluent und terminierend ist.*

Vollständige Reduktionssysteme mit effektiver Reduktionsrelation $\longrightarrow$ erlauben nunmehr die Lösung des Wortproblems durch Berechnen der eindeutigen Normalformen und deren Vergleich. Leider ist im Allgemeinen nicht zu erwarten, daß ein Reduktionssystem vollständig ist, und schlimmer noch, Konfluenz und Terminierung sind unentscheidbare Eigenschaften. Daher wollen wir im Folgenden schwächere Kriterien vorstellen, die Vollständigkeit garantieren.

Definition 1.2.4 *Ein Reduktionssytem* $(\mathcal{E}, \longrightarrow)$ *heißt* **lokal konfluent***, falls für alle* a, a_1, a_2 *in* $\mathcal{E}$ $a \longrightarrow a_1$ *und* $a \longrightarrow a_2$ *die Existenz eines* a_3 *in* $\mathcal{E}$ *impliziert mit* $a_1 \stackrel{*}{\longrightarrow} a_3$ *und* $a_2 \stackrel{*}{\longrightarrow} a_3$*.*

Das Lemma von Newmann zeigt, daß für terminierende Reduktionssysteme die Eigenschaften Konfluenz und lokale Konfluenz äquivalent sind.

Lemma 1.2.5 (Lemma von Newmann) *Es sei* $(\mathcal{E}, \longrightarrow)$ *ein noethersches Reduktionssystem. Dann ist* $(\mathcal{E}, \longrightarrow)$ *genau dann konfluent, wenn es lokal konfluent ist.*

Somit kann für terminierende Reduktionssysteme ein Konfluenztest auf einen Test für lokale Konfluenz reduziert werden. Es bleibt, hinreichende Bedingungen für die Terminierung eines Reduktionssystems zu geben.

Definition 1.2.6 *Eine binäre Relation* $\succeq$ *auf einer Menge* $\mathcal{M}$ *ist eine* **Partialordnung***, falls für* a, b *und* c *aus* $\mathcal{M}$ *folgendes gilt:*

1. $\succeq$ *ist reflexiv, d.h.* $a \succeq a$*,*
2. $\succeq$ *ist transitiv, d.h.* $a \succeq b$ *und* $b \succeq c$ *implizieren* $a \succeq c$*,*
3. $\succeq$ *ist anti-symmetrisch, d.h.* $a \succeq b$ *und* $b \succeq a$ *implizieren* $a = b$*.*

Eine Partialordnung heißt **total**, falls für a und b aus $\mathcal{M}$ immer entweder $a \succeq b$ oder $b \succeq a$ gilt. Mit $\succ$ bezeichnen wir den irreflexiv transitiven Teil von $\succeq$, d.h. $a \succ b$ genau dann wenn $a \succeq b$ und $a \neq b$. Eine Partialordnung $\succeq$ heißt **wohlfundiert**, falls die korrespondierende Ordnung $\succ$ keine unendlichen Ketten der Form $a_0 \succ a_1 \succ a_2 \succ \ldots$ zuläßt, wobei a_i aus $\mathcal{M}$ und i aus $\mathbf{N}$. Mit Hilfe solcher wohlfundierten Ordnungen können wir nun ein hinreichendes Kriterium für die Terminierung eines Reduktionssystems geben.

Lemma 1.2.7 *Es sei* $(\mathcal{E}, \longrightarrow)$ *ein Reduktionssystem und* $\succeq$ *eine wohlfundierte Partialordnung auf* $\mathcal{E}$ *mit* $\longrightarrow \subseteq \succ$*. Dann ist* $(\mathcal{E}, \longrightarrow)$ *noethersch.*

Wir werden später sehen, daß Gröbnerbasen gerade als „Vervollständigung" eines terminierenden Reduktionssystems über $\mathbf{K}[x_1, \ldots, x_n]$ durch das Auflösen nicht lokal konfluenter Situationen entstehen.

1.3 Gauß-Elimination für lineare Gleichungssysteme

In diesem Abschnitt wollen wir uns mit Nullstellengebilden von linearen Gleichungssystemen beschäftigen, d.h. von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$ der Gestalt $f = \sum_{i=1}^n a_i \cdot x_i + a_{n+1}$ mit a_i aus $\mathbf{K}$. Die Idee, solche Nullstellengebilde algorithmisch zu behandeln, basiert darauf, zu einem linearen Gleichungssystem eine Matrix zu assoziieren, die in Dreiecksgestalt transformiert wird.

Als Beispiel betrachten wir zwei Polynome $f_1 = x + y - z$ und $f_2 = 2 \cdot x + 3 \cdot y + 2 \cdot z$ aus $\mathbf{Q}[x, y, z]$. Das von diesen Polynomen bestimmte Nullstellengebilde $V_{\mathbf{Q}}(f_1, f_2)$ sind genau die Lösungsmenge des Gleichungssystems

$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 0 \\ 2 \cdot x & + & 3 \cdot y & + & 2 \cdot z & = & 0 \end{array}$$

Die dazugehörige Matrix läßt sich durch eine einfache Zeilenoperation auf Dreiecksgestalt bringen, nämlich

$$\begin{pmatrix} 1 & 1 & -1 & 0 \\ 2 & 3 & 2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 4 & 0 \end{pmatrix}$$

Somit wird unser Nullstellengebilde auch von folgendem Gleichungssystem beschrieben

$$\begin{array}{rcrcrcl} x & + & y & - & z & = & 0 \\ & & y & + & 4 \cdot z & = & 0 \end{array}$$

welches die Nullstellen $x = 5 \cdot z$ und $y = -4 \cdot z$ für alle z aus $\mathbf{Q}$ hat.

Eigentlich sind die Zeilenoperationen auf der zu einem Gleichungssystem $f_1, \ldots, f_k$ assoziierten Matrix nichts anderes als Änderungen an der Basis des Ideals $\langle f_1, \ldots, f_k \rangle$. So wird in unserem Beispiel das Polynom f_2 durch $f_2 - 2 \cdot f_1 = y + 4 \cdot z =: f_3 \in \langle f_1, f_2 \rangle$ ersetzt. Dies ändert nicht das erzeugte Ideal, da auch $f_2 = 2 \cdot f_1 + f_3 \in \langle f_1, f_3 \rangle$ und somit $\langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$. Eine solche Änderung der Basis eines Ideals kann durch einen Reduktionsbegriff ausgedrückt werden. Dazu nehmen wir an, daß die Variablen des Polynomringes wie folgt „geordnet" sind: $x_1 > \ldots > x_n > 1$. Für ein Polynom $f = \sum_{i=1}^k a_i \cdot x_i + a_{n+1}$ bezeichnen wir für den kleinsten Index j mit $a_j \neq 0$ $\mathsf{HM}(f) = a_j \cdot x_j$ als den **Kopf** oder das **Kopfmonom**, $\mathsf{HC}(f) = a_j$ als den **Kopfkoeffizienten** und $\mathsf{HT}(f) = x_j$ als den **Kopfterm**. Falls $\mathsf{HM}(f) = a_{n+1}$, so definieren wir $\mathsf{HT}(f) = 1$.

Definition 1.3.1 *Es seien f und g zwei lineare Polynome aus $\mathbf{K}[x_1, \ldots, x_n]$. Wir sagen g reduziert f, falls $\mathsf{HT}(f) = \mathsf{HT}(g)$. Wir schreiben dann $f \longrightarrow_g f - (\mathsf{HC}(f) \cdot \mathsf{HC}(g)^{-1}) \cdot g$.*

In unserem Beispiel gilt also $f_2 = 2 \cdot x + 3 \cdot y + 2 \cdot z \longrightarrow_{f_1 = x+y-z} y + 4 \cdot z$.

Reduktion eines Polynoms mit einem anderen eliminiert also das Vorkommen des Kopfterms in dem reduzierten Polynom. Da wir Polynome über einem Körper betrachten, ist die Definition von Reduktion in diesem Falle symmetrisch, d.h. wenn f ein Polynom g reduziert, so reduziert auch g das Polynom f. Ein Reduktionsschritt entspricht genau einer Zeilenoperation in dem oben vorgestellten Lösungsverfahren mittels Matrizen. In diesem Zusammenhang kann nun in Abhängigkeit von der auf den Variablen definierten Ordnung ein Algorithmus für Gauß-Elimination basierend auf Reduktion angegeben werden.

Gauss-Elimination mit Reduktion

Eingabe: Eine endliche Menge linearer Polynome F aus $\mathbf{K}[x_1, \ldots, x_n]$.
Ausgabe: Eine endliche Menge von Polynomen G mit $V(F) = V(G)$, und zu jeder Variablen $x_1, \ldots, x_n$ gibt es maximal ein Polynom in G, dessen größte Variable x_i ist, und G enthält maximal ein konstantes Polynom.

$G := F$;
while es gibt $f, g \in G$ mit $\mathsf{HT}(f) = \mathsf{HT}(g)$ **do**
  ersetze f durch $f - (\mathsf{HC}(f) \cdot \mathsf{HC}(g)^{-1}) \cdot g$ in G;
endwhile

Falls dieser Algorithmus terminiert, folgt die Korrektheit sofort, da dann die Menge G keine zwei Polynome mit gleichem Kopfterm mehr enthält. Um zu sehen, daß der Algorithmus terminiert, muß man sich den Reduktionsprozeß etwas genauer anschauen. Reduktion eines Polynoms f mit einem Polynom g läßt den Kopfterm von f kleiner werden, da durch die Subtraktion des entsprechenden $\mathbf{K}$-Vielfachen von g der Kopfterm von F eliminiert wird und nur kleinere Terme zu f hinzugefügt und bereits vorhandene modifiziert werden können. Da es jedoch nur endlich viele Variablen gibt, kann jedes Polynom in G maximal $n+1$-mal reduziert werden.

Eine solche durch Reduktion bestimmte Polynommenge G hat nun wichtige Eigenschaften, die es uns erlauben, die in Abschnitt 1.1 formulierten Probleme zu lösen, sofern G kein konstantes Polynom enthält. In diesem Spezialfall ist das beschriebene Nullstellengebilde nämlich leer und somit kann man die Probleme direkt beantworten. O.B.d.A nehmen wir also an G enthalte kein konstantes Polynom. Problem 1 ist dann die Frage, ob sich ein beliebiges lineares Polynom als $\mathbf{K}$-Linearkombination der Elemente in G darstellen läßt. Diese Frage läßt sich lösen, indem man testet, ob ein Polynom sich mit den Polynomen aus G zu Null reduzieren läßt. Summiert man die bei einer solchen Reduktionskette nach Null auftretenden Polynomvielfachen auf, so erhält man eine Darstellung des reduzierten Polynoms als Linearkombination von Polynomen aus G mit Multiplikatoren aus $\mathbf{K}$ wie in Problem 2 gefordert. Es ist zu beachten, daß auf Grund der besonderen Form der Polynome in G eine Reduktionskette jedes Polynom maximal einmal benutzen kann, d.h. wir haben als Schranke für die Länge von Reduktionsketten $|G| \leq n+1$. Die Frage, ob zwei lineare Polynome f und g kongruent sind bezüglich des von G beschriebenen Nullstellengebildes, läßt sich durch Reduktion der Differenz $f-g$ mit G beantworten. Erhalten wir die Null, so sind die beiden Polynome kongruent (Problem 3). Um für das Rechnen im Quotientenring (Problem 4) eindeutige Repräsentanten der Nebenklassen zu erhalten, erweitern wir den Begriff der Reduktion etwas: f ist mit g reduzibel, falls die Variable $\mathsf{HT}(g)$ im Polynom f vorkommt. Reduktion bedeutet dann Elimination dieses Vorkommens in f durch Subtraktion eines geeigneten $\mathbf{K}$-Vielfachen von g. Als Normalform eines Polynoms f bezüglich eine Polynommenge G bezeichnet man dann ein Polynom, welches durch eine Reduktionskette mit Polynomen aus G berechnet werden kann und welches selbst nicht mehr bezüglich G reduzibel ist. Hat G die Eigenschaften, die im obigen Algorithmus spezifiziert wurden, so sind solche Normalformen eindeutig und können als Repräsentanten zum Rechnen im Quotientenring benutzt werden.

Übungen

1. Führen Sie das hier vorgestellte Verfahren für die Polynome $f_1 = y - z$, $f_2 = x + 2 \cdot y + 3 \cdot z$ und $f_3 = 3 \cdot x - 4 \cdot y + 2 \cdot z$ aus $\mathbf{Q}[x, y, z]$ durch.

1.4 Euklids Algorithmus – Eine Lösung für $\mathbf{K}[x]$

Vielfach werden Buchbergers Ideen auch als Verallgemeinerung des euklidischen Algorithmus von $\mathbf{K}[x]$ zu $\mathbf{K}[x_1, \ldots, x_n]$ vorgestellt. Daher soll hier kurz auf diesen Spezialfall eingegangen werden, nicht zuletzt, um eine weitere Idee einer Definition von Reduktion aufzuzeigen. Wir werden Ideale in $\mathbf{K}[x]$ charakterisieren und zeigen, wie die in Abschnitt 1.1 vorgestellten Probleme sich mittels Reduktion lösen lassen.

Ein Polynom f aus $\mathbf{K}[x]\backslash\{0\}$ schreiben wir als $f = \sum_{i=0}^{d} a_i \cdot x^i$ mit $a_i \in \mathbf{K}$, $d \in \mathbf{N}$ und $a_d \neq 0$. Wir bezeichnen d als den **Grad** von f, auch geschrieben als $\mathsf{grad}(f)$. Das Monom $\mathsf{HM}(f) = a_d \cdot x^d$ ist der Kopf, $\mathsf{HC}(f) = a_d$ der führende Koeffizient, $\mathsf{HT}(f) = x^d$ der führende Term und $\mathsf{RED}(f) = \sum_{i=0}^{d-1} a_i \cdot x^i$ der Rest von f. Für das Nullpolynom[6] gilt $\mathsf{HM}(0) = \mathsf{HC}(0) = \mathsf{RED}(0) = \mathsf{grad}(0) = 0$ und $\mathsf{HT}(0) = x^0 = 1$. Zum Beispiel gilt für das Polynom $f = 3 \cdot x^4 + 5 \cdot x + 2$, $\mathsf{grad}(f) = 4$, $\mathsf{HM}(f) = 3 \cdot x^4$, $\mathsf{HC}(f) = 3$, $\mathsf{HT}(f) = x^4$ und $\mathsf{RED}(f) = 5 \cdot x + 2$. Eine wichtige Beobachtung ist, daß für Polynome f und g aus $\mathbf{K}[x]\backslash\{0\}$ gilt

$$\mathsf{grad}(f) \leq \mathsf{grad}(g) \text{ genau dann, wenn } \mathsf{HT}(f) \text{ teilt } \mathsf{HT}(g).$$

Dieser Sachverhalt motiviert als Kernstück des euklidischen Algorithmus folgenden Satz, der die Division mit Rest von Polynomen charakterisiert.

Satz 1.4.1 *Es sei g ein Polynom aus $\mathbf{K}[x]\backslash\{0\}$. Dann läßt sich jedes Polynom f aus $\mathbf{K}[x]$ schreiben als $f = g * q + r$ mit $q, r \in \mathbf{K}[x]$ und $r = 0$ oder $\mathsf{grad}(r) < \mathsf{grad}(g)$. Die Polynome q und r sind hierbei eindeutig bestimmt.*

Ein wichtiges Korollar dieses Satzes, welches wir schon benutzt haben, beschäftigt sich mit der Anzahl der Nullstellen eines Polynoms aus $\mathbf{K}[x]$.

[6] Eigentlich müßte man zwischen dem Nullpolynom und der Null in $\mathbf{K}$ formal unterscheiden, aber es wird davon ausgegangen, daß der Leser dies automatisch tut.

Korollar 1.4.2 *Ein Polynom f aus $\mathbf{K}[x]\backslash\{0\}$ hat maximal $\mathsf{grad}(f)$ Nullstellen.*

Polynomdivision soll nun einem Beispiel vorgestellt werden. Es seien $f = x^3 + 7\cdot x^2 + 11\cdot x + 8$ und $g = x + 5$ zwei Polynome in $\mathbf{Q}[x]$. Division von f mit g ergibt dann $x^2 + 2\cdot x + 1$ Rest 3 und kann wie folgt ausgeführt werden:

$$\begin{array}{rrcrcrcrcccccc}
 & x^3 & + & 7\cdot x^2 & + & 11\cdot x & + & 8 & : & x+5 & = & x^2 & & \\
- & (x^3 & + & 5\cdot x^2) & & & & & & & & & & \\ \cline{1-4}
 & & & 2\cdot x^2 & + & 11\cdot x & + & 8 & & & & & +\,2\cdot x & \\
 & & - & (2\cdot x^2 & + & 10\cdot x) & & & & & & & & \\ \cline{3-6}
 & & & & & x & + & 8 & & & & & & +\,1 \\
 & & & & - & (x & + & 5) & & & & & & \\ \cline{5-8}
 & & & & & & & 3 & & & & & &
\end{array}$$

Dieses Vorgehen kann nun als Reduktion aufgefaßt werden, indem man ein Polynom f als Regel $\mathsf{HM}(f) \longrightarrow -\mathsf{RED}(f)$ beschreibt und über die Anwendbarkeit der Regel eine Reduktionsrelation auf dem Polynomring erhält. Da wir für das entstehende Reduktionssystem im ersten Schritt Terminierung (und später auch lokale Konfluenz) erreichen wollen, werden wir eine wohlfundierte Partialordnung auf Polynomen einführen, in der die Reduktionsrelation enthalten sein wird. Für den Spezialfall $\mathbf{K}[x]$ benutzen wir die durch den Grad der Polynome induzierte Gradordnung.

Definition 1.4.3 *Für zwei verschiedene Polynome f und g aus $\mathbf{K}[x]$ schreiben wir $f > g$ genau dann, wenn $\mathsf{grad}(f) > \mathsf{grad}(g)$ und $g > f$ genau dann, wenn $\mathsf{grad}(g) > \mathsf{grad}(f)$. Sonst heißen f und g unvergleichbar.*

Im Folgenden wollen wir skizzieren, wie von einem Polynom g ein noethersches Reduktionssystem induziert wird. Zu jedem Polynom f aus $\mathbf{K}[x]$ mit $\mathsf{grad}(f) \geq \mathsf{grad}(g)$ assozieren wir ein Paar $(f, f - (\mathsf{HC}(f)\cdot\mathsf{HC}(g)^{-1})\cdot g * x^{\mathsf{grad}(f)-\mathsf{grad}(g)})$. Es hat sich als einfacher erwiesen, Reduktionssysteme nicht durch die gesamte Reduktionsrelation, sondern durch eine Menge von Regeln und die Beschreibung ihrer Anwendung anzugeben. Für den Polynomring $\mathbf{K}[x]$ sind diese Regeln gerade wieder Polynome, die wie folgt zur Reduktion benutzt werden dürfen.

Definition 1.4.4 *Für zwei Polynome f und g aus $\mathbf{K}[x]\backslash\{0\}$ gilt: g reduziert f genau dann, wenn $\mathsf{grad}(g) \leq \mathsf{grad}(f)$. Wir erhalten die Reduktion $f \longrightarrow_g f - (\mathsf{HC}(f)\cdot\mathsf{HC}(g)^{-1})\cdot g * x^{\mathsf{grad}(f)-\mathsf{grad}(g)}$.*

Es gibt eine Fülle von Möglichkeiten, Reduktion in einem Polynomring zu definieren. So kann man die Stelle, an der reduziert wird (in unserer Definition ist dies der Kopf des Polynoms f), variieren, oder man kann mehrere Polynome zur Reduktion zulassen. Hier wurde die Kopfreduktion deshalb gewählt, weil mit ihr die im vorherigen Beispiel vorgestellte Polynomdivision modelliert werden kann. Es gilt nämlich für unsere

Polynome $f = x^3 + 7 \cdot x^2 + 11 \cdot x + 8$ und $g = x + 5$,

$$f \longrightarrow_g 2 \cdot x^2 + 11 \cdot x + 8 \longrightarrow_g x + 8 \longrightarrow_g 3.$$

Dieser Reduktionsprozeß liefert offensichtlich den Rest der Division von f durch g. Sammelt man die in den einzelnen Schritten benutzten Multiplikanten von g auf, so erhält man x^2, $2 \cdot x$ und 1, welche aufsummiert gerade den Teiler $x^2 + 2 \cdot x + 1$ ergeben. Somit kann unser Reduktionsprozeß wie folgt in einen Algorithmus verwandelt werden, der Teiler und Rest eines Polynoms berechnet:

NORMALFORM IN $\mathbf{K}[x]$

Eingabe: f und g aus $\mathbf{K}[x]$ mit g nicht gleich Null.
Ausgabe: Der Rest r, wobei $f = q * g + r$ und $r = 0$ oder $\mathsf{grad}(r) < \mathsf{grad}(g)$.

$q := 0$;
$r := f$;
while $\mathsf{grad}(g) \leq \mathsf{grad}(r)$ **do**
  $r := r - (\mathsf{HC}(r) \cdot \mathsf{HC}(g)^{-1}) \cdot g * x^{\mathsf{grad}(r) - \mathsf{grad}(g)}$;
  % Reduziere r mit g, d.h. $r \longrightarrow_g$
  $q := q + (\mathsf{HC}(r) \cdot \mathsf{HC}(g)^{-1}) \cdot x^{\mathsf{grad}(r) - \mathsf{grad}(g)}$;
  % dies ist für die Normalformbestimmung überflüssig, zeigt jedoch, wie man diesen Prozeß
  % benutzen kann, um den Teiler zu bestimmen.
endwhile

Eine weitere wichtige Eigenschaft von Reduktion erlaubt es, sie zur Transformation von Idealbasen einzusetzen. Für ein Ideal $\mathfrak{i} = \langle f, g \rangle$ und ein Polynom h mit $f \longrightarrow_g h$ gilt nämlich auch $\mathfrak{i} = \langle h, g \rangle$. Da für je zwei Polynome f und g, welche beide nicht gleich Null sind, immer $\mathsf{grad}(f) \leq \mathsf{grad}(g)$ oder $\mathsf{grad}(g) \leq \mathsf{grad}(f)$ gilt, muß immer eines mit dem anderen reduzibel sein. Diese Idee liegt dem Ergebnis folgenden Satzes zugrunde.

Satz 1.4.5 *In $\mathbf{K}[x]$ wird jedes Ideal von genau einem Element erzeugt.*

Beweis :
Es sei $\mathfrak{i}$ ein nicht-triviales Ideal in $\mathbf{K}[x]$. Wir wählen g aus $\mathfrak{i} \backslash \{0\}$ so, daß der Grad $n = \mathsf{grad}(g)$ minimal unter allen Elementen des Ideals ist. Somit läßt sich nach Satz 1.4.1 jedes weitere Polynom f aus $\mathfrak{i}$ schreiben als $f = q * g + r$, wobei $r = 0$ gelten muß, da $\mathsf{grad}(r) < \mathsf{grad}(g) = n$ wegen $r \in \mathfrak{i}$ und der Wahl von n minimal nicht möglich ist. Dies impliziert aber $f = q * g$ und daher $\mathfrak{i} \subseteq \langle g \rangle$. Da die Umkehrung auch gilt, folgt die Behauptung.

q.e.d.

Der Beweis dieses Satzes ist natürlich nicht konstruktiv, da er das Auswahlaxiom für die Wahl von g benutzt. Im Folgenden werden wir nun sehen wie, ausgehend von einer Basis des Ideals, ein geeignetes g berechnet werden kann. Um dies zu tun, benötigen wir den Begriff des größten gemeinsamen Teilers zweier (und später mehrerer) Polynome.

Definition 1.4.6 *Es seien f und g zwei Polynome aus $\mathbf{K}[x]$, von denen eines ungleich Null ist. Als* **größten gemeinsamen Teiler** *bezeichnen wir ein Polynom $h = \mathsf{ggT}(f, g)$ mit folgenden Eigenschaften:*

1. *h teilt echt f und g, d.h. die Teilung erfolgt mit Rest Null.*
2. *Jedes weitere Polynom, welches f und g echt teilt, teilt auch h echt.*
3. *h ist monisch, d.h. $\mathsf{HC}(h) = 1$.*

Der größte gemeinsame Teiler zweier Polynome ist eindeutig und wir kennen aus der linearen Algebra folgenden Satz, den wir hier nicht beweisen wollen.

Satz 1.4.7 *Es seien f und g zwei Polynome aus $\mathbf{K}[x]$, von denen eines ungleich Null ist. Dann existiert der größte gemeinsame Teiler von f und g, und es gelten folgende Aussagen:*

1. $\langle f, g\rangle = \langle \mathsf{ggT}(f, g)\rangle$.
2. $\mathsf{ggT}(f, g) = \mathsf{ggT}(f - g * h, g)$ *ein weiteres Polynom $h \in \mathbf{K}[x]$.*

Die zweite Aussage kann mit unserer Definition von Reduktion verknüpft werden. Gilt nämlich $f \longrightarrow_g h$, so folgt $\mathsf{ggT}(f, g) = \mathsf{ggT}(h, g)$. Wir sehen sofort, daß daher unsere Reduktion eingesetzt werden kann, um Euklids Algorithmus zu modellieren.

EUKLIDS ALGORITHMUS MIT REDUKTION

Eingabe: f und g aus $\mathbf{K}[x]$ mit f nicht gleich Null.
Ausgabe: $h = \mathsf{ggT}(f, g)$, der größte gemeinsame Teiler von f und g.

$h := \mathsf{HC}(f)^{-1} \cdot f$;
$p := g$;
while $p \neq 0$ **do**
  $r :=$ NORMALFORM(h, p);
  $h := \mathsf{HC}(p)^{-1} \cdot p$;
  $p := r$;
endwhile

In unserem Beispiel von oben erhalten wir für die Eingabe von $f = x^3 + 7 \cdot x^2 + 11 \cdot x + 8$ und $g = x + 5$ folgenden Ablauf:

$h := x^3 + 7 \cdot x^2 + 11 \cdot x + 8$;
$p := x + 5$;
da $p \neq 0$ gilt, berechnen wir in einem ersten Durchlauf der Schleife
  $r :=$ NORMALFORM$(x^3 + 7 \cdot x^2 + 11 \cdot x + 8, x + 5) = 3$;
  $h := x + 5$;

$p := 3;$
da noch immer $p \neq 0$ gilt, berechnen wir
$r :=$ NORMALFORM$(x + 5, 3) = 0;$
$h := 1;$
$p := 0;$
und da nun $p = 0$ gilt, hält der Algorithmus mit Ergebnis $\mathsf{ggT}(f, g) = h = 1$.

Diese Aussagen über Ideale, die ursprünglich durch eine Basis mit zwei Polynomen beschrieben wurden, lassen sich nun wie folgt für endliche Mengen von Polynomen verallgemeinern.

Definition 1.4.8 *Es seien $f_1, \ldots f_k$ Polynome aus $\mathbf{K}[x]$, von denen eines ungleich Null ist. Als* **größten gemeinsamen Teiler** *bezeichnen wir ein Polynom $h = \mathsf{ggT}(f_1, \ldots f_k)$ mit folgenden Eigenschaften:*

1. *h teilt echt jedes der Polynome $f_1, \ldots f_k$.*
2. *Jedes weitere Polynom, welches $f_1, \ldots f_k$ echt teilt, teilt auch h echt.*
3. *h ist monisch.*

Wieder ist der größte gemeinsame Teiler eindeutig und es gelten folgende wichtige Zusammenhänge, die seine Berechnung mittels Rekursion ermöglichen.

Satz 1.4.9 *Es seien $f_1, \ldots, f_k$ Polynome aus $\mathbf{K}[x]\backslash\{0\}$. Dann existiert der größte gemeinsame Teiler von $f_1, \ldots, f_k$, und es gelten folgende Aussagen:*

1. $\langle f_1, \ldots, f_k \rangle = \langle \mathsf{ggT}(f_1, \ldots, f_k) \rangle$.
2. $\mathsf{ggT}(f_1, \ldots, f_k) = \mathsf{ggT}(f_1, \mathsf{ggT}(f_2, \ldots, f_k))$.

Mit Hilfe dieser Behandlungsmethoden für Ideale in $\mathbf{K}[x]$ können nun die in Abschnitt 1.1 vorgestellten Probleme wie folgt gelöst werden:

> Gegeben sei ein Ideal $\mathfrak{i}$ durch eine endliche Basis $f_1, \ldots, f_k \in \mathbf{K}[x]\backslash\{0\}$.
> Bestimme das Polynom $h = \mathsf{ggT}(f_1, \ldots, f_k)$.
> Dann gilt $\mathfrak{i} = \langle h \rangle$.

Die Lösung von Problem 1 ergibt sich aus der Tatsache, daß ein Polynom f aus $\mathbf{K}[x]$ nun genau dann in $\mathfrak{i}$ liegt, wenn NORMALFORM$(f, h) = 0$. Falls die Normalformreduktion Null ergibt, so summieren sich die zur Reduktion benutzten Multiplikanten von h gerade zu einer Darstellung, wie sie in Problem 2 gefordert wird, auf. Um festzustellen, ob zwei Polynome f und g die gleiche Auswertungsabbildung bezüglich $\mathfrak{i}$ beschreiben (Problem 3), testet man einfach, ob NORMALFORM$(f - g, h) = 0$. Das Rechnen in dem Quotientenring $\mathbf{K}[x]/\mathfrak{i}$ wird ermöglicht, da für Polynome f aus $\mathbf{K}[x]$, NORMALFORM(f, h) immer eindeutig ist, nämlich der Rest von f dividiert durch g (Problem 4).

Im Verlauf dieser Vorlesung werden wir nun sehen, daß die Methode der Gröbnerbasen genau dieses Vorgehen für einen Polynomring $\mathbf{K}[x_1, \ldots x_n]$ verallgemeinert. Da $\mathbf{K}[x_1, \ldots x_n]$ kein Hauptidealring mehr ist, d.h. Ideale werden im Allgemeinen nicht mehr von nur einem Polynom erzeugt, werden wir zum Berechnen von Normalformen bezüglich eines Ideals in der Regel mehrere Polynome zur Reduktion benutzen und durch diesen erweiterten Reduktionsbegriff zusätzliche Bedingungen an unsere Idealbasen stellen, um eine „einfache" Lösung der Probleme 1 bis 4 durch Reduktion zu gewährleisten.

Übungen

1. Bestimmen Sie eine Erzeugende des Ideals, das von den Polynomen $x^6 - 1$ und $x^4 + 2 \cdot x^3 + 2 \cdot x^2 - 2 \cdot x - 3$ in $\mathbf{Q}[x]$ erzeugt wird. Liegt $x^5 + x^3 + x^2 - 7$ in diesem Ideal? Zeigen Sie, daß $x^4 + 2 \cdot x^2 - 3$ im Ideal liegt und stellen Sie es als Linearkombination von $x^6 - 1$ und $x^4 + 2 \cdot x^3 + 2 \cdot x^2 - 2 \cdot x - 3$ dar.

2. Modifizieren Sie den Euklid'schen Algorithmus so, daß er zu zwei Polynomen f_1 und f_2 aus $\mathbf{K}[x]$ Polynome f, u_1, u_2 aus $\mathbf{K}[x]$ liefert mit $f = \mathsf{ggT}(f_1, f_2)$ und $f = u_1 * f_1 + u_2 * f_2$. Wenden Sie den Algorithmus auf die Polynome aus der vorherigen Aufgabe an.

3. Zeigen Sie, daß $\mathbf{K}[x, y]$ kein Hauptidealring mehr ist. Insbesondere kann das Ideal $\langle x, y \rangle$ nicht von einem Element erzeugt werden.

Kapitel 2

Gröbnerbasen – Die theoretischen Grundlagen

Grau, teurer Freund, ist alle Theorie.

GOETHE

In diesem Kapitel wollen wir Gröbnerbasen in Polynomringen definieren und Buchbergers Algorithmus zu ihrer Berechnung vorstellen.

2.1 Zulässige Ordnungen

Wir haben im vorherigen Kapitel gesehen, wie man zu dem Polynomring $\mathbf{K}[x]$ und einem beliebigen Polynom g ein Reduktionssystem assoziieren kann, indem man g als Regel auffaßt, mit der unter der Gradbedingung andere Polynome reduziert werden dürfen. Dieses „Reduzieren" verkleinert die reduzierten Polynome bezüglich der Gradordnung, die eine wohlfundierte Partialordung auf $\mathbf{K}[x]$ ist. Daher terminiert ein solcher Reduktionsprozeß immer (vergleiche den Algorithmus NORMALFORMin $\mathbf{K}[x]$). Die wesentliche Idee, die diese Terminierung garantiert, liegt darin begründet, daß die gewählte Gradordnung bezüglich der Multiplikation mit Termen **zulässig** ist, d.h. für alle Terme x^n, x^m, x^d mit n, m, d aus $\mathbf{N}$ gilt zum einen $x^n \geq 1$. Weiterhin impliziert $x^n > x^m$ auch $x^n \circ x^d = x^{n+d} > x^{m+d} = x^m \circ x^d$. Dieser Begriff der Zulässigkeit soll nun für den Polynomring $\mathbf{K}[x_1, \ldots x_n]$ verallgemeinert werden. Zur Erinnerung war die Menge der Terme über den Variablen $x_1, \ldots, x_n$ definiert als

$$\mathsf{T}^n = \{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbf{N}\}.$$

Auf dieser Menge sollen nun Ordnungen mit bestimmten Eigenschaften benutzt werden.

Definition 2.1.1 *Eine totale Ordnung $\geq$ auf T^n heißt* **zulässig***, falls für alle Terme t_1, t_2 und t aus T^n gilt*

1. *$t \geq 1$ und*

2. *$t_1 > t_2$ impliziert $t_1 \circ t > t_2 \circ t$.*

Totale zulässige Ordnungen auf T^n werden auch **Termordungen** genannt. Es folgen nun einige wichtige Beispiele für diese Klasse von Ordnungen. Im Folgenden sei $\mathsf{grad}_{x_i}(t)$ der Exponent der Variable x_i im Term t.

Definition 2.1.2 *Ein Term s heißt* **lexikographisch kleiner** *als ein weiterer Term t bezüglich der Präzedenz $x_1 > \ldots > x_n$, falls es ein $1 \leq k \leq n$ gibt, so daß für alle $j < k$ gilt $\mathsf{grad}_{x_j}(s) = \mathsf{grad}_{x_j}(t)$ und $\mathsf{grad}_{x_k}(s) < \mathsf{grad}_{x_k}(t)$.*

Definition 2.1.3 *Ein Term s heißt* **länge-lexikographisch kleiner** *als ein weiterer Term t bezüglich der Präzedenz $x_1 > \ldots > x_n$, falls entweder $\sum_{j=1}^n \mathsf{grad}_{x_j}(s) < \sum_{j=1}^n \mathsf{grad}_{x_j}(t)$ oder $\sum_{j=1}^n \mathsf{grad}_{x_j}(s) = \sum_{j=1}^n \mathsf{grad}_{x_j}(t)$, und es gibt ein $1 \leq k \leq n$, so daß für alle $j < k$ gilt $\mathsf{grad}_{x_j}(s) = \mathsf{grad}_{x_j}(t)$ und $\mathsf{grad}_{x_k}(s) < \mathsf{grad}_{x_k}(t)$.*

Definition 2.1.4 *Ein Term s heißt* **umgekehrt-länge-lexikographisch kleiner** *als ein weiterer Term t bezüglich der Präzedenz $x_1 > \ldots > x_n$, falls entweder $\sum_{j=1}^n \mathsf{grad}_{x_j}(s) < \sum_{j=1}^n \mathsf{grad}_{x_j}(t)$ oder $\sum_{j=1}^n \mathsf{grad}_{x_j}(s) = \sum_{j=1}^n \mathsf{grad}_{x_j}(t)$, und es gibt ein $1 \leq k \leq n$, so daß für alle $j > k$ gilt $\mathsf{grad}_{x_j}(s) = \mathsf{grad}_{x_j}(t)$ und $\mathsf{grad}_{x_k}(s) > \mathsf{grad}_{x_k}(t)$.*

Es ist leicht zu zeigen, daß diese Ordnungen tatsächlich Termordnungen sind. Im Folgenden sei $>$ immer eine Termordnung auf T^n. Wir wollen zeigen, daß eine solche Ordnung wichtige Eigenschaften hat, die es ermöglichen, eine terminierende Reduktion für Polynome zu definieren. Hierzu schauen wir uns zuerst noch einmal den Teilbarkeitsbegriff auf Termen etwas genauer an. Ein Term t_1 teilt einen Term t_2 genau dann, wenn es einen Term t gibt mit $t_1 \circ t = t_2$. Für Terme $t_1 \equiv x_1^{i_1} \ldots x_n^{i_n}$ und $t_2 \equiv x_1^{j_1} \ldots x_n^{j_n}$ in T^n bedeutet dies, $i_l \leq j_l$ für alle $1 \leq l \leq n$ und $t \equiv x_1^{j_1 - i_1} \ldots x_n^{j_n - i_n}$. Ist nun ein Term t_1 ein Teiler von t_2, so gilt für jede beliebige Termordung $\leq$ immer $t_1 \leq t_2$. Um dies zu sehen, nehmen wir an, daß die Aussage falsch sei. Da eine Termordung total ist, muß also $t_1 > t_2$ gelten. Da sicher auch $t_2 \geq 1$ gilt, erhalten wir für den Term t mit $t_1 \circ t = t_2$

$$\underbrace{t_1 \circ t}_{t_2} > t_2 \circ t \geq 1 \circ t = t.$$

Weiter folgt aus $t \geq 1$ die Ungleichung $t_2 \circ t \geq t_2 \circ 1 = t_2$, was im Widerspruch zu $t_2 > t_2 \circ t$ steht.

Eine weitere wichtige Eigenschaft von Termordnungen ist, daß sie wohlfundiert sind, d.h. es gibt keine unendlichen Ketten der Form $t_1 > t_2 > \ldots$ von Termen t_i aus T^n, $i \in \mathbf{N}$. Diese Aussage kann mit Hilfe von Hilberts Basissatz für den Polynomring $\mathbf{K}[x_1, \ldots x_n]$ gezeigt werden, ist aber in der Literatur auch als Lemma von Dickson bekannt.

Lemma 2.1.5 *Es sei S eine Teilmenge von T^n. Dann gibt es eine endliche Teilmenge S' von S, so daß jedes Element aus S einen Teiler in S' hat.*

Beweis :
Der Beweis erfolgt durch Induktion nach n. Für $\mathsf{T}^1 = \{x^i \mid i \in \mathbf{N}\}$ kann in S das Element kleinsten Grades als Teilmenge S' mit der gewünschten Eigenschaft ausgezeichnet werden. Im Induktionsschritt $n > 1$ wählen wir einen beliebigen Term s aus S, z.B. $s = x_1^{e_1} \dots x_n^{e_n}$. Dann lassen sich alle weiteren Terme aus S, die nicht von s geteilt werden, auf folgende Mengen aufteilen:

$$T_{i,j} = \{t \mid t \in S, \mathsf{grad}_{x_i}(t) = j\}$$

mit $1 \leq i \leq n$ und $0 \leq j \leq e_i - 1$. Da alle Terme einer Menge $T_{i,j}$ nach Definition in der Variablen x_i denselben Exponenten haben, kann $T_{i,j}$ auch als eine Teilmenge der Termmenge $\mathsf{T}^{n-1}(\{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n\})$ aufgefaßt werden. Somit kann jeweils die Induktionshypothese angewandt werden, d.h. es existieren endlich Teilmengen $S'_{i,j} \subseteq T_{i,j}$ so daß jeder Term in $T_{i,j}$ von einem Term in $S'_{i,j}$ geteilt wird. Die Menge

$$S' = \{s\} \cup \bigcup_{\substack{1 \leq i \leq n \\ 0 \leq j \leq e_i - 1}} S'_{i,j}$$

ist somit eine endliche Teilmenge von S mit der gewünschten Eigenschaft.

q.e.d.

Nun können wir zeigen, daß Termordnungen wohlfundiert sind. Nehmen wir an, es gäbe eine unendliche absteigende Kette von Termen

$$t_1 > t_2 > \dots, t_i \in \mathsf{T}^n, i \in \mathbf{N}.$$

Dann bilden diese Terme eine Menge S, für die nach dem Lemma von Dickson eine endliche Teilmenge $S' = \{t_{i_1}, \dots, t_{i_k}\}$ mit $t_{i_1} > \dots > t_{i_k}$ existieren muß, so daß zu jedem Term t_j ein Teiler t_{i_l} in S' existiert, und es gilt $t_j \geq t_{i_l}$. Ist obige Kette unendlich, so gibt es für den Term t_{i_k+1} einen Teiler t_{i_l} in S', und es muß gelten $t_{i_k+1} \geq t_{i_l}$ im Widerspruch zu $t_{i_l} \geq t_{i_k} > t_{i_k+1}$.

Termordnungen können nun zu Partialordnungen auf den Polynomen fortgesetzt werden. Hierzu führen wir noch einige Begriffe ein. Für ein Polynom $f = \sum_{i=1}^k a_i \cdot t_i$ mit $a_i \in \mathbf{K}\backslash\{0\}$, $t_i \in \mathsf{T}^n$ und $t_1 > \dots > t_k$ bezeichne $\mathsf{HM}(f) = a_1 \cdot t_1$ das Kopfmonom bestehend aus Kopfkoeffizient $\mathsf{HC}(f) = a_1$ und Kopfterm $\mathsf{HT}(f) = t_1$. Mit $\mathsf{RED}(f) = \sum_{i=2}^k a_i \cdot t_i$ bezeichnen wir den Rest des Polynoms, und $\mathsf{T}(f) = \{t_1, \dots, t_k\}$ ist die Menge der in f auftretenden Terme. Für das Nullpolynom definieren wir $\mathsf{HM}(0) = \mathsf{HC}(0) = \mathsf{HT}(0) = \mathsf{RED}(0) = 0$.

Definition 2.1.6 *Es seien f und g Polynome und $>$ eine Termordnung auf T^n. Diese wird auf $\mathbf{K}[x_1, \dots, x_n]$ wie folgt zu einer Partialordnung fortgesetzt: Ist f nicht das Nullpolynom, so gilt immer $f > 0$. Weiter gilt $f > g$ genau dann, wenn $\mathsf{HT}(f) > \mathsf{HT}(g)$ oder $\mathsf{HT}(f) = \mathsf{HT}(g)$ und $\mathsf{RED}(f) > \mathsf{RED}(g)$.*

Diese von der Termordnung induzierte Partialordnung auf Polynomen ist wiederum wohlfundiert.

Lemma 2.1.7 *Die von einer Termordnung wie in Definition 2.1.6 beschrieben induzierte Polynomordnung auf* $\mathbf{K}[x_1, \ldots, x_n]$ *ist wohlfundiert.*

Beweis :
Es sei $\geq$ eine Partialordung auf $\mathbf{K}[x_1, \ldots, x_n]$, die von einer Termordnung $\geq$ auf T^n wie in Definition 2.1.6 beschrieben induziert wird. Wir nehmen an, diese Ordnung sei auf $\mathbf{K}[x_1, \ldots, x_n]$ nicht wohlfundiert und zeigen, daß dies einen Widerspruch zur Wohlfundiertheit der entsprechenden Termordung auf T^n impliziert.
Es sei also $f_0 > f_1 > \ldots f_k > \ldots$, $k \in \mathbf{N}$, eine echte unendliche Kette in $\mathbf{K}[x_1, \ldots, x_n]$. Dann können wir rekursiv eine Folge von Paaren $\{\{(t_k, g_{kl}) \mid l \in \mathbf{N}\} \mid k \in \mathbf{N}\}$ wie folgt definieren:
Für $k = 0$ sei $t_0 = \min\{\mathsf{HT}(f_i) \mid i \in \mathbf{N}\}$. Weiter sei $j \in \mathbf{N}$ der kleinste Index, so daß $\mathsf{HT}(f_j) = t_0$. Dann gilt auch $\mathsf{HT}(f_{j+l}) = t_0$ für alle $l \in \mathbf{N}$ und wir definieren $g_{0l} = f_{j+l} - \mathsf{HM}(f_{j+l})$, d.h. $\mathsf{HT}(g_{0l}) < t_0$ für alle $l \in \mathbf{N}$.
Analog setzen wir für $k+1$, $t_{k+1} = \min\{\mathsf{HT}(g_{kl}) \mid l \in \mathbf{N}\}$. Es sei wieder $j \in \mathbf{N}$ der kleinste Index, so daß $\mathsf{HT}(g_{kj}) = t_{k+1}$, d.h. $\mathsf{HT}(g_{k(j+l)}) = t_{k+1}$ für alle $l \in \mathbf{N}$. Weiter setzen wir wieder $g_{(k+1)l} = g_{k(j+l)} - \mathsf{HM}(g_{k(j+l)})$. Dann gilt:

1. Für alle $s \in \mathsf{T}(g_{kl})$ gilt $s < t_k$,

2. Für alle $k \in \mathbf{N}$ ist $g_{k0} > g_{k1} > \ldots$ eine echte fallende Kette in $\mathbf{K}[x_1, \ldots, x_n]$.

Insbesondere ist dann auch $t_0 > t_1 > \ldots$ eine echte fallende Kette in T^n im Widerspruch zur Wohlfundiertheit der Termordnung $\geq$ auf T^n.

q.e.d.

Wir werden im Folgenden zeigen, wie Reduktion basierend auf Teilbarkeit von Termen im Polynomring definiert werden kann.

Übungen

✓ 1. Zeigen Sie, daß die hier vorgestellten Ordungen auf Termen tatsächlich Termordnungen sind.

✓ 2. Zeigen Sie, daß es für $\mathsf{T}^1 = \{x^i \mid i \in \mathbf{N}\}$ nur eine Termordnung gibt.

✓ 3. Zeigen Sie, daß für den Polynomring $\mathbf{K}[x, y]$ die länge-lexikographische und die umgekehrt-länge-lexikographische Ordnung übereinstimmen.

☼ 4. Gegeben seien Polynome $f_1, \ldots, f_k$ und $g_1, \ldots, g_k$ aus $\mathbf{K}[x_1, \ldots, x_n]$. Zeigen Sie, daß $\mathsf{HT}(\sum_{i=1}^{k} f_i * g_i) \leq \max_{1 \leq i \leq k}\{\mathsf{HT}(f_i) \circ \mathsf{HT}(g_i)\}$. Gilt hier sogar die Gleichheit?

2.2 Polynomdivision in $\mathbf{K}[x_1, \ldots, x_n]$

In diesem Abschnitt wollen wir die Polynomdivision, die wir für den Polynomring $\mathbf{K}[x]$ kennengelernt haben, verallgemeinern. In Abschnitt 1.4 haben wir gesehen, wie ein Polynom f aus $\mathbf{K}[x]$ durch ein Polynom g aus $\mathbf{K}[x]\backslash\{0\}$ geteilt werden kann. Wie haben festgestellt, daß diese Division zwei eindeutige Polynome q und r aus $\mathbf{K}[x]$ liefert, so daß sich f schreiben läßt als $f = q * g + r$, und entweder ist $r = 0$ oder aber $\mathsf{grad}(r) < \mathsf{grad}(g)$.

Unser Ziel ist es nun, ein Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$ durch Polynome $g_1, \ldots, g_k$ aus $\mathbf{K}[x_1, \ldots, x_n]\backslash\{0\}$ zu dividieren in dem Sinne, daß wir f ausdrücken wollen als Summe

$$f = q_1 * g_1 + \ldots + q_k * g_k + r,$$

wobei $q_1, \ldots, q_k, r$ wieder Polynome aus $\mathbf{K}[x_1, \ldots, x_n]$ sind. An den Rest r werden wiederum bestimmte Bedingungen geknüpft werden. Diese Bedingungen werden ähnlich wie im Falle von $\mathbf{K}[x]$ von der für den Polynomring gewählten Termordnung abhängen.

Die Grundidee für die Division ist ganz analog: Wir versuchen, den Kopf von f durch ein geeignetes Vielfaches eines der Polynome $g_1, \ldots, g_k$ zu eliminieren. Im Unterschied zu $\mathbf{K}[x]$ werden wir jedoch nicht aufhören, sobald der Kopfterm des Resultates nicht mehr teilbar ist, sondern dann gegebenenfalls mit kleineren teilbaren Termen weitermachen, um insgesamt zu erreichen, daß der so berechnete Rest nicht mehr weiter dividierbar ist. Dies war für $\mathbf{K}[x]$ nicht nötig, da dort die Dividierbarkeit eines kleineren Termes sofort auch die Dividierbarkeit des Kopftermes impliziert.

Zuerst wollen wir uns dieses Vorgehen an einem Beispiel verdeutlichen. Wir betrachten Polynome aus $\mathbf{Q}[x, y]$ und wählen als Termordnung die von $x > y$ induzierte lexikographische Ordnung.

Es seien also $f = xy^2 + y^2$ und $g_1 = xy - 1$, $g_2 = y^2 - 1$ unsere Polynome aus $\mathbf{Q}[x, y]$. Dann erhalten wir für die Division von f mit g_1 erst einmal

$$\begin{array}{rrrrrl} & xy^2 & + & y^2 & & : \quad xy - 1 \; = \; y. \\ - & (xy^2 & - & y) & & \\ \hline & & & y^2 & + \; y & \end{array}$$

Für die Division von des Restes $y^2 + y$ mit g_2 erhalten wir

$$\begin{array}{rrrrrl} & y^2 & + & y & & : \quad y^2 - 1 \; = \; 1. \\ - & (y^2 & - & 1) & & \\ \hline & & & y & + \; 1 & \end{array}$$

Da $y + 1$ weder durch g_1 noch durch g_2 teilbar ist, erhalten wir also

$$f = y * g_1 + g_2 + (y + 1).$$

Auf der anderen Seite dividiert natürlich auch g_2 unser Polynom f, da $\mathsf{HT}(g_2) = y^2$ und $\mathsf{HT}(f) = xy^2$. In diesem Falle erhalten wir

$$\begin{array}{rrrrl} & xy^2 & + & y^2 & \quad : \quad y^2 - 1 \;=\; x. \\ - & (xy^2 & - & x) & \\ \hline & & & x & + \; y^2 \end{array}$$

Der Kopf dieses Restes ist x und somit weder durch $\mathsf{HT}(g_1)$ noch durch $\mathsf{HT}(g_2)$ teilbar. Da wir jedoch als Bedingung an unseren Rest auf jeden Fall fordern wollen, daß kein in ihm vorkommender Term mit den Polynomen $g_1, \ldots, g_k$ dividierbar ist, müssen wir uns auch den Term y^2 anschauen. Es zeigt sich, daß dieser Term von $\mathsf{HT}(g_2)$ geteilt wird und wir erhalten

$$\begin{array}{rrrrl} & x & + & y^2 & \quad : \quad y^2 - 1 \;=\; 1. \\ - & (y^2 & - & 1) & \\ \hline & & & x & + \; 1 \end{array}$$

$x + 1$ ist nun nicht mehr mit g_1 oder g_2 teilbar. So erhalten wir nun eine zweite, von unserer ersten verschiedene, Darstellung von f, nämlich

$$f = 0 * g_1 + (x + 1) * g_2 + (x + 1).$$

Dieses Beispiel zeigt uns, daß im Gegensatz zu der Division mit Rest in $\mathbf{K}[x]$ bei einer Division von f mit Polynomen $g_1, \ldots, g_k$ aus $\mathbf{K}[x_1, \ldots, x_n]$ weder die Polynome $q_1, \ldots, q_k$ noch der Rest r eindeutig sein müssen. Dennoch läßt sich ähnlich zu Satz 1.4.1 formulieren:

Satz 2.2.1 *Es seien $f, g_1, \ldots, g_k$ Polynome aus $\mathbf{K}[x_1, \ldots, x_n]$ und $\leq$ eine Termordnung auf T^n. Dann kann man f schreiben als*

$$f = q_1 * g_1 + \ldots + q_k * g_k + r$$

mit Polynomen $q_1, \ldots, q_k, r$ aus $\mathbf{K}[x_1, \ldots, x_n]$, so daß $r = 0$ oder kein Term in r durch $\mathsf{HT}(g_1), \ldots, \mathsf{HT}(g_k)$ teilbar ist. Weiterhin gilt für alle $1 \leq i \leq k$, falls $q_i * g_i \neq 0$, $\mathsf{HT}(f) \geq \mathsf{HT}(q_i * g_i)$.

Wir haben schon gesehen, daß der Rest r nicht eindeutig sein muß. In $\mathbf{K}[x]$ konnte Division mit Rest benutzt werden, um das Enthaltenseinproblem für Ideale zu lösen. Es stellt sich nun die Frage, ob hier Ähnliches erwartet werden kann.

Gilt $r = 0$ so folgt direkt

$$f = q_1 * g_1 + \ldots + q_k * g_k \in \langle g_1, \ldots, g_k \rangle.$$

Leider ist dies jedoch nur eine hinreichende Bedingung, wie folgendes Beispiel zeigt. Wir betrachten die Polynome $f = xy^2 - x$ und $g_1 = xy - 1$, $g_2 = y^2 - 1$ aus $\mathbf{Q}[x, y]$. Dann erhalten wir zwei verschiedene Darstellungen von f, nämlich

$$f = y * g_1 + 0 * g_2 + (-x + y)$$

und

$$f = 0 * g_1 + x * g_2 + 0.$$

Somit liegt f in dem Ideal $\langle g_1, g_2\rangle$, hat jedoch nicht nur Darstellungen der gewünschten Form mit Rest Null. Wir werden im Folgenden sehen, daß für bestimmte Polynommengen $r = 0$ auch eine notwendige Bedingung für das Enthaltensein in einem Ideal sein wird. Dazu führen wir im nächsten Abschnitt den Begriff der Reduktion für den Polynomring $\mathbf{K}[x_1, \ldots, x_n]$ ein.

Übungen

1. Formulieren Sie analog zu Euklids Algorithmus einen Divisionsalgorithmus für $\mathbf{K}[x_1, \ldots, x_n]$. ☼

2.3 Reduktion und Normalformen

Die Kernidee von Buchbergers Algorithmus ist der Einsatz von Polynomen als Regeln zur Reduktion. Ein Polynom f wird bezüglich der gewählten Termordnung aufgespalten in das Kopfmonom und den Rest. Die so erhaltene Regel „Kopfterm $\longrightarrow$ - Rest" kann dann wie folgt zur Reduktion benutzt werden.

Definition 2.3.1 *Es seien f und p Polynome in $\mathbf{K}[x_1, \ldots, x_n]$. Wir sagen f* **reduziert** p **an einem Monom** $a \cdot t$ **in** p **in einem Schritt**, *falls der Kopfterm $\mathsf{HT}(f)$ den Term t teilt. Wir schreiben dann*

$$p \longrightarrow_f p - (a \cdot \mathsf{HC}(f)^{-1}) \cdot f * s$$

wobei $\mathsf{HT}(f) \circ s = t$. f **reduziert** *p, falls es ein Monom in p gibt, so daß diese Bedingung erfüllt ist. Reduktion bezüglich einer Menge von Polynomen F ist definiert, falls es ein f in F gibt, welches p reduziert, und wir schreiben $p \longrightarrow_F$.*

Assoziiert man zu einer Menge von Polynomen F die Termmenge $\mathsf{HT}(F) = \{\mathsf{HT}(f) \mid f \in F\}$, so beschreibt die Menge $R(F) = \{t \circ s \mid t \in \mathsf{HT}(F), s \in \mathsf{T}^n\}$ gerade die Menge der Terme, die mit einem Polynom aus F reduzibel sind[1]. Enthält ein Polynom keinen Term aus dieser Menge, so heißt es bezüglich F irreduzibel. Da unsere Partialordnung auf Polynomen eine Erweiterung unserer Termordnung ist und diese zulässig und wohlfundiert ist, sind Reduktionsschritte wie oben definiert verkleinernd. Für $p \longrightarrow_f q$ gilt $p > q$, und es kann keine unendlichen Reduktionsketten geben.

Mit $\overset{*}{\longrightarrow}_F$ bezeichnen wir den reflexiv transitiven Abschluß der Reduktion $\longrightarrow_F$, und eine Normalform eines Polynoms f ist ein Polynom $\tilde{f}$, welches bezüglich F irreduzibel ist und für das $f \overset{*}{\longrightarrow}_F \tilde{f}$ gilt. Folgender Algorithmus zeigt auf, wie solche Normalformen berechnet werden können.

[1] Diese Menge wird auch häufig als das von $\mathsf{HT}(F)$ erzeugte Termideal in T^n bezeichnet.

NORMALFORM

Eingabe: Ein Polynom f und eine endliche Polynommenge F aus $\mathbf{K}[x_1, \ldots, x_n]$.
Ausgabe: h eine Normalform von f bezüglich F.

$h := f$;
while $R(F) \cap \mathsf{T}(h) \neq \emptyset$ **do**
  wähle g aus F mit $R(g) \cap \mathsf{T}(h) \neq \emptyset$;
  reduziere h mit g und weise das Ergebnis h zu;
endwhile

Dieser Algorithmus terminiert immer, da Polynomreduktion noethersch ist. Er ist jedoch nicht-deterministisch, da die Wahl von g und die Wahl des zu reduzierenden Monoms in h frei sind. Für Implementierungen können hier verschiedene Auswahlstrategien benutzt werden. Den Spezialfall der Kopfreduktion haben wir schon für den Fall $\mathbf{K}[x]$ im vorherigen Kapitel kennengelernt. Im Allgemeinen können verschiedene Normalformen eines Polynoms bezüglich Reduktion mit einer Polynommenge existieren.

Betrachten wir als Beispiel noch einmal die Polynome $f = xy^2 + y^2$ und $g_1 = xy - 1$, $g_2 = y^2 - 1$ aus $\mathbf{Q}[x, y]$ mit lexikographischer Ordnung und Präzedenz $x > y$. Dann können wir einmal f zuerst am Kopf mit g_1 und dann am Kopf mit g_2 reduzieren und erhalten

$$f \longrightarrow_{g_1} y^2 + y \longrightarrow_{g_2} y + 1.$$

Reduziert man hingegen f zuerst mit g_2 so erhält man

$$f \longrightarrow_{g_2} x + y^2 \longrightarrow_{g_2} x + 1.$$

Wünschenswert wäre natürlich, daß Normalformen von Polynomen eindeutig sind. Dies ist, wie unser Beispiel zeigt, für beliebige Mengen von Polynomen nicht zu erwarten. Daher können wir in diesem Rahmen nun eine erste normalformbasierte Definition von Gröbnerbasen geben: Eine endliche Menge G von Polynomen heißt **Gröbnerbasis** (des Ideals $\langle G \rangle$) genau dann, wenn für jedes Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$ genau eine Normalform (unabhängig von der Reduktionsstrategie) bezüglich Reduktion mit Polynomen aus G existiert. Im nächsten Abschnitt werden wir diese Basen genauer kennenlernen. Nun wollen wir zum Abschluß noch einige nützliche Eigenschaften der hier vorgestellten Reduktion sammeln.

Lemma 2.3.2 *Es seien f, g und h Polynome und F eine endliche Menge von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$.*

1. *Falls $f - g \longrightarrow_F h$, so existieren Polynome f' und g' in $\mathbf{K}[x_1, \ldots, x_n]$, so daß $f \xrightarrow{*}_F f'$, $g \xrightarrow{*}_F g'$ und $h = f' - g'$.*

2. *Ist 0 eine Normalform von $f - g$ bezüglich F, so existiert ein Polynom h aus $\mathbf{K}[x_1, \ldots, x_n]$, so daß $f \xrightarrow{*}_F h$ und $g \xrightarrow{*}_F h$.*

3. *$f \overset{*}{\longleftrightarrow}_F g$ genau dann, wenn f und g in der gleichen Äquivalenzklasse modulo $\langle F \rangle$ liegen.*

4. *$f \overset{*}{\longrightarrow}_F 0$ impliziert $a \cdot f * s \overset{*}{\longrightarrow}_F 0$ für alle $a \in \mathbf{K}$ und $s \in \mathsf{T}^n$.*

Punkt 2 wird in der Literatur häufig als Translationslemma bezeichnet und gibt eine hinreichende Bedingung für Konfluenz der Reduktion $\longrightarrow_F$ an. Punkt 3 zeigt auf, daß unsere Reduktion gerade die vom Ideal $\langle F \rangle$ erzeugte Kongruenz beschreibt. Daher kann Reduktion im Zusammenhang mit Gröbnerbasen später wirkungsvoll für das Lösen idealtheoretischer Probleme eingesetzt werden.

Übungen

1. Zeigen Sie, daß es bezüglich einer nichtleeren Polynommenge F aus $\mathbf{K}[x_1, \ldots, x_n]$ keine unendlichen Reduktionsketten geben kann. ☼

2. Beweisen Sie die Aussagen aus Lemma 2.3.2. ✓

3. Zeigen Sie, daß für Polynome f, g und Polynommengen F aus $\mathbf{K}[x_1, \ldots, x_n]$ und Terme s gilt: ✓
   (a) Falls $f \in F$, so $f * g \overset{*}{\longrightarrow}_F 0$.
   (b) Falls $f \overset{*}{\longrightarrow}_F g$, so $f * s \overset{*}{\longrightarrow}_F g * s$.

4. Zeigen Sie, daß für Polynome f, g, h, r, s und Polynommengen F aus $\mathbf{K}[x_1, \ldots, x_n]$ folgendes *nicht* mehr gelten muß: ✓
   (a) Falls $f \overset{+}{\longrightarrow}_F r$ und $g \overset{+}{\longrightarrow}_F s$, so $f + g \overset{+}{\longrightarrow}_F r + s$.
   (b) Falls $f \overset{+}{\longrightarrow}_F r$ und $g \overset{+}{\longrightarrow}_F s$, so $f * g \overset{+}{\longrightarrow}_F r * s$.
   (c) Falls $f + g \overset{+}{\longrightarrow}_F h$, $f \overset{+}{\longrightarrow}_F r$ und $g \overset{+}{\longrightarrow}_F s$, wobei h, r und s bezüglich F reduziert sind, so $r + s = h$.

5. Es sei $F = \{f_1, \ldots, f_k\}$ eine Teilmenge von $\mathbf{K}[x_1, \ldots, x_n] \backslash \{0\}$ und f ein Polynom mit $f = \sum_{i=1}^{k} h_i * f_i$ mit $\mathsf{HT}(f) = \max_{1 \leq i \leq k}\{\mathsf{HT}(h_i * f_i)\}$. Zeigen Sie, daß dies *nicht* $f \overset{+}{\longrightarrow}_F 0$ impliziert. ☼

2.4 Gröbnerbasen und ihre Charakterisierungen

Gröbnerbasen werden in der Literatur auf verschiedene Arten motiviert, definiert und charakterisiert. Hier soll nun ein kurzer Überblick gegeben und die Äquivalenz der Charakterisierungen gezeigt werden. Im Folgenden sei G immer eine endliche Menge von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$. Eine erste Charakterisierung hatten wir bereits im letzten Abschnitt kennengelernt.

Charakterisierung 1: (Eindeutige Normalformen)
G heißt Gröbnerbasis (des Ideals $\langle G \rangle$) genau dann, wenn für jedes Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$ genau eine Normalform bezüglich G existiert.

Eine auf den ersten Blick sehr einfache Charakterisierung, hinter der sich jedoch auch wieder die Beschreibung der mit einer Polynommenge reduziblen Terme verbirgt, erhält man durch das von den Kopftermen erzeugte sogenannte Termideal.

Charakterisierung 2: (Kopfterme)
G heißt Gröbnerbasis (des Ideals $\langle G \rangle$) genau dann, wenn $\mathsf{HT}(\langle G \rangle \backslash \{0\}) = \{t \circ s \mid t \in \mathsf{HT}(G), s \in \mathsf{T}^n\}$.

Die nächste Charakterisierung verallgemeinert die Charakterisierung über die Kopfterme insoweit, als sie eine Beschreibung der Idealelemente durch besondere Linearkombinationen gewährleistet. Solche Basen heißen in der Literatur Standardbasen und sind äquivalent zu Gröbnerbasen.

Charakterisierung 3: (Standardbasis)
G heißt Gröbnerbasis (des Ideals $\langle G \rangle$) genau dann, wenn jedes Polynom f aus $\langle G \rangle$ eine Repräsentation der Gestalt $f = \sum_{i=1}^{k} a_i \cdot g_i * s_i$ hat mit $a_i \in \mathbf{K}$, $g_i \in G$, $s_i \in \mathsf{T}^n$ und $\mathsf{HT}(g_i * s_i) \leq \mathsf{HT}(f)$ für alle $1 \leq i \leq k$.

Ebenfalls über die Idealelemente aber mittels Reduktion erfolgt die nächste Charakterisierung.

Charakterisierung 4: (Idealbeschreibung)
G heißt Gröbnerbasis (des Ideals $\langle G \rangle$) genau dann, wenn für alle f aus $\langle G \rangle$ gilt $f \xrightarrow{*}_G 0$.

Im Kontext der Ersetzungssysteme lassen sich Gröbnerbasen über den Begriff der Konfluenz beschreiben.

Charakterisierung 5: (Konfluenz)
G heißt Gröbnerbasis (des Ideals $\langle G \rangle$) genau dann, wenn $\xleftrightarrow{*}_G$ die Idealkongruenz beschreibt und $\longrightarrow_G$ konfluent ist.

Die Forderung, daß die Reduktionsrelation auch die Idealkongruenz beschreibt, ist in unserem Fall trivial (vergleiche Lemma 2.3.2). Benutzt man jedoch andere Definitionen von Reduktion, so muß diese Eigenschaft hinzugenommen werden.

Alle bisherigen Charakterisierungen von Gröbnerbasen sind nicht konstruktiv und ermöglichen weder einen effektiven Test der Eigenschaften noch eine Berechnung der Gröbnerbasen. Dies soll nun durch eine Methode, die wir bei der Beschreibung von Reduktionssystemen kennengelernt haben, geschehen. Wir erinnern uns, daß für noethersche Reduktionsrelationen ein Konfluenztest auf einen Test der lokalen Konfluenz reduziert werden kann. Also fragen wir uns, welche Situationen für einen solchen Test untersucht werden müssen. Wann können zwei Polynome f und g zur Reduktion eines Polynomes p eingesetzt werden? Eine erste Antwort ist, wenn $\mathsf{HT}(f)$ und $\mathsf{HT}(g)$ beide einen Term aus $\mathsf{T}(p)$ teilen.

Man sieht jedoch sofort, daß, wenn dies zwei verschiedene Terme sind, wir diese beiden Reduktionen wieder zusammenführen können. Wir nehmen an p reduziere sich an einem Monom $a_1 \cdot t_1$ mit f zu $p_1 = p - a_1 \cdot \mathsf{HC}(f)^{-1} \cdot f * s_1$ und an einem anderen Monom

$a_2 \cdot t_2$ mit g zu $p_2 = p - a_2 \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2$ und o.B.d.A. $t_1 > t_2$. Dann ist sicherlich $a_1 \cdot t_1$ ein Monom in p_2 und wir können p_2 mit f zu

$$\begin{aligned} q &= p_2 - a_1 \cdot \mathsf{HC}(f)^{-1} \cdot f * s_1 \\ &= p - a_2 \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 - a_1 \cdot \mathsf{HC}(f)^{-1} \cdot f * s_1 \end{aligned}$$

reduzieren. Ist nun auch $a_2 \cdot t_2$ ein Monom in p_1, so sind wir fertig, da p_1 dann mit g zu q reduzibel ist. Es bleibt also der Fall, daß $a_2 \cdot t_2$ kein Monom in p_1 mehr ist. Wir unterscheiden dann, ob in p_1 kein Monom mit Term t_2 mehr vorkommt oder ob t_2 in p_1 den Koeffizienten $b \neq a_2$ hat. In diesen beiden Fällen enthält das Polynom q wieder den Term t_2 nur jetzt mit Koeffizienten $-a_2$ beziehungsweise $b - a_2$, denn es gilt auch $q = p_1 - a_2 \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2$, und man sieht sofort, daß q sich mit g reduzieren läßt und zwar im Fall $t_2 \notin \mathsf{T}(p_1)$ zu

$$\begin{aligned} q - (-a_2) \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 &= p_1 - a_2 \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 + a_2 \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 \\ &= p_1 \end{aligned}$$

und falls t_2 in p_1 den Koeffizienten b hat zu

$$\begin{aligned} q - (b - a_2) \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 &= p_1 - a_2 \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 - (b - a_2) \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2 \\ &= p_1 - b \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2. \end{aligned}$$

Im ersten Fall sind wir fertig und im zweiten Fall müssen wir noch p_1 mit g am Monom $b \cdot t_2$ zu $p_1 - b \cdot \mathsf{HC}(g)^{-1} \cdot g * s_2$ reduzieren. Somit sind auch in allen diesen Fällen die Reduktionen zusammenführbar.

Kritisch wird es nur, wenn beide Polynome zur Reduktion *desselben* Terms benutzt werden. Es stellt sich also die Frage, welche Terme von zwei Polynome gleichzeitig reduziert werden können. Für zwei Terme $t_1 \equiv x_1^{i_1} \dots x_n^{i_n}$ und $t_2 \equiv x_1^{j_1} \dots x_n^{j_n}$ ist das kleinste gemeinesame Vielfache definiert als $\mathsf{kgV}(t_1, t_2) = x_1^{\max\{i_1,j_1\}} \dots x_n^{\max\{i_n,j_n\}}$. Dann gilt, daß für jeden Term t, der sowohl von t_1 als auch von t_2 geteilt wird, auch $\mathsf{kgV}(t_1, t_2)$ ein Teiler ist. Buchberger zeigte, daß gerade dies die Terme sind, die zu den Situationen führen, die für einen Test auf lokale Konfluenz untersucht werden müssen.

Definition 2.4.1 *Es seien f und g zwei Polynome aus $\mathbf{K}[x_1, \dots, x_n] \backslash \{0\}$ und s_1, s_2 zwei Terme, so daß $\mathsf{kgV}(\mathsf{HT}(f), \mathsf{HT}(g)) = \mathsf{HT}(f) \circ s_1 = \mathsf{HT}(g) \circ s_2$. Dann wird folgendes Polynom*

$$\mathsf{spol}(f, g) = \mathsf{HC}(f)^{-1} \cdot f * s_1 - \mathsf{HC}(g)^{-1} \cdot g * s_2$$

als **s-Polynom** *zu f und g bezeichnet.*

Diese Polynome können nun benutzt werden, um Gröbnerbasen in Polynomringen konstruktiv zu charakterisieren und ermöglichen es, für eine endliche Menge von Polynomen zu testen, ob diese eine Gröbnerbasis ist.

Charakterisierung 6: (Buchberger)
G heißt Gröbnerbasis (des Ideals $\langle G \rangle$) genau dann, wenn für alle f und g aus G $\mathsf{spol}(f, g) \xrightarrow{*}_G 0$.

Wir zeigen nun, daß die hier vorgestellten Charakterisierungen von Gröbnerbasen äquivalent sind.

Satz 2.4.2 *Für eine endliche Menge von Polynomen G aus $\mathbf{K}[x_1,\ldots,x_n]$ sind äquivalent:*

1. *Jedes Polynom f in $\mathbf{K}[x_1,\ldots,x_n]$ hat eine eindeutige Normalform bezüglich Reduktion mit Polynomen aus G unabhängig von der gewählten Reduktionsstrategie.*
2. $\mathsf{HT}(\langle G\rangle\backslash\{0\}) = \{t \circ s \mid t \in \mathsf{HT}(G), s \in \mathsf{T}^n\}$.
3. *Für alle f und g aus G, $f \neq g$, gilt $\mathsf{spol}(f,g) \xrightarrow{*}_G 0$.*
4. *$\xleftrightarrow{*}_G$ erfaßt die Idealkongruenz von $\langle G\rangle$, und $\longrightarrow_G$ ist konfluent.*
5. *Jedes f aus $\langle G\rangle$ hat eine Darstellung der Form $f = \sum_{i=1}^{k} a_i \cdot g_i * s_i$ mit $a_i \in \mathbf{K}$, $g_i \in G$, $s_i \in \mathsf{T}^n$, und $\mathsf{HT}(g_i * s_i) \leq \mathsf{HT}(f)$ für alle $1 \leq i \leq k$.*
6. *Für alle f aus $\langle G\rangle$ gilt $f \xrightarrow{*}_G 0$.*

Beweis :
$1 \Longrightarrow 2$:
Nach Lemma 2.3.2 beschreibt die Reduktion $\longrightarrow_G$ die Idealkongruenz von $\langle G\rangle$, d.h. es gilt $f \xleftrightarrow{*}_G g$ genau dann, wenn f und g in der gleichen Äquivalenzklasse modulo $\langle G\rangle$ liegen. Da insbesondere 0 in $\langle G\rangle$ liegt, gilt für jedes f aus $\langle G\rangle$, $f \xleftrightarrow{*}_G 0$. Wir zeigen, daß dies $f \xrightarrow{*}_G 0$ impliziert durch Induktion nach n mit $f \xleftrightarrow{n}_G 0$. Ist $n = 1$ so folgt $f \longrightarrow_G 0$ aus der Tatsache, daß $f \longleftrightarrow_G 0$ und 0 irreduzibel ist. Sei also $f \longleftrightarrow_G g \xleftrightarrow{n-1}_G 0$. Dann impliziert die Induktionshypothese $g \xrightarrow{*}_G 0$. Gilt $f \longrightarrow_G g$ so sind wir fertig. Gilt jedoch $g \longrightarrow_G f$, so muß 0 auch Normalform von f sein, da 0 eine Normalform von g war und diese eindeutig ist laut Voraussetzung. Insbesondere gilt dann auch, daß jedes Polynom des Ideals mit Reduktionen, die zuerst immer den Kopfterm reduzieren, nach Null reduzibel sein muß. Daher folgt $\mathsf{HT}(\langle G\rangle\backslash\{0\}) \subseteq \{t \circ s \mid t \in \mathsf{HT}(G), s \in \mathsf{T}^n\}$. Die Umkehrung gilt sofort, da für alle $s \in \mathsf{T}^n$, $g * s$ im Ideal $\langle G\rangle$ liegen muß.
$2 \Longrightarrow 3$:
Die Tatsachen, daß jeder Kopfterm eines Polynoms aus dem Ideal $\langle G\rangle$ zu den mit G reduziblen Termen gehört und daß die Reduktion eines Polynoms des Ideals wieder zu einem Polynom des Ideals führt, implizieren, daß jedes Polynom des Ideals sich zu Null reduzieren läßt. Da insbesondere für f und g aus G das s-Polynom im Ideal $\langle G\rangle$ liegt, gilt die Behauptung.
$3 \Longrightarrow 4$:
Daß die Reduktion die Idealkongruenz erfaßt, folgt aus Lemma 2.3.2. Um Konfluenz zu zeigen, reicht es, lokale Konfluenz auf Termen zu zeigen, da Reduktion eines Polynoms an verschiedenen Termen immer aufgelöst werden kann. Weiterhin ist ein Term, der mit zwei verschiedenen Polynomen f und g reduzibel ist, ein Termvielfaches des $\mathsf{kgV}(\mathsf{HT}(f), \mathsf{HT}(g))$. Es ist also Konfluenz für den Term $t = \mathsf{kgV}(\mathsf{HT}(f), \mathsf{HT}(g)) \circ s = \mathsf{HT}(f) \circ s_1 = \mathsf{HT}(g) \circ s_2$ nachzuweisen. Dann gilt

$$t \longrightarrow_f t - \mathsf{HC}(f)^{-1} \cdot f * s_1 \text{ und } t \longrightarrow_g t - \mathsf{HC}(g)^{-1} \cdot g * s_2.$$

Weiter erhalten wir

$$\begin{aligned} & -(t - \mathsf{HC}(f)^{-1} \cdot f * s_1) + (t - \mathsf{HC}(g)^{-1} \cdot g * s_2) \\ = \ & \mathsf{HC}(f)^{-1} \cdot f * s_1 - \mathsf{HC}(g)^{-1} \cdot g * s_2 \\ = \ & \mathsf{spol}(f, g) * s. \end{aligned}$$

Aus $\mathsf{spol}(f, g) \xrightarrow{*}_G 0$ folgt $\mathsf{spol}(f, g) * s \xrightarrow{*}_G 0$, und somit sind die Polynome $t - \mathsf{HC}(f)^{-1} \cdot f * s_1$ und $t - \mathsf{HC}(g)^{-1} \cdot g * s_2$ zusammenführbar (vergleiche die Resulate von Lemma 2.3.2).

$4 \Longrightarrow 5$:

Aus der Konfluenz der Reduktion und der Existenz der Null als Normalform der Elemente aus dem Ideal folgt, daß jedes f aus $\langle G \rangle$ zu Null reduzibel ist, und man kann sich als Strategie auf Reduktionen am Kopf der Polynome zurückziehen. Diese Form der Reduktion impliziert direkt eine Darstellung der Form $f = \sum_{i=1}^{k} a_i \cdot g_i * s_i$ mit $a_i \in \mathbf{K}$, $g_i \in G$, $s_i \in \mathsf{T}^n$ und $\mathsf{HT}(g_i * s_i) \leq \mathsf{HT}(f)$ für alle $1 \leq i \leq k$.

$5 \Longrightarrow 6$:

Dies folgt unmittelbar aus der Darstellung der Idealelemente, da der jeweilige Kopfterm immer einen Kopfterm eines Polynoms aus G als Teiler hat und somit jedes Polynom im Ideal außer der Null am Kopf reduzibel sein muß. Somit kann nur Null eine Normalform für Idealelemente sein.

$6 \Longrightarrow 1$:

Nehmen wir an, ein Polynom f habe zwei verschiedene Normalformen f_1 und f_2 bezüglich G. Dann liegt $f_1 - f_2$ in dem von G erzeugten Ideal, da $f \xrightarrow{*}_F f_1$ und $f \xrightarrow{*}_F f_2$ $f_1 \xleftrightarrow{*}_F f_2$ impliziert. Dann folgt jedoch aus $f_1 \neq f_2$ daß $f_1 - f_2 \xrightarrow{*}_F 0$ und nach Lemma 2.3.2 die Existenz eines Polynoms h, so daß $f_1 \xrightarrow{*}_F h$ und $f_2 \xrightarrow{*}_F h$ gelten muß im Widerspruch zu der Tatsache, daß f_1 und f_2 beide in Normalform sein sollen.

q.e.d.

Übungen

1. Es sei G eine Gröbnerbasis und f, g Polynome in $\mathbf{K}[x_1, \ldots, x_n]$, wobei g bezüglich G reduziert ist. Zeigen Sie, daß $f - g \in \langle G \rangle$ impliziert $f \xrightarrow{*}_G g$. ✓

2. Es seien G und G' zwei Gröbnerbasen desselben Ideals bezüglich einer Termordnung und f ein Polynom aus $\mathbf{K}[x_1, \ldots, x_n]$. Zeigen Sie, daß für die Normalformen g beziehungsweise g' von f bezüglich G beziehungsweise G' gilt: $g = g'$. ✓

2.5 Buchbergers Algorithmus

Wie wir im vorherigen Abschnitt gesehen haben, liefert Buchbergers Charakterisierung der Gröbnerbasen über s-Polynome einen konstruktiven Zugang zu ihrer Berechnung. Im Prinzip findet eine Vervollständigung einer Reduktionsrelation statt. Für eine endliche Basis eines Ideals wird ein Test auf lokale Konfluenz durchgeführt, und falls die Basis noch nicht lokal konfluent ist, wird sie so lange transformiert, bis wir unser Ziel erreicht haben.

Buchbergers Algorithmus

Eingabe: Eine endliche Menge von Polynomen F aus $\mathbf{K}[x_1, \ldots, x_n]$.
Ausgabe: Eine Gröbnerbasis G von $\langle F \rangle$.

```
G := F;
B := {(f,g) | f,g ∈ G, f ≠ g};
while B ≠ ∅ do
    wähle ein Paar (f,g) aus B;
    B := B\{(f,g)};
    h := spol(f,g);
    h := NORMALFORM(h,G);
    if h ≠ 0 then
        B := B ∪ {(f,h) | f ∈ G};
        G := G ∪ {h};
    endif
endwhile
```

Setzt man voraus, daß bei der Auswahl von Paaren aus der Menge B eine faire Strategie benutzt wird, d.h. jedes Paar, welches in die Menge eingefügt wird, wird auch zu einem bestimmten Zeitpunkt zur s-Polynombildung herangezogen, so wird deutlich, daß dieser Prozeß eine Gröbnerbasis aufzählt.

Satz 2.5.1 *Dieser Algorithmus ist total korrekt.*

Beweis :
Falls dieser Algorithmus terminiert, so berechnet er eine Menge von Polynomen G mit $F \subseteq G$ und $\langle F \rangle = \langle G \rangle$. Weiterhin gilt für alle Polynome f, g in G, $\mathsf{spol}(f, g) \xrightarrow{*}_G 0$, und somit ist G nach Buchbergers Charakterisierung eine Gröbnerbasis. Es bleibt also, die Terminierung zu zeigen. Dies kann mittels Dicksons Lemma geschehen. Betrachtet man nämlich die Menge $\mathsf{HT}(\langle F \rangle \backslash \{0\})$, so ist dies eine (unendliche) Teilmenge von Termen aus T^n. Diese enthält nun eine endliche Teilmenge S, so daß jeder Kopfterm eines Polynoms aus dem Ideal $\langle F \rangle$ von einem Term aus S geteilt wird. Da unser Algorithmus eine Gröbnerbasis erzeugt, wissen wir, daß es für jeden Term s aus S irgendwann ein Polynom g_s in G geben wird, dessen Kopfterm s teilt. Wenn nun die Menge G zu einem Zeitpunkt zu jedem s in S ein solches Polynom g_s enthält, so wird von diesem

Zeitpunkt an kein weiteres Polynom mehr in G aufgenommen. Dies folgt daraus, daß die gebildeten s-Polynome Elemente des Ideals $\langle F\rangle$ sind und somit sowohl ihr Kopfterm als auch alle Kopfterme der durch Reduktion mit G entstehenden Folgepolynome von einem Term in S geteilt werden und somit wieder mit G reduzibel sein müssen. Somit muß ihre Normalform bezüglich G Null sein. Dann wird jedoch auch die Menge B nur noch verkleinert, d.h. der Algorithmus wird terminieren.

q.e.d.

Zur Illustration des Vorgehens des Algorithmus ein Beispiel.

Wir berechnen die Gröbnerbasis des Ideals, das von den Polynomen $f_1 = x^2y + 2 \cdot x$ und $f_2 = y^2 + x$ aus $\mathbf{Q}[x, y]$ erzeugt wird. Dabei setzen wir als Termordnung die länge-lexikographische Ordnung induziert von $x > y$ voraus. Wir erhalten:
$G := \{f_1, f_2\}$;
$B := \{(f_1, f_2)\}$; (das symmetrische Paar (f_2, f_1) führt zum s-Polynom $\mathsf{spol}(f_2, f_1) = -\mathsf{spol}(f_1, f_2)$ und kann daher vernachlässigt werden, ebenso wie s-Polynome von Paaren (f, f))
Für das Paar (f_1, f_2) bestimmen wir das s-Polynom $h := (x^2y+2\cdot x)*y-(y^2+x)*x^2 = -x^3 + 2 \cdot xy$, welches bezüglich G irreduzibel ist.
Wir erhalten nun:
$G := G \cup \{-x^3 + 2 \cdot xy\}$;
$B := \{(f_1, -x^3 + 2 \cdot xy), (f_2, -x^3 + 2 \cdot xy)\}$;
Für das Paar $(f_1, -x^3 + 2 \cdot xy)$ bestimmen wir das s-Polynom $h = (x^2y + 2 \cdot x) * x - (x^3 - 2 \cdot xy) * y = 2 \cdot xy^2 + 2 \cdot x^2$, welches sich mit f_2 aus G zu Null reduziert.
Für das Paar $(f_2, -x^3 + 2 \cdot xy)$ bestimmen wir das s-Polynom $h = (y^2 + x) * x^3 - (x^3 - 2 \cdot xy) * y^2 = x^4 + 2 \cdot xy^3$, welches sich mit f_2 und $x^3 - 2 \cdot xy$ zu Null reduzieren läßt.
Somit ist B leer, und wir erhalten die Gröbnerbasis $G = \{x^2y+2\cdot x, y^2+x, x^3-2\cdot xy\}$.

Ebenso ist jedoch die Menge $\{x^2y+2\cdot x, y^2+x, x^3-2\cdot xy, x^4+2\cdot xy^3\}$ eine Gröbnerbasis des Ideals $\langle G\rangle$, und wir sehen, daß Gröbnerbasen im Allgemeinen nicht eindeutig sein müssen. Im nächsten Abschnitt werden wir Bedingungen für die Eindeutigkeit solcher Basen liefern.

Übungen

1. Berechnen Sie die Gröbnerbasis des von $2 \cdot xy^2 + 3 \cdot x + 4 \cdot y^2$ und $y^2 - 2 \cdot y - 2$ in $\mathbf{Q}[x, y]$ erzeugten Ideals bezüglich ◷
   (a) der von $x > y$ induzierten lexikographischen Termordnung,
   (b) der von $x > y$ induzierten länge-lexikographischen Termordnung.
2. Zeigen Sie, wie die Schritte des Euklid'schen Algorithmus zu Buchbergers Algorithmus korrespondieren (vergleiche Abschnitt 1.4). ☼
3. Zeigen Sie, wie die Schritte der Gauß-Elimination zu Buchbergers Algorithmus korrespondieren (vergleiche Abschnitt 1.3). ☼

4. Es sei F eine endliche Menge von Polynomen in $\mathbf{K}[x_1,\ldots x_n]$, deren Elemente Differenzen zweier Terme sind, d.h. von der Gestalt $s-t$ oder $-s+t$ mit $s,t\in\mathsf{T}^n$. Zeigen Sie, daß bezüglich jeder Termordnung das von F erzeugte Ideal eine Gröbnerbasis hat, deren Elemente wiederum nur Polynome sind, die Differenzen zweier Terme sind. ☼

2.6 Reduzierte Gröbnerbasen

Buchbergers Algorithmus berechnet für eine Menge von Polynomen F eine Gröbnerbasis des Ideals $\langle F\rangle$. Da jedoch sowohl die Wahl des nächsten zu bearbeitenden Paares aus der Menge B als auch die Normalformberechnung nicht festgelegt sind, ist die resultierende Basis im Allgemeinen nicht eindeutig. Daher führen wir hier den Begriff der reduzierten Basen ein.

Definition 2.6.1 *Eine Menge von Polynomen heißt* **reduziert**, *falls kein Polynom in der Menge von den anderen Polynomen der Menge reduziert werden kann.*

Gröbnerbasen haben nun folgende wichtige Eigenschaft, die es erlaubt, aus einer Gröbnerbasis eine reduzierte Gröbnerbasis des gleichen Ideals zu berechnen.

Lemma 2.6.2 *Es sei G eine Gröbnerbasis, und für zwei verschiedene Polynome f und g aus G gelte $f\longrightarrow_g h$. Dann ist die Menge $G' := (G\backslash\{f\})\cup\{h\}$ wieder eine Gröbnerbasis von $\langle G\rangle$.*

Lemma 2.6.3 *Es sei G eine Gröbnerbasis, und für zwei verschiedene Polynome f und g aus G gelte, daß der Kopfterm $\mathsf{HT}(f)$ den Kopfterm $\mathsf{HT}(g)$ teilt. Dann ist die Menge $G' := G\backslash\{g\}$ bereits eine Gröbnerbasis von $\langle G\rangle$.*

Die Gültigkeit beider Lemmata folgt sofort, wenn man sich an die Charakterisierung von Gröbnerbasen über die Kopfterme des Ideals erinnert. Es gilt nämlich in beiden Fällen,

$$\mathsf{HT}(\langle G\rangle\backslash\{0\}) = \{t\circ s \mid t\in\mathsf{HT}(G'), s\in\mathsf{T}^n\}.$$

Somit kann aus einer beliebigen Gröbnerbasis durch Reduktion eine reduzierte Gröbnerbasis berechnet werden. Reduzierte Gröbnerbasen sind eindeutig, wenn man zusätzlich verlangt, daß die Polynome monisch sind, d.h. auf 1 normierte Kopfkoeffizienten haben.

Satz 2.6.4 *Jedes Ideal in $\mathbf{K}[x_1,\ldots,x_n]$ hat eine eindeutige normierte reduzierte Gröbnerbasis (bezüglich der gewählten Termordnung).*

Beweis :
O.B.d.A. nehmen wir an, das Ideal sei nicht trivial. Die Existenz reduzierter Gröbnerbasen folgt aus Hilberts Basissatz (Satz 1.1.2) und den vorherigen Lemmata, und ihre

Normierung erfolgt durch Multiplikation mit dem Inversen des respektiven Kopfkoeffizienten. Um die Eindeutigkeit zu zeigen, nehmen wir an, es gäbe zwei normierte reduzierte Gröbnerbasen G und H des Ideals. Da $G \neq H$ gelten soll, gibt es ein h, welches o.B.d.A in $H \backslash G$ liegt. Da G auch eine Gröbnerbasis des gleichen Ideals ist, muß es ein Polynom g in G geben, dessen Kopfterm $\mathsf{HT}(g)$ den Kopfterm $\mathsf{HT}(h)$ teilt. Da dann auch H wiederum ein Polynom enthalten muß, dessen Kopfterm den Term $\mathsf{HT}(g)$ teilt und H reduziert ist, muß $\mathsf{HT}(g) = \mathsf{HT}(h)$ gelten. Da beide Mengen zusätzlich normiert sind, wissen wir, daß der Kopfterm des Polynoms $g-h$ kleiner als $\mathsf{HT}(h)$ ist. Gleichzeitig impliziert $g \neq h$ $g - h \neq 0$, und da $g - h$ wieder im Ideal $\langle G \rangle$ liegt, gibt es Polynome sowohl in G als auch in H, welche $g - h$ reduzieren. Dies impliziert jedoch, daß entweder g mit G oder h mit H reduzibel sein muß, im Widerspruch zu der Annahme, daß beide Basen reduziert waren.

q.e.d.

Übungen

1. Modifizieren Sie Buchbergers Algorithmus so, daß er normierte reduzierte Gröbnerbasen berechnet. ☼

2. Ersetzen Sie in Lemma 2.6.2 und Lemma 2.6.3 den Begriff „Gröbnerbasis" durch „Idealbasis". Gelten die Aussagen immer noch? ☼

3. Zeigen Sie: Sind zwei Polynommengen G und H reduzierte Gröbnerbasen desselben Ideals so gilt $|G| = |H|$ und $\mathsf{HT}(G) = \mathsf{HT}(H)$. ☼

Kapitel 3

Anwendungen von Gröbnerbasen

Der Worte sind genug gewechselt!
laßt mich auch endlich Taten seh'n!

GOETHE

3.1 Einfache Folgerungen

Aus den verschiedenartigen Charakterisierungen von Gröbnerbasen, die wir im vorherigen Kapitel kennengelernt haben, lassen sich Eigenschaften ableiten, die direkte Lösungen für idealtheoretische Probleme in $\mathbf{K}[x_1, \ldots, x_n]$ liefern.

GLEICHHEITSPROBLEM

Gegeben:		Zwei endliche Idealbasen F und G aus $\mathbf{K}[x_1, \ldots, x_n]$.
Frage:		Gilt $\langle F \rangle = \langle G \rangle$?
Vorgehen:	1.	Bestimme für die Ideale $\langle F \rangle$ und $\langle G \rangle$ normierte reduzierte Gröbnerbasen F' und G'.
	2.	Es gilt $\langle F \rangle = \langle G \rangle$ genau dann, wenn $F' = G'$.

Ein eng verwandtes Problem erhält man, wenn man im Gleichheitsproblem für zwei Ideale eines der Ideale als trivial, d.h. als gesamt $\mathbf{K}[x_1, \ldots, x_n]$, annimmt.

TRIVIALITÄTSPROBLEM

Gegeben:		Eine endliche Idealbasis F aus $\mathbf{K}[x_1, \ldots, x_n]$.
Frage:		Ist $\langle F \rangle = \langle 1 \rangle = \mathbf{K}[x_1, \ldots, x_n]$?
Vorgehen:	1.	Bestimme die normierte reduzierte Gröbnerbasis F' von $\langle F \rangle$.
	2.	Es gilt $\langle F \rangle = \langle 1 \rangle$ genau dann, wenn $F' = \{1\}$.

Alternativ kann man auch eine beliebige Gröbnerbasis F' von $\langle F \rangle$ bestimmen und testen, ob sich 1 mit F' zu Null reduzieren läßt. Dies ist genau dann der Fall, wenn F' ein Element aus $\mathbf{K}\backslash\{0\}$ enthält.

UNTERIDEALPROBLEM

Gegeben: Zwei endliche Idealbasen F und G aus $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gilt $\langle F\rangle \subseteq \langle G\rangle$?

Vorgehen:
1. Bestimme für das Ideal $\langle G\rangle$ eine Gröbnerbasis G'.
2. Es gilt $\langle F\rangle \subseteq \langle G\rangle$ genau dann, wenn jedes Polynom aus F sich bezüglich G' nach Null reduzieren läßt.

Dieses Vorgehen kann natürlich auch benutzt werden, um das Gleichheitsproblem für Ideale mittels beliebiger Gröbnerbasen der Ideale zu lösen, da gilt $\langle F\rangle = \langle G\rangle$ genau dann, wenn $\langle F\rangle \subseteq \langle G\rangle$ und $\langle G\rangle \subseteq \langle F\rangle$.

Eines der wichtigsten Probleme für Ideale ist die Frage, ob ein Polynom in einem gegebenen Ideal liegt.

ENTHALTENSEINSPROBLEM

Gegeben: Eine endliche Idealbasis F und ein Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gilt $f \in \langle F\rangle$?

Vorgehen:
1. Bestimme eine Gröbnerbasis F' von $\langle F\rangle$.
2. Es gilt $f \in \langle F\rangle$ genau dann, wenn f sich mit F' zu Null reduzieren läßt.

Eng verwandt mit diesem Problem ist die Frage nach der Darstellung eines Idealelementes bezüglich einer gegebenen Idealbasis. Besonders einfach ist die Antwort, wenn die Idealbasis eine Gröbnerbasis ist.

DARSTELLUNGSPROBLEM

Gegeben: Eine Gröbnerbasis F in $\mathbf{K}[x_1, \ldots, x_n]$ und ein Polynom f aus $\langle F\rangle$.

Aufgabe: Stelle f als Linearkombination der Polynome in F dar.

Vorgehen: Reduziere f bezüglich F nach Null. Die dabei in den einzelnen Reduktionsschritten benutzten Vielfache der Polynome aus F liefern eine Linearkombination.

Dieses Darstellungsproblem kann auch bezüglich einer beliebigen endlichen Idealbasis formuliert werden. Dann benötigt man eine modifizierte Version von Buchbergers Algorithmus, die neben einer Gröbnerbasis auch für jedes Element dieser Basis die Linearkombination aus den ursprünglichen Elementen speichert. Dies ist möglich, da ein solches „Merken" der beteiligten Polynome und ihrer Multiplikatoren in die Funktionen zur Normalformbestimmung und zur s-Polynombestimmung eingebaut werden kann (vergleiche die Normalformbestimmung in $\mathbf{K}[x]$ auf Seite 15, die genau um eine solche Komponente erweitert wurde). Diese Linearkombinationen der Gröbnerbasenelemente in den ursprünglichen Polynomen werden dann in die durch Nullreduktion für das gewünschte Idealelement bestimmte Linearkombination eingesetzt, und somit kann durch geeignetes Ausmultiplizieren die gewünschte Darstellung bestimmt werden. Dies geschieht wie folgt: Es sei $F = \{f_1, \ldots, f_k\}$ die ursprüngliche Idealbasis und $G = \{g_1, \ldots, g_s\}$ eine Gröbnerbasis mit $g_i = \sum_{j=1}^{k} h_j^i * f_j$, $h_j^i \in \mathbf{K}[x_1, \ldots, x_n]$ für $1 \leq i \leq s$. Ergibt sich für ein Polynom f aus $\langle F \rangle$ nun durch Reduktion $f \xrightarrow{*}_G 0$ eine Linearkombination $f = \sum_{l=1}^{s} h_l * g_l$, $h_l \in \mathbf{K}[x_1, \ldots, x_n]$ so erhalten wir

$$\begin{aligned} f = \sum_{l=1}^{s} h_l * g_l &= \sum_{l=1}^{s} h_l * (\sum_{j=1}^{k} h_j^l * f_j) \\ &= \sum_{l=1}^{s} (\sum_{j=1}^{k} h_l * h_j^l * f_j) \\ &= \sum_{j=1}^{k} \sum_{l=1}^{s} (h_l * h_j^l) * f_j \\ &= \sum_{j=1}^{k} (\sum_{l=1}^{s} h_l * h_j^l) * f_j, \end{aligned}$$

und somit erhalten wir für f eine Darstellung in den Erzeugenden aus F. Als nächstes formulieren wir ein weiteres Idealproblem, welches eng verwandt ist mit dem Rechnen in Quotientenringen, d.h. in Quotienten des Polynomrings $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$, wobei $\mathfrak{i}$ ein Ideal ist.

Kongruenzproblem

Gegeben:		Eine endliche Idealbasis F und zwei Polynome f und g aus $\mathbf{K}[x_1, \ldots, x_n]$.
Frage:		Ist f kongruent zu g bezüglich $\langle F \rangle$, d.h. sind die Polynome f und g im Quotienten $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ „gleich”?
Vorgehen:	1.	Bestimme eine Gröbnerbasis F' von $\langle F \rangle$.
	2.	f ist genau dann kongruent zu g bezüglich $\langle F \rangle$, wenn sich die Differenz $f - g$ bezüglich F' nach Null reduzieren läßt.

Eine andere Möglichkeit, auf Kongruenz modulo eines Ideals zu testen, ist, die Normalformen bezüglich der Reduktion mit einer Gröbnerbasis des Ideals zu bestimmen. Diese müssen nämlich für Elemente einer Nebenklasse übereinstimmen. Diese Eigenschaft liefert eine Lösung für das nächste Problem.

Repräsentantenproblem

Gegeben:		Eine endliche Idealbasis F und ein Polynom f in $\mathbf{K}[x_1, \ldots, x_n]$.
Aufgabe:		Bestimme einen eindeutigen Repräsentanten von f modulo $\langle F \rangle$.
Vorgehen:	1.	Bestimme eine Gröbnerbasis F' von $\langle F \rangle$.
	2.	Berechne als eindeutigen Repräsentanten die Normalform von f bezüglich F'.

Im nächsten Abschnitt wollen wir kurz skizzieren, wie solche eindeutigen Repräsentanten das effektive Rechnen in Quotientenringen ermöglichen.

Übungen

☼ 1. Zeigen Sie, wie das Wortproblem für ein kommutatives Monoid in den Erzeugenden $x_1, \ldots, x_n$ mit Darstellung $\{l_i = r_i \mid l_i, r_i \in \mathsf{T}^n, 1 \leq i \leq k, k \in \mathbf{N}\}$ mit Hilfe elementarer Gröbnerbasenmethoden lösbar ist. (Hinweis: Übungsaufgabe 4 in Abschnitt 2.5)

3.2 Quotientenringe

In diesem Abschnitt wollen wir zeigen, wie Gröbnerbasen eingesetzt werden können, um in Quotientenringen zu rechnen. Dies war Buchbergers Aufgabenstellung, die zur Entwicklung der Gröbnerbasen führte.

Im Folgenden sei $\mathfrak{i}$ ein Ideal in $\mathbf{K}[x_1, \ldots, x_n]$ und $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ der Quotientenring von $\mathbf{K}[x_1, \ldots, x_n]$ modulo $\mathfrak{i}$. Der kanonische Homomorphismus von $\mathbf{K}[x_1, \ldots, x_n]$ nach $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ ist definiert durch

$$f \longmapsto [f]_{\mathfrak{i}}$$

wobei $[f]_{\mathfrak{i}} = f + \mathfrak{i}$ die Nebenklasse von f modulo $\mathfrak{i}$ bezeichnet. Die Ringoperationen werden durch

$$[f]_{\mathfrak{i}} + [g]_{\mathfrak{i}} = [f + g]_{\mathfrak{i}},$$

$$[f]_{\mathfrak{i}} * [g]_{\mathfrak{i}} = [f * g]_{\mathfrak{i}}$$

definiert. Im Folgenden sei nun das Ideal $\mathfrak{i}$ durch eine Gröbnerbasis G gegeben. Dann können wir in den Nebenklassen $[f]_{\mathfrak{i}}$ als Repräsentanten die Normalform eines Polynoms der Nebenklasse bezüglich G auszeichnen, d.h. der Repräsentant von $[f]_{\mathfrak{i}}$ ist gerade $\textsc{Normalform}(f, G)$. Da G eine Gröbnerbasis ist, sind die gewählten Repräsentanten eindeutig, und unsere Ringoperationen lassen sich wie folgt effektiv formulieren:

$$[f]_{\mathfrak{i}} + [g]_{\mathfrak{i}} := \textsc{Normalform}(f + g, G),$$

$$[f]_{\mathfrak{i}} * [g]_{\mathfrak{i}} := \textsc{Normalform}(f * g, G).$$

Quotientenringe können als $\mathbf{K}$-Vektorräume aufgefaßt werden und erlauben eine einfache Charakterisierung ihrer Vektorraumbasis.

Lemma 3.2.1 *Für jedes Ideal $\mathfrak{i} \subseteq \mathbf{K}[x_1, \ldots, x_n]$ gilt:*

1. *$\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ ist ein $\mathbf{K}$-Vektorraum.*

2. *Die Menge $B = \{[t]_{\mathfrak{i}} \mid t \in \mathsf{T}^n\}$ ist eine (unabhängige) Basis dieses Vektorraums.*

Beweis :

1. Zur Erinnerung ist $V = \mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ ein $\mathbf{K}$-Vektorraum, wenn folgende Eigenschaften erfüllt sind:

   (a) Es gibt eine Abbildung $K \times V \longrightarrow V$, $(a, [f]_\mathfrak{i}) \longmapsto a \cdot [f]_\mathfrak{i}$ eine sogenannte Multiplikation mit Skalaren.

   (b) $(a \cdot b) \cdot [f]_\mathfrak{i} = a \cdot (b \cdot [f]_\mathfrak{i})$ für alle $a, b \in \mathbf{K}$, $[f]_\mathfrak{i} \in V$.

   (c) $a \cdot ([f]_\mathfrak{i} + [g]_\mathfrak{i}) = a \cdot [f]_\mathfrak{i} + a \cdot [g]_\mathfrak{i}$ für alle $a \in \mathbf{K}$, $[f]_\mathfrak{i}, [g]_\mathfrak{i} \in V$.

   (d) $(a + b) \cdot [f]_\mathfrak{i} = a \cdot [f]_\mathfrak{i} + b \cdot [f]_\mathfrak{i}$ für alle $a, b \in \mathbf{K}$, $[f]_\mathfrak{i} \in V$.

   (e) $1 \cdot [f]_\mathfrak{i} = [f]_\mathfrak{i}$ für alle $[f]_\mathfrak{i} \in V$.

   Man rechnet nun leicht nach, daß dies für folgende natürliche Definition der Skalarmultiplikation erfüllt ist:

   $$a \cdot [f]_\mathfrak{i} := [a \cdot f]_\mathfrak{i}$$

   für $a \in \mathbf{K}$, $[f]_\mathfrak{i} \in V$.

2. Man sieht sofort, daß B den Quotienten $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ bezüglich Multiplikation mit Elementen aus $\mathbf{K}$ erzeugt. Daher bleibt zu zeigen, daß B auch linear unabhängig ist. Im Folgenden sei G eine Gröbnerbasis von $\mathfrak{i}$. Als Repräsentanten der Elemente aus B können daher die Normalformen $\{\hat{t} = \text{NORMALFORM}(t, G) \mid t \in \mathsf{T}^n\}$ gewählt werden. Gilt nun für $a_i \in \mathbf{K}$ und $[t_i]_\mathfrak{i}$, $1 \leq i \leq k$, $\sum_{i=1}^{k} a_i \cdot [t_i]_\mathfrak{i} = 0$, so gilt auch $\text{NORMALFORM}(\sum_{i=1}^{k} a_i \cdot \hat{t_i}, G) = 0$. Da jedoch die Elemente $\hat{t_i}$ bereits in Normalform bezüglich G sind, müssen die in der Summe vorkommenden a_i alle gleich Null sein, d.h. die Basiselemente sind unabhängig.

q.e.d.

Im Beweis der zweiten Aussage dieses Lemmas haben wir gesehen, wie Gröbnerbasen benutzt werden können, um eine (nicht notwendigerweise) endliche $\mathbf{K}$-Vektorraumbasis eines Quotientenringes zu bestimmen. Zu einer solchen Basis kann dann eine Multiplikationstafel aufgestellt werden, wiederum mittels Normalformbestimmung, da gilt $[t_i]_\mathfrak{i} * [t_j]_\mathfrak{i} = [t_i \circ t_j]_\mathfrak{i} = \text{NORMALFORM}(t_i \circ t_j, G)$.

Wir werden im nächsten Abschnitt sehen, daß eine $\mathbf{K}$-Vektorraumbasis B eines Quotientenringes $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ genau dann endlich ist, wenn $\mathfrak{i}$ nulldimensional ist, d.h. das Nullstellengebilde endlich ist.

Übungen

1. Bestimmen Sie zu $f_1 = x^3y^2z - xz^2$, $f_2 = xy^2z - xyz$ und $f_3 = x^2y^2 - z^2$ eine Basis des Quotientenrings als $\mathbf{K}$-Vektorraum, und stellen Sie die Multiplikationstafel für die Basiselemente auf.

2. Es sei $\mathfrak{i} = \langle F \rangle$ ein Ideal in $\mathbf{K}[x_1, \ldots, x_n]$. Ein Element $[f]_\mathfrak{i}$ heißt invertierbar in $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ genau dann, wenn es ein $[g]_\mathfrak{i}$ gibt mit $[g * f]_\mathfrak{i} = [1]_\mathfrak{i}$. Zeigen Sie, wie man zu gegebenem Polynom f und endlicher Idealbasis F aus $\mathbf{K}[x_1, \ldots, x_n]$ entscheiden kann, ob $[f]_{\langle F \rangle}$ invertierbar ist. ☼
   Hinweis: Es sei z eine neue Variable. Überlegen Sie, welche Eigenschaften eine Gröbnerbasis des Ideals $\langle F \cup \{f * z - 1\} \rangle$ bezüglich einer lexikographischen Ordnung mit Präzedenz $z > x_1 > \ldots > x_n$ hat.

3.3 Eliminationseigenschaften

Benutzt man spezielle Termordnungen, Eliminationsordnungen genannt, so erhält man weitere nützliche Eigenschaften von Gröbnerbasen, welche es erlauben, Informationen über das zu einem Ideal assoziierte Nullstellengebilde abzulesen.

Im Folgenden seien in diesem Abschnitt $X = \{x_1, \ldots, x_n\}$ und $Y = \{y_1, \ldots, y_m\}$ zwei disjunkte Mengen von Variablen und $\geq_X$ beziehungsweise $\geq_Y$ Termordnungen auf den jeweiligen Mengen von Termen, die wir hier zur Unterscheidung mit $\mathsf{T}^n(X)$ und $\mathsf{T}^m(Y)$ bezeichnen wollen.

$$\mathsf{T}^{n+m}(X, Y) = \{x_1^{i_1} \ldots x_n^{i_n} y_1^{j_1} \ldots y_m^{j_m} \mid i_1, \ldots, i_n, j_1, \ldots, j_m \in \mathbf{N}\}$$

bezeichnet die Menge der Terme über den Variablen $X \cup Y$. Dann können wir das lexikographische Produkt $\geq_{X,Y}$ dieser beiden Ordnungen wie folgt definieren:

Definition 3.3.1 *Es seien $t_1 = x_1^{i_1} \ldots x_n^{i_n} y_1^{j_1} \ldots y_m^{j_m}$ und $t_2 = x_1^{k_1} \ldots x_n^{k_n} y_1^{l_1} \ldots y_m^{l_m}$ zwei Terme aus $T^{n+m}(X, Y)$. Dann gilt $t_1 \geq_{X,Y} t_2$ genau dann, wenn $x_1^{i_1} \ldots x_n^{i_n} \geq_X x_1^{k_1} \ldots x_n^{k_n}$ oder ($x_1^{i_1} \ldots x_n^{i_n} = x_1^{k_1} \ldots x_n^{k_n}$ und $y_1^{j_1} \ldots y_m^{j_m} \geq_Y y_1^{l_1} \ldots y_m^{l_m}$).*

Eine solche Ordnung wird auch **Eliminationsordnung** oder Blockordnung mit X größer Y genannt. Als Beispiele für Eliminationsordnungen haben wir bereits die lexikographischen Ordnungen kennengelernt (vergleiche Definition 2.1.2).

Bisher haben wir immer Ideale bezüglich des fest gewählten Grundringes $\mathbf{K}[x_1, \ldots, x_n]$ betrachtet. Betrachtet man nun eine Polynommenge aus $\mathbf{K}[X]$, so kann man diese auch als Polynommenge aus $\mathbf{K}[X, Y]$ auffassen und sich das von der Polynommenge erzeugte Ideal in dem respektiven Ring betrachten. Um solche Ideale zu unterscheiden, beschreiben wir für eine Menge S eines Ringes R mit $\langle S \rangle_R$ das von S in R erzeugte Ideal. Ist nun $R \subseteq R'$, so gilt für die von S in R beziehungsweise R' erzeugten Ideale $\langle S \rangle_R \subseteq \langle S \rangle_{R'}$. Das nächste Lemma zeigt nun einen der großen Vorteile von Gröbnerbasen bezüglich Eliminationsordnungen auf.

Lemma 3.3.2 *Es sei G eine Gröbnerbasis in $\mathbf{K}[X, Y]$ bezüglich einer Eliminationsordnung $\geq_{X,Y}$ mit X größer Y. Dann gilt:*

1. $\langle G \rangle_{\mathbf{K}[X,Y]} \cap \mathbf{K}[Y] = \langle G \cap \mathbf{K}[Y] \rangle_{\mathbf{K}[Y]}$.

2. $G \cap \mathbf{K}[Y]$ ist eine Gröbnerbasis für $\langle G \cap \mathbf{K}[Y] \rangle_{\mathbf{K}[Y]}$ bezüglich $\geq_Y$.

Beweis :

1. Aus der Definition eines Ideals folgt sofort $\langle G \cap \mathbf{K}[Y] \rangle_{\mathbf{K}[Y]} \subseteq \langle G \rangle_{\mathbf{K}[X,Y]} \cap \mathbf{K}[Y]$. Um die Umkehrung zu sehen, benutzen wir die Tatsache, daß auf Grund der lexikographischen Produktordnung für ein Polynom f aus $\mathbf{K}[X,Y]$ gilt: $\mathsf{HT}(f) \in \mathsf{T}^m(Y)$ genau dann, wenn $f \in \mathbf{K}[Y]$. Somit kann die Reduktionskette nach Null eines Polynoms aus $\langle G \rangle_{\mathbf{K}[X,Y]} \cap \mathbf{K}[Y]$ nur Polynome aus $G \cap \mathbf{K}[Y]$ benutzen und liefert daher eine Repräsentation von f als Linearkombination von Polynomen aus $G \cap \mathbf{K}[Y]$ mit Multiplikanden aus $\mathbf{K}[Y]$, d.h. es muß auch gelten $\langle G \rangle_{\mathbf{K}[X,Y]} \cap \mathbf{K}[Y] \subseteq \langle G \cap \mathbf{K}[Y] \rangle_{\mathbf{K}[Y]}$.

2. Um zu zeigen, daß $G \cap \mathbf{K}[Y]$ eine Gröbnerbasis von $\langle G \cap \mathbf{K}[Y] \rangle_{\mathbf{K}[Y]}$ bezüglich $\geq_Y$ ist, benutzen wir die Charakterisierung der Gröbnerbasen über die Idealeigenschaft, d.h. darüber, daß sich jedes Polynom aus dem Ideal bezüglich der Gröbnerbasis zu Null reduzieren läßt. Es gilt nämlich, da G Gröbnerbasis für $\langle G \rangle_{\mathbf{K}[X,Y]}$ ist, daß jedes Polynom aus $\langle G \cap \mathbf{K}[Y] \rangle_{\mathbf{K}[Y]}$ sich mit Polynomen aus G zu Null reduzieren lassen muß. Da jedoch wie oben gesehen Polynome mit Kopftermen aus $\mathsf{T}^m(Y)$ aus $\mathbf{K}[Y]$ sein müssen, sind die zur Reduktion benutzten Polynome alle aus $G \cap \mathbf{K}[Y]$, und wir sind fertig.

q.e.d.

Für ein Ideal $\mathfrak{i} \subseteq \mathbf{K}[X,Y]$ ist der Schnitt $\mathfrak{i} \cap \mathbf{K}[Y]$ wieder ein Ideal aufgefaßt als eine Menge aus $\mathbf{K}[Y]$. Dieses Ideal wird **Eliminationsideal** genannt, da in diesem Ideal die Variablen der Menge X „eliminiert" wurden. Wir haben im vorherigen Lemma gesehen, wie solche Eliminationsideale durch Berechnen der Gröbnerbasis bezüglich einer lexikographischen Eliminationsordnung bestimmt werden können. Im Folgenden zeigen wir, wie Gröbnerbasenmethode eingesetzt werden können, um zu testen, ob ein Ideal nulldimensional ist.

Erinnern wir uns zuerst an einige Begriffe, die wir im Einleitungskapitel zur Motivation kennengelernt hatten. F sei eine nichtleere Menge von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$ und $\mathbf{k}$ ein beliebiger Erweiterungskörper von $\mathbf{K}$, d.h. $\mathbf{k}$ ist ein Körper mit $\mathbf{K} \subseteq \mathbf{k}$. Wir definieren als das Nullstellengebilde von F in $\mathbf{k}^n$ die Menge

$$V_{\mathbf{k}}(F) = \{(a_1, \ldots, a_n) \in \mathbf{k}^n \mid f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in F\}.$$

Nullstellengebilde von Idealen sind eindeutig durch eine beliebige Basis des Ideals gekennzeichnet, jedoch wesentlich abhängig von dem gewählten Körper $\mathbf{k}$. Nimmt man z.B. als Körper die reellen Zahlen, so gilt

$$V_{\mathbf{R}}(\{x^2 + y^2\}) = V_{\mathbf{R}}(\{x, y\}) = \{(0,0)\} \subseteq \mathbf{R}^2.$$

Für die komplexen Zahlen gilt jedoch

$$V_{\mathbf{C}}(\{x^2+y^2\}) = \{(\alpha, \sqrt{-1}\cdot\alpha), (\alpha, -\sqrt{-1}\cdot\alpha), (\sqrt{-1}\cdot\alpha, \alpha)(-\sqrt{-1}\cdot\alpha, \alpha) \mid \alpha \in \mathbf{R}\}$$

und

$$V_{\mathbf{C}}(\{x,y\}) = \{(0,0)\}.$$

Dieses Beispiel zeigt, daß zwei Ideale über einem Körper das gleiche Nullstellengebilde beschreiben können, obwohl sie eigentlich doch nicht gleich sind bezüglich anderer Erweiterungskörper. Dieses Phänomen wird uns später wieder bei der Formulierung von Hilberts Nullstellensätzen begegnen und wir werden dort spezielle Erweiterungskörper, nämlich algebraisch abgeschlossene Erweiterungen, kennenlernen.

Wir hatten in der Einleitung auch folgende Abbildungen kennengelernt, die sich für $\mathbf{K}[x_1,\ldots,x_n]$ und $\mathbf{k}^n$ analog definieren lassen:

$$\mathbf{K}[x_1,\ldots,x_n] \supseteq F \longmapsto V_{\mathbf{k}}(F) \subseteq \mathbf{k}^n$$

und

$$\mathbf{k}^n \supseteq N \longmapsto I(N) \subseteq \mathbf{K}[x_1,\ldots,x_n].$$

Insbesondere haben wir im ersten Kapitel über die Zusammenhänge zwischen Nullstellengebilden und Idealen gesprochen und festgestellt, daß zwar $\mathfrak{i} \subseteq I(V_{\mathbf{k}}(\mathfrak{i}))$ gilt, die Umkehrung in der Regel jedoch nicht mehr. Dies liegt daran, daß das Ideal $I(V_{\mathbf{k}}(\mathfrak{i}))$ eine weitere wichtige Eigenschaft hat, die beliebige Ideal nicht haben müssen.

Lemma 3.3.3 *Es sei V eine Varietät und f ein Polynom in $\mathbf{K}[x_1,\ldots,x_n]$. Gibt es ein $m \in \mathbf{N}$ so daß $f^m \in I(V)$, so gilt auch $f \in I(V)$.*

Beweis :
Es sei $(a_1,\ldots,a_n) \in V$ eine beliebige Nullstelle. Gilt nun für $m \in \mathbf{N}$, $f^m \in I(V)$, so gilt auch $(f(a_1,\ldots,a_n))^m = 0$ und somit $f(a_1,\ldots,a_n) = 0$. Da $(a_1,\ldots,a_n)$ beliebig aus V gewählt war, folgt somit $f \in I(V)$.

q.e.d.

Das Ideal, welches alle Polynome enthält, die auf einer Varietät verschwinden, hat somit die Eigenschaft, daß, sobald eine Potenz eines Polynoms in ihm enthalten ist, auch das Polynom selbst darin enthalten ist. Insbesondere sind dann alle Potenzen dieses Polynoms darin enthalten. Daß beliebige Ideale diese Eigenschaft nicht haben müssen, sieht man an folgendem Beispiel: Es gilt sicher nicht, daß das Polynom x im Ideal $\langle x^2\rangle \subseteq \mathbf{K}[x]$ liegt.

Definition 3.3.4 *Ein Ideal $\mathfrak{i}$ aus $\mathbf{K}[x_1,\ldots,x_n]$ heißt* **radikal***, wenn aus $f^m \in \mathfrak{i}$, für $m \in \mathbf{N}$, immer auch $f \in \mathfrak{i}$ folgt.*

Somit ist das Ideal $I(V_{\mathbf{k}}(\mathfrak{i}))$ eigentlich ein radikales Ideal und, falls $\mathfrak{i}$ kein radikales Ideal war, wird folglich $\mathfrak{i} \neq I(V_{\mathbf{k}}(\mathfrak{i}))$ gelten. Ein beliebiges Ideal kann nun in ein radikales Ideal eingebettet werden.

Definition 3.3.5 *Für ein Ideal* $\mathfrak{i}$ *aus* $\mathbf{K}[x_1,\dots,x_n]$ *bezeichnen wir mit der Menge*

$$\sqrt{\mathfrak{i}} = \{f \in \mathbf{K}[x_1,\dots,x_n] \mid \text{ es existiert } m \in \mathbf{N}, \text{ so daß } f^m \in \mathfrak{i}\}$$

das **Radikal** *von* $\mathfrak{i}$.

Direkt aus der Definition kann man $\mathfrak{i} \subseteq \sqrt{\mathfrak{i}}$ ablesen, da $f = f^1 \in \mathfrak{i}$ wiederum $f \in \sqrt{\mathfrak{i}}$ impliziert.

Lemma 3.3.6 *Es sei* $\mathfrak{i}$ *ein Ideal aus* $\mathbf{K}[x_1,\dots,x_n]$. *Dann ist* $\sqrt{\mathfrak{i}}$ *ein radikales Ideal.*

Beweis :
Da $\mathfrak{i} \subseteq \sqrt{\mathfrak{i}}$, gilt sicherlich $0 \in \sqrt{\mathfrak{i}}$. Um additive Abgeschlossenheit zu zeigen, nehmen wir an $f, g \in \sqrt{\mathfrak{i}}$ und für $k, l \in \mathbf{N}$ gelte $f^k, g^l \in \mathfrak{i}$. Rechnet man die Potenz $(f+g)^{k+l-1}$ aus, so stellt man fest, daß für jeden Summanden $f^i g^j$ gilt $i + j = k + l - 1$ und entweder $i \geq k$ oder $j \geq l$. Somit liegen alle $f^i g^j$ in $\mathfrak{i}$ und insbesondere gilt $(f+g)^{k+l-1} \in \mathfrak{i}$, d.h. $f + g \in \sqrt{\mathfrak{i}}$. Analog gilt für $h \in \mathbf{K}[x_1,\dots,x_n]$ wiederum $(f * h)^k = f^k * h^k \in \mathfrak{i}$ und somit $f * h \in \sqrt{\mathfrak{i}}$. Es bleibt zu zeigen, daß $\sqrt{\mathfrak{i}}$ radikal ist. Nehmen wir also an $f^m \in \sqrt{\mathfrak{i}}$ für ein $m \in \mathbf{N}$. Dann gilt es ein $k \in \mathbf{N}$ so, daß $(f^m)^k \in \mathfrak{i}$. Somit ist nach der Definition des Radikals aber auch f in $\sqrt{\mathfrak{i}}$ und wir sind fertig.

q.e.d.

Ein weiterer Zusammenhang zwischen Idealen und ihren Radikalen wird in Hilberts Nullstellensätzen formuliert.

Satz 3.3.7 (Hilberts Nullstellensatz) *Es sei* $\mathfrak{i}$ *ein Ideal aus* $\mathbf{K}[x_1,\dots,x_n]$. *Weiter sei* $\bar{\mathbf{K}}$ *der zu* $\mathbf{K}$ *gehörige algebraische Abschluß, d.h. derjenige Erweiterungskörper, in dem jedes Polynom* $f \in \mathbf{K}[x] \backslash \mathbf{K}$ *eine Nullstelle hat*[1]. *Dann gilt:*

1. $V_{\bar{\mathbf{K}}}(\mathfrak{i}) = \emptyset$ *genau dann, wenn* $\mathfrak{i} = \mathbf{K}[x_1,\dots,x_n]$.
2. $\sqrt{\mathfrak{i}} = I(V_{\bar{\mathbf{K}}}(\mathfrak{i}))$.

Definition 3.3.8 *Eine Menge von Polynomen* $F \subseteq \mathbf{K}[x_1,\dots,x_n]$ *heißt* **nulldimensional**, *falls das dazugehörige Nullstellengebilde* $V_{\bar{\mathbf{K}}}(F)$ *endlich ist.*

Nulldimensionale Ideale lassen sich nun wie folgt charakterisieren.

Satz 3.3.9 *Für ein Ideal* $\mathfrak{i} \subseteq \mathbf{K}[x_1,\dots,x_n]$ *sind folgende Aussagen äquivalent:*

1. *Das Nullstellengebilde* $V_{\bar{\mathbf{K}}}(\mathfrak{i})$ *ist endlich.*
2. *Für jedes* $1 \leq i \leq n$ *existiert ein Polynom* $f_i \in \mathfrak{i} \cap \mathbf{K}[x_i]$.

[1] Der Übergang zum algebraischen Abschluß ist notwendig, da es sonst auch nichttriviale Ideale mit nichtleerer Varietät gibt, z.B. $\langle x^2 + 1\rangle$ in $\mathbf{Q}[x]$

Beweis :
$1 \Longrightarrow 2$:
Wir nehmen an, $V_{\bar{\mathbf{K}}}(\mathfrak{i})$ sei endlich. Falls dieses Nullstellengebilde leer ist, gilt $\mathfrak{i} = \mathbf{K}[x_1, \ldots, x_n]$ (Hilberts Nullstellensatz), und die Behauptung folgt sofort, da ja dann $\mathfrak{i}$ die 1 enthält. Sei also $V_{\bar{\mathbf{K}}}(\mathfrak{i}) = \{a_1, \ldots, a_m\} \subseteq \mathbf{K}^n$ mit $a_j = (a_1^j, \ldots, a_n^j)$. Wir wählen ein $1 \leq i \leq n$ fest. Da $\mathbf{K}$ ein Körper ist, gibt es zu jedem $a_i^k \in \mathbf{K}$, $1 \leq k \leq m$, ein Polynom $f_i^k \in \mathbf{K}[x_i]$, welches a_i^k als Nullstelle hat. Man kann also insbesondere ein $f \in \mathbf{K}[x_i]$ wählen, welches alle a_i^k für $1 \leq k \leq m$ als Nullstelle hat, nämlich $f = \prod_{k=1}^m f_i^k$. Dann sind alle Nullstellen von $\mathfrak{i}$ auch Nullstellen von f. Nach Hilberts Nullstellensatz gilt dann $f^m \in \mathfrak{i}$ für eine geeignete Potenz von f, und da f^m auch aus $\mathbf{K}[x_i]$ ist, folgt die Behauptung.
$2 \Longrightarrow 1$:
Nun gelte umgekehrt, daß es zu jedem $1 \leq i \leq n$ ein Polynom $f_i \in \mathfrak{i} \cap \mathbf{K}[x_i]$ gibt. Da jede Nullstelle a aus $V_{\bar{\mathbf{K}}}(\mathfrak{i})$ eine Nullstelle von f_i sein muß und ein Polynom g aus $\mathbf{K}[x_i]$ maximal $\mathsf{grad}(g)$ Nullstellenhaben kann, kann es insgesamt nur endlich viele Nullstellen geben, nämlich maximal $\prod_{i=1}^n \mathsf{grad}(f_i)$.

q.e.d.

Die Aussage dieses Satzes läßt sich auch mittels Gröbnerbasen formulieren.

Korollar 3.3.10 *Es sei G eine Gröbnerbasis aus $\mathbf{K}[x_1, \ldots, x_n]$. Dann ist das von G erzeugte Ideal genau dann nulldimensional, wenn es für jede Variable x_i, $1 \leq i \leq n$, ein Polynom g_i in G gibt mit $\mathsf{HT}(g_i) = x_i^{d_i}$, $d_i \in \mathbf{N}$.*

Beweis :
Dies folgt sofort, wenn man sich an die Charakterisierung der Gröbnerbasen über die Kopfterme erinnert. Da laut Satz 3.3.9 zu jedem $1 \leq i \leq n$ ein Polynom $f_i \in \mathfrak{i} \cap \mathbf{K}[x_i]$ existiert, muß die Gröbnerbasis ein Polynom enthalten, dessen Kopfterm $\mathsf{HT}(f_i)$ teilt, also eine Potenz der Variablen x_i ist.

q.e.d.

Betrachten wir als Beispiel das von $F = \{x^2y - y + x, xy^2 - x\}$ erzeugte Ideal in $\mathbf{Q}[x, y]$. Dann ist $G = \{x^2y - y + x, y^2 - xy - x^2, x^3 + y - 2 \cdot x\}$ eine reduzierte normierte Gröbnerbasis dieses Ideals bezüglich der länge-lexikographischen Ordnung, die von $x < y$ induziert wird. Nach unseren bisherigen Sätzen können wir nun ableiten, daß F nulldimensional ist und maximal $2 \cdot 3 = 6$ Nullstellen hat. Tatsächlich hat das Nullstellengebilde 5 Nullstellen, nämlich $\{(0,0), (\alpha, -1), (-\alpha, 1), (\alpha', -1), (-\alpha', 1)\}$ wobei α und α' die Nullstellen der Gleichung $z^2 - z - 1$ sind. Berechnet man nun eine Gröbnerbasis bezüglich einer Eliminationsordnung, so erhält man zusätzliche Informationen über die Nullstellen. Eine Gröbnerbasis unseres Ideals bezüglich der lexikographischen Ordnung, die von $x < y$ impliziert wird, ist $G = \{x^5 - 3 \cdot x^3 + x, y + x^3 - 2 \cdot x\}$. Nun lassen sich die Nullstellen direkt bestimmen indem man zuerst die Gleichung $x^5 - 3 \cdot x^3 + x = 0$ löst und dann die gefundenen Lösungen in die Gleichung $y + x^3 - 2 \cdot x = 0$ einsetzt, um so weitere Lösungen zu finden.

Somit kann mit Hilfe von lexikographischen Ordnungen für nulldimensionale Ideale eine Gröbnerbasis in „Dreiecksgestalt" berechnet werden, die das Berechnen von Nullstellen auf das Ausrechnen von Nullstellen von Polynomen in *einer* Variablen reduziert. Nulldimensionale Ideale werden in zwei von uns betrachteten Anwendungen, dem Lösen algebraischer Gleichungssysteme und dem geometrischen Beweisen, eine Rolle spielen. Hierbei werden wir auch einen Enthaltenseintest für Radikale benötigen.

Satz 3.3.11 *Es sei F eine Polynommenge und f ein Polynom aus $\mathbf{K}[x_1,\ldots,x_n]$. Dann ist f genau dann in dem Radikal von $\langle F\rangle$, wenn 1 im Ideal $\langle F, f*z-1\rangle \subseteq \mathbf{K}[x_1,\ldots,x_n,z]$ liegt, wobei z eine neue Variable ist.*

Beweis :
Nach Hilberts Nullstellensatz gilt für das Radikal von $\langle F\rangle$ immer $I(V_{\bar{\mathbf{K}}}(\langle F\rangle)) = \sqrt{\langle F\rangle}$. Daher liegt ein Polynom f genau dann in $\sqrt{\langle F\rangle}$, wenn jede Nullstelle aus $V_{\bar{\mathbf{K}}}(\langle F\rangle)$ auch Nullstelle des Polynoms ist. Nehmen wir nun zuerst an, daß f in $\sqrt{\langle F\rangle}$ liegt. Wir wollen zeigen, daß dann das Nullstellengebilde von $\langle F, f*z-1\rangle$ leer ist, d.h. die Polynome aus F haben mit dem Polynom $f*z-1$ keine gemeinsame Nullstelle. Angenommen es gibt eine gemeinsame Nullstelle $(a_1,\ldots,a_n,b)\in\mathbf{K}^{n+1}$ von F und $f*z-1$. Dann ist $(a_1,\ldots,a_n)\in\mathbf{K}^n$ eine gemeinsame Nullstelle der Polynome in F und eine Nullstelle des Polynoms $f*b-1$. Da jedoch $(a_1,\ldots,a_n)$ auch eine Nullstelle von f sein muß, erhalten wir beim Auswerten des Polynoms $f*b-1$ einen Widerspruch. Also muß das Nullstellengebilde von $\langle F, f*z-1\rangle$ leer sein und somit $\langle F, f*z-1\rangle = \mathbf{K}[x_1,\ldots,x_n,z]$, und die 1 liegt in diesem Ideal. Nehmen wir umgekehrt an, daß $1\in\langle F, f*z-1\rangle$, so läßt sich die 1 wie folgt als Linearkombination von Elementen aus F und $f*z-1$ darstellen:

$$1 = \sum_{i=1}^{m} f_i * g_i + (f*z-1)*g$$

mit $g_1,\ldots,g_m,g\in\mathbf{K}[x_1,\ldots,x_n,z]$. Somit erhalten wir für jede gemeinsame Nullstelle $(a_1,\ldots,a_n)$ von F die Gleichung

$$1 = (f(a_1,\ldots,a_n)*z-1)*g(a_1,\ldots,a_n,z),$$

wobei die rechte Seite ein Polynom in $\mathbf{K}[z]$ ist, da sowohl $f(a_1,\ldots,a_n)*z-1$ als auch $g(a_1,\ldots,a_n,z)$ Polynome in z sind. Wäre nun $(a_1,\ldots,a_n)$ keine Nullstelle von f, so können wir für z den Wert $f(a_1,\ldots,a_n)^{-1}\in\mathbf{K}$ einsetzen, was zu einem Widerspruch

$$1 = (f(a_1,\ldots,a_n)\cdot f(a_1,\ldots,a_n)^{-1}-1)*g(a_1,\ldots,a_n,f(a_1,\ldots,a_n)^{-1}) = 0$$

führt. Somit muß f für $(a_1,\ldots,a_n)$ zu Null werden und daher im Radikal $\sqrt{\langle F\rangle}$ liegen.

q.e.d.

Somit kann auch das Enthaltenseinproblem für Radikale mit Gröbnerbasismethoden gelöst werden.

ENTHALTENSEINPROBLEM FÜR RADIKALE

Gegeben: Eine endliche Idealbasis F und ein Polynom f in $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gilt $f \in \sqrt{\langle F \rangle}$?

Vorgehen:
1. Bestimme eine Gröbnerbasis F' von $\langle F, f*z-1 \rangle$ in $\mathbf{K}[x_1, \ldots, x_n, z]$.
2. Es gilt $f \in \sqrt{\langle F \rangle}$ genau dann, wenn 1 sich mit F' zu Null reduzieren läßt.

Berechnet man in diesem Verfahren eine normierte reduzierte Gröbnerbasis, so testet man, ob die Gröbnerbasis gleich der Menge $\{1\}$ ist. Es läßt sich nun leicht überprüfen, ob das Polynom x im Radikal $\sqrt{\langle x^2 \rangle}$ liegt. Es ergibt sich nämlich beim Berechnen einer entsprechenden Gröbnerbasis für $\{x^2, xz-1\}$ nur ein S-Polynom, nämlich $x^2 * z - (xz - 1) * x = 1$, und wir sind fertig.

Eine weitere Folgerung dieses Testes ist, daß man entscheiden kann, ob zwei Ideale das gleiche Radikal erzeugen.

GLEICHHEITSPROBLEM FÜR RADIKALE

Gegeben: Zwei endliche Idealbasen F und G aus $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gilt $\sqrt{\langle F \rangle} = \sqrt{\langle G \rangle}$?

Vorgehen:
1. Berechne Gröbnerbasen F' und G' der Ideale $\langle F \rangle$ und $\langle G \rangle$ in $\mathbf{K}[x_1, \ldots, x_n]$.
2. Führe für jedes $f \in F'$ den Radikaltest für $\langle G \rangle$ durch, d.h. teste ob $\sqrt{\langle F \rangle} \subseteq \sqrt{\langle G \rangle}$.
3. Führe für jedes $g \in G'$ den Radikaltest für $\langle F \rangle$ durch, d.h. teste ob $\sqrt{\langle G \rangle} \subseteq \sqrt{\langle F \rangle}$.

Der für den Radikalenthaltenseinstest benutzte Trick des Einführens einer neuen Variable kann auch benutzt werden, um Erzeugende für den Schnitt zweier Ideale zu finden.

Satz 3.3.12 *Es seien* $\mathfrak{i}$ *und* $\mathfrak{j}$ *zwei Ideale in* $\mathbf{K}[x_1, \ldots, x_n]$ *und* z *eine neue Variable. Dann gilt*

$$\mathfrak{i} \cap \mathfrak{j} = \langle \mathfrak{i} * z, \mathfrak{j} * (z-1) \rangle \cap \mathbf{K}[x_1, \ldots, x_n],$$

wobei $\mathfrak{i} * z = \{f * z \mid f \in \mathfrak{i}\}$ *und* $\mathfrak{j} * (z-1) = \{f * (z-1) \mid f \in \mathfrak{j}\}$.

Beweis :
Jedes Polynom f aus $\mathfrak{i} \cap \mathfrak{j}$ läßt sich schreiben als Summe $f = f * z - f * (z-1)$ und liegt somit im Ideal $\langle \mathfrak{i} * z, \mathfrak{j} * (z-1) \rangle \cap \mathbf{K}[x_1, \ldots, x_n]$. Ist umgekehrt $f \in \langle \mathfrak{i} * z, \mathfrak{j} * (z-1) \rangle \cap \mathbf{K}[x_1, \ldots, x_n]$, so gilt $f = \sum_{i=1}^{k} f_i * z * p_i + \sum_{j=1}^{l} g_j * (z-1) * q_j$ mit Polynomen f_i aus $\mathfrak{i}$, g_j aus $\mathfrak{j}$ und p_i, q_j aus $\mathbf{K}[x_1, \ldots, x_n, z]$. Da f selbst die Variable z nicht enthält, erhalten wir durch Einsetzen von $z = 1$ $f \in \mathfrak{i}$ und durch Einsetzen von $z = 0$ $f \in \mathfrak{j}$, insbesondere also $f \in \mathfrak{i} \cap \mathfrak{j}$.

q.e.d.

Sind die Ideale durch erzeugende Mengen F und G gegeben, so kann sofort eine Gröbnerbasenlösung zur Beschreibung einer Basis des Schnittes angegeben werden.

SCHNITT VON IDEALEN

Gegeben: Zwei endliche Idealbasen F und G aus $\mathbf{K}[x_1, \ldots, x_n]$.

Aufgabe: Bestimme eine Basis für $\langle F \rangle \cap \langle G \rangle$.

Vorgehen:
1. Berechne eine Gröbnerbasis F' von $\langle \{f*z, g*(z-1) \mid f \in F, g \in G\} \rangle$ in $\mathbf{K}[x_1, \ldots, x_n, z]$ bezüglich einer Eliminationsordnung mit $z > x_i$ für $1 \leq i \leq n$.
2. $F' \cap \mathbf{K}[x_1, \ldots, x_n]$ ist eine Basis für $\langle F \rangle \cap \langle G \rangle$ (dies ist sogar eine Gröbnerbasis).

Diese Ideen lassen sich natürlich für den Schnitt von mehr als zwei Idealen verallgemeinern. Nachdem wir nun vorgestellt haben, wie man mit Hilfe von Gröbnerbasen ein Erzeugendensystem für den Schnitt von Idealen bestimmen kann, schließen wir diesen Abschnitt mit einer Technik zur Bestimmung des Quotienten zweier Ideale.

Definition 3.3.13 *Für zwei Ideale* $\mathfrak{i}$ *und* $\mathfrak{j}$ *in* $\mathbf{K}[x_1, \ldots, x_n]$ *definieren wir den Quotienten als die Menge*

$$\mathfrak{i}/\mathfrak{j} = \{g \mid g \in \mathbf{K}[x_1, \ldots, x_n], g * \mathfrak{j} \subseteq \mathfrak{i}\}$$

wobei $g * \mathfrak{j} = \{g * f \mid f \in \mathfrak{j}\}$.

Dann läßt sich dieser wie folgt beschreiben:

Lemma 3.3.14 *Es seien* $\mathfrak{i}$ *und* $\mathfrak{j} = \langle f_1, \ldots, f_k \rangle$ *zwei Ideale in* $\mathbf{K}[x_1, \ldots, x_n]$. *Dann gilt*

$$\mathfrak{i}/\mathfrak{j} = \bigcap_{i=1}^{k} (\mathfrak{i}/\langle f_i \rangle).$$

Beweis :
Aus $f \in \mathfrak{i}/\mathfrak{j}$ folgt nach Definition sofort $f * \mathfrak{j} \subseteq \mathfrak{i}$ und somit $f * f_i \in \mathfrak{i}$ für jedes $1 \leq i \leq k$, d.h. $f \in \mathfrak{i}/\langle f_i \rangle$ für jedes $1 \leq i \leq k$, also insbesondere $f \in \bigcap_{i=1}^{k} (\mathfrak{i}/\langle f_i \rangle)$. Umgekehrt impliziert $f \in \bigcap_{i=1}^{k} (\mathfrak{i}/\langle f_i \rangle)$, daß $f * f_i \in f\langle f_i \rangle \subseteq \mathfrak{i}$ für jedes $1 \leq i \leq k$ und daher $f * \mathfrak{j} \subseteq \mathfrak{i}$, also insbesondere $f \in \mathfrak{i}/\mathfrak{j}$.

q.e.d.

Dieses Lemma erlaubt es nunmehr den Quotienten zweier Ideale über endlich viele Quotienten der Form $\mathfrak{i}/\langle f \rangle$ zu beschreiben. Dies läßt sich wiederum durch Gröbnerbasen tun, da diese speziellen Quotienten sich auf unser Idealschnittproblem reduzieren lassen.

Lemma 3.3.15 *Es sei* $\mathfrak{i}$ *ein Ideal und* f *ein Polynom ungleich dem Nullpolynom aus* $\mathbf{K}[x_1, \ldots, x_n]$. *Dann gilt*

$$\mathfrak{i}/\langle f \rangle = f^{-1} * (\mathfrak{i} \cap \langle f \rangle)$$

wobei $f^{-1} = \frac{1}{f}$.

Beweis :
Die Elemente aus der Menge $f^{-1} * (\mathfrak{i} \cap \langle f \rangle)$ sind wohldefiniert, da jedes g aus $\mathfrak{i} \cap \langle f \rangle$ als $f * q$ mit $q \in \mathbf{K}[x_1, \ldots, x_n]$ dargestellt werden kann.

Nimmt man zuerst an, daß $g \in \mathfrak{i}/\langle f \rangle$, so gilt $g * f \in \mathfrak{i}$, insbesondere $g * f \in \mathfrak{i} \cap \langle f \rangle$ und somit $g \in f^{-1} * (\mathfrak{i} \cap \langle f \rangle)$. Umgekehrt impliziert $g \in f^{-1} * (\mathfrak{i} \cap \langle f \rangle)$, daß $g * f \in \mathfrak{i} \cap \langle f \rangle \subseteq \mathfrak{i}$ und daher auch $g \in \mathfrak{i}/\langle f \rangle$.

q.e.d.

Im nächsten Abschnitt werden wir einfache Anwendungen der hier gezeigten Sätze sehen, die aus dem in der Einleitung beschriebenen Wechselspiel zwischen Idealbasen und Nullstellengebilden motiviert sind.

Übungen

1. Testen Sie, ob das von $\{x^2 + y^2 - 1, xy - 1, y^2 - x\}$ erzeugte Ideal nulldimensional ist.

2. Es sei $\mathfrak{i}$ ein nulldimensionales Ideal in $\mathbf{K}[x_1, \ldots, x_n]$ und seien $g_i \in \mathfrak{i} \cap \mathbf{K}[x_i]$ für $1 \leq i \leq n$ Polynome wie in Satz 3.3.9 beschrieben. Zeigen Sie: Das Nullstellengebilde von $\mathfrak{i}$ hat maximal $\prod_{i=1}^{n} \mathsf{grad}(g_i)$ Elemente.

3. Mit Gröbnerbasentechniken kann man in der Regel nicht die in Satz 3.3.9 beschriebenen Polynome direkt berechnen, jedoch kann man Gröbnerbasen benutzen, um solche Polynome zu finden. Im Folgenden sei $\mathfrak{i}$ ein nulldimensionales Ideal in $\mathbf{K}[x_1, \ldots, x_n]$ mit einer beliebigen Gröbnerbasis G. Dann kann man Polynome aus $\mathfrak{i} \cap \mathbf{K}[x_i]$ für $1 \leq i \leq n$ wie folgt bestimmen:

   (a) Es sei $m \in \mathbf{N}$ minimal gewählt, so daß die Menge $\{1+\mathfrak{i}, x_i+\mathfrak{i}, \ldots, x_i^m+\mathfrak{i}\}$ linear abhängig in $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{i}$ ist. m kann man durch folgenden Test bestimmen: Es seien $y_0, \ldots, y_m$ $m+1$ neue Variablen. Weiter rechne man die Summe $\sum_{j=0}^{m} y_j * \textsc{Normalform}(x_i^j, G)$ als Polynom in $\mathbf{K}[y_1, \ldots, y_m][x_1, \ldots, x_n]$ aus. Mit $\mathfrak{j}$ bezeichnen wir das von den Koeffizienten dieses Polynoms in $\mathbf{K}[y_1, \ldots, y_m]$ erzeugte Ideal. Es gilt nun, die Menge $\{1+\mathfrak{i}, x_i+\mathfrak{i}, \ldots, x_i^m+\mathfrak{i}\}$ ist genau dann linear abhängig, wenn $V_{\bar{\mathbf{K}}}(\mathfrak{j}) \neq \{0\}$ und letzteres läßt sich mittels Gröbnerbasen entscheiden.

   (b) Für ein Tupel $(a_0, \ldots, a_m) \in V_{\bar{\mathbf{K}}}((j))$ gilt $f = \sum_{j=0}^{m} a_j \cdot x_i^j \in \mathfrak{i}$ und somit $f \in \mathfrak{i} \cap \mathbf{K}[x_i]$.

   Die hier vorgestellte Methode kann auch benutzt werden, um eine Gröbnerbasis bezüglich einer Termordnung $<_1$ mittels linearer Algebra in eine Gröbnerbasis bezüglich einer Termordnung $<_2$ umzuwandeln.

      i. Für Terme $t_1, \ldots, t_r$ entscheide man, ob die Menge $\{t_1 + \mathfrak{i}, \ldots, t_r + \mathfrak{i}\}$ linear abhängig ist.

      ii. Für die Terme $t_1, \ldots, t_r$ gelte $1 <_2 t_1 <_2 \ldots <_2 t_r$. Entscheiden Sie, ob es in $\mathfrak{i}$ ein Polynom gibt mit Kopfterm t_r bezüglich $<_2$.

iii. Benutzen Sie diese Ideen, um einen Algorithmus anzugeben, der zu einer gegebenen Gröbnerbasis bezüglich $<_1$ eine Gröbnerbasis bezüglich $<_2$ bestimmt.

iv. Kann Ihr Algorithmus auch für nicht nulldimensionale Ideale funktionieren?

4. Zeigen Sie, daß für zwei Polynome f und g aus $\mathbf{K}[x_1, \ldots, x_n]$ gilt $\langle f \rangle \cap \langle g \rangle = \langle \mathsf{kgV}(f, g) \rangle$.

5. Berechnen Sie den Idealquotienten von $\langle x^3 + 2x^2y + xy^2, y \rangle$ und $\langle x^2, x + y \rangle$ in $\mathbf{Q}[x, y]$.

3.4 Nichtlineare Gleichungssysteme und geometrisches Beweisen

In diesem Abschnitt wollen wir kennenlernen, wie Gröbnerbasen eingesetzt werden können, um algebraische Gleichungssyteme zu lösen. Eine endliche nicht leere Menge $F = \{f_1, \ldots, f_k\}$ von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$ beschreibt durch

$$\begin{array}{rcl} f_1(x_1, \ldots, x_n) & = & 0 \\ & \vdots & \\ f_k(x_1, \ldots, x_n) & = & 0 \end{array}$$

ein algebraisches Gleichungssystem. Aus den Ergebnissen des vorherigen Abschnittes wissen wir, wann das dazugehörige Nullstellengebilde $V_{\bar{\mathbf{K}}}(F)$ leer, endlich oder unendlich ist und wie wir dies testen können. Zur Erinnerung gilt für eine normierte reduzierte Gröbnerbasis G bezüglich der lexikographischen Ordnung mit $x_1 > \ldots > x_n$:

1. $V_{\bar{\mathbf{K}}}(F)$ ist leer genau dann, wenn $G = \{1\}$.

2. $V_{\bar{\mathbf{K}}}(F)$ ist endlich und nicht leer genau dann, wenn G zu jeder Variablen x_i, $1 \le i \le n$ ein Polynom g_i mit $\mathsf{HT}(g_i) = x_i^{d_i}$, $d_i \in \mathbf{N}$ enthält.

3. Sonst ist $V_{\bar{\mathbf{K}}}(F)$ unendlich.

Beispiel 3.4.1 *Wir betrachten den Polynomring $\mathbf{Q}[x, y, z]$ mit lexikographischer Ordnung induziert von $x > y > z$.*

Für $F_1 = \{xy^2 - y^2 + x - 1, x^3 + x^2, y_2 - y\}$ erhalten wir die normierte reduzierte Gröbnerbasis $\{1\}$. Somit haben die Polynome keine gemeinsame Nullstelle.

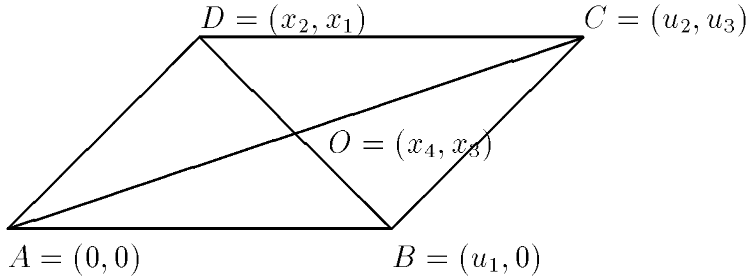
Für $F_2 = \{x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\}$ erhalten wir die normierte reduzierte Gröbnerbasis $\{x + y + z^2 - 1, y^2 - y - z^2 + z, 2 \cdot yz^2 + z^4 - z^2, z^6 - 4 \cdot z^4 + 4 \cdot z^3 - z^2\}$. Somit hat das Nullstellengebilde nur endlich viele Lösungen.

Für $F_3 = \{xy^2 - y^2 + x^2 - 1, xy - y, x^3 - x^2 - x + 1\}$ erhalten wir die normierte reduzierte Gröbnerbasis $\{x^2 - 1, xy - y\}$. Somit hat das Nullstellengebilde unendlich viele Lösungen.

Dieser algorithmische Zugang zu Untersuchungen des Nullstellengebildes eines Ideals findet zum Beispiel im automatischen Beweisen in der ebenen euklidische Geometrie eine schöne Anwendung. Hierbei wird ausgenutzt, daß sich die ebene euklidische Geometrie[2] axiomatisieren und in Prädikatenlogik erster Stufe ausdrücken läßt. Dies kann man bei Hilbert und Tarski nachlesen. 1977 stellte nun der chinesische Mathematiker Wu Wen-tsün eine algebraische Methode vor, mit der er geometrische Sätze automatisch „beweisen" konnte. Seine Idee bestand darin, Formeln der Gestalt $\forall x_1 \ldots \forall x_n h_1 = 0 \wedge \ldots \wedge h_k = 0 \longrightarrow g = 0$ mit Polynomen $h_1, \ldots, h_k, g$ aus $\mathbf{Q}[x_1, \ldots, x_n]$ durch Untersuchungen der durch die Polynomgleichungen beschriebenen Nullstellen zu bestätigen oder geeignete Zusatzbedingungen für die Gültigkeit der Formel zu finden. Diese Idee wurde in den 80er Jahren von Autoren wie Chou, Kapur, Kutzler und Stifter weiterentwickelt. Wir wollen hier die Methode von Chou genauer vorstellen.

Erster Schritt im Rahmen einer automatischen Behandlung der ebenen euklidischen Geometrie ist eine Übersetzung der geometrischen Sätze in Algebra. Die Grundlagen hierfür legte bereits im 17ten Jahrhundert der französische Mathematiker René Descartes durch seine analytische Betrachtung der ebenen euklidischen Geometrie. Er führte zur Beschreibung der Punkte in der Ebene ein rechtwinkliges Koordinatensystem ein und beschrieb geometrische Figuren wie Gerade, Kreis, Ellipse oder Parabel durch analytische Gleichungen der Form $f(x, y) = 0$.

Mit dieser Idee kann nun ein Zusammenhang zwischen Geometrien und algebraischen Strukturen hergestellt werden. Dies soll hier nur kurz skizziert werden. Es sei im folgenden $\mathbf{K}$ ein pythagoreischer Körper, d.h. zu allen a, b aus $\mathbf{K}$ gibt es ein c aus $\mathbf{K}$ mit $a^2 + b^2 = c^2$. Zum Beispiel ist der Körper der reellen Zahlen pythagoreisch. Diese Eigenschaft zusammen mit der Forderung, daß der Körper Charakteristik Null haben muß, wird benötigt, damit das durch die algebraische Interpretation erzeugte Modell die Axiome der ebenen euklidischen Geometrie erfüllt. Wir wollen hierauf jedoch in dieser Vorlesung nicht näher eingehen. Die wesentliche Idee ist, einen geometrischen Satz durch eine Menge von Polynomen $h_1, \ldots, h_k$ (genannt Hypothesen) und ein Polynom g (genannt Konklusion oder Behauptung) aus $\mathbf{K}[x_1, \ldots, x_n]$ zu beschreiben. Dies soll an einem Beispiel erläutert werden.



Wir wollen formulieren, daß die Diagonalen in einem Parallelogramm sich halbieren. Dazu gehen wir in obigem Bild von einer Koordinatisierung der Parallelogrammeckpunkte durch $A = (0, 0)$, $B = (u_1, 0)$, $C = (u_2, u_3)$, $D = (x_2, x_1)$ und des Schnittpunktes der Diagonalen durch $O = (x_4, x_3)$ aus. Dann können wir die geometrische

[2]Hier müssen eigentlich verschiedene Axiomatisierungen z.B. nach Euklid, Hilbert oder Tarski unterschieden werden.

Situation wie folgt beschreiben:

$h_1 = u_1x_1 - u_1u_3 = 0$ besagt, daß die Geraden duch A, B und D, C parallel sind.

$h_2 = u_3x_2 - (u_2 - u_1)x_1 = 0$ besagt, daß die Geraden duch A, D und C, B parallel sind.

$h_3 = x_1x_4 - (x_2 - u_1)x_3 - u_1x_1 = 0$ besagt, daß O auf der Geraden durch B, D liegt.

$h_4 = u_3x_4 - u_2x_3 = 0$ besagt, daß O auf der Geraden durch A, C liegt.

Die Wahl der verschieden Variablen u_i und x_i soll uns hier nicht weiter kümmern. Sie entsteht, wenn man nach der von Chou vorgeschlagenen Methode geometrische Sachverhalte übersetzt und spiegelt wieder, welche Koordinaten „frei" gewählt werden und welche nach dieser Wahl von den frei gewählten Punkten abhängig sind. Die Behauptung, daß sich die Diagonalen halbieren, läßt sich dann durch das Polynom $g = 2 \cdot u_2x_4 + 2 \cdot u_3x_3 - u_3^2 - u_2^2 = 0$ formulieren.

Im Wesentlichen beschäftigt uns nun folgendes Problem:

Gegeben: Eine geometrische Situation, welche durch die Polynomgleichungen $h_1, \ldots, h_k$ beschrieben ist, und eine Behauptung über diese Situation, formuliert durch eine weitere Polynomgleichung g aus $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gilt die Behauptung g, also gilt die Formel

$$\forall x_1 \ldots \forall x_n \, h_1 = 0 \wedge \ldots \wedge h_k = 0 \longrightarrow g = 0?$$

Betrachtet man die Nullstellengebilde $V_{\mathbf{K}}(h_1, \ldots, h_k)$ und $V_{\mathbf{K}}(g)$ über dem zu der Geometrie assoziierten Körper $\mathbf{K}$, also im Fall der ebenen euklidischen Geometrie z.B. die reellen Zahlen, so kann dieses Problem auch algebraisch formuliert werden. $V_{\mathbf{K}}(h_1, \ldots, h_k)$ beschreibt nämlich die Instanzen, welche die gewünschte geometrische Situation erfüllen. Somit muß nur überprüft werden, ob auch die Behauptung g für diese Instanzen gilt. Wir können also unser Problem wie folgt umformulieren:

Gegeben: Eine Menge von Polynomen $h_1, \ldots, h_k, g$ aus $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gilt $V_{\mathbf{K}}(h_1, \ldots, h_k) \subseteq V_{\mathbf{K}}(g)$?

Diese Frage werden wir nun unter Ausnutzung von Hilberts Nullstellensatz und einem Lemma, welches auch Rosinowitschs Trick genannt wird, mit Hilfe von Gröbnerbasen beantworten.

Lemma 3.4.2 (Rosinowitsch) *Für ein Polynom g aus $\mathbf{K}[x_1, \ldots, x_n]$ sind äquivalent:*

1. *Die Ungleichung $g \neq 0$ ist erfüllbar.*

2. *Die Gleichung $g * z - 1 = 0$ ist erfüllbar für eine neue Variable z.*

Beweis :

Nehmen wir zuerst an die Ungleichung $g \neq 0$ sei erfüllbar. Dann gibt es eine Instanz

$(a_1, \ldots, a_n)$ aus $\mathbf{K}^n$, so daß $g(a_1, \ldots, a_n) = c \neq 0$. Mit einer zusätzlichen Belegung $z = c^{-1}$ gilt dann $g(a_1, \ldots, a_n) \cdot c^{-1} - 1 = 0$. Ist umgekehrt $g * z - 1 = 0$ erfüllbar, so ist für eine Lösung dieser Gleichung sicherlich g nicht gleich Null.

q.e.d.

Diese Idee einer zusätzlichen Variablen haben wir auch im vorherigen Abschnitt im Zusammenhang mit der Charakterisierung des Schnittes von Idealen kennengelernt. Damals half diese Technik uns, ein Erzeugendensystem des Schnittes mittels Gröbnerbasen zu bestimmen. Hier benützen wir nun eine ähnliche Technik, um mit Hilfe von Gröbnerbasen die Gültigkeit unserer Formel $\forall x_1 \ldots \forall x_n \, h_1 = 0 \wedge \ldots \wedge h_k = 0 \longrightarrow g = 0$ zu entscheiden.

Satz 3.4.3 *Für Polynome $h_1, \ldots, h_k, g$ aus $\mathbf{K}[x_1, \ldots, x_n]$ sind folgende Aussagen äquivalent:*

1. *Die Formel $\forall x_1 \ldots \forall x_n \, h_1 = 0 \wedge \ldots \wedge h_k = 0 \longrightarrow g = 0$ ist wahr.*
2. $1 \in \langle h_1, \ldots, h_k, g * z - 1 \rangle_{\mathbf{K}[x_1, \ldots, x_n, z]}$.

Beweis :
Die Gültigkeit der Formel $\forall x_1 \ldots \forall x_n \, h_1 = 0 \wedge \ldots \wedge h_k = 0 \longrightarrow g = 0$ impliziert für die Nullstellengebilde sofort $V_{\bar{\mathbf{K}}}(h_1, \ldots, h_k) \subseteq V_{\bar{\mathbf{K}}}(g)$, wobei $\bar{\mathbf{K}}$ eine algebraische Erweiterung von $\mathbf{K}$ ist. Für die Polynomgleichung $g * z - 1 = 0$ gilt weiterhin $V_{\bar{\mathbf{K}}}(g) \cap V_{\bar{\mathbf{K}}}(g * z - 1) = \emptyset$ und somit auch $V_{\bar{\mathbf{K}}}(h_1, \ldots, h_k) \cap V_{\bar{\mathbf{K}}}(g * z - 1) = \emptyset$. Nach Hilberts Nullstellensatz impliziert dies $\langle h_1, \ldots, h_k, g * z - 1 \rangle_{\mathbf{K}[x_1, \ldots, x_n, z]} = \mathbf{K}[x_1, \ldots, x_n, z]$ und somit die Behauptung. Umgekehrt folgt aus $1 \in \langle h_1, \ldots, h_k, g * z - 1 \rangle_{\mathbf{K}[x_1, \ldots, x_n, z]} = \mathbf{K}[x_1, \ldots, x_n, z]$, daß die Polynome $h_1, \ldots, h_k, g * z - 1$ keine gemeinsame Nullstelle in $\bar{\mathbf{K}}$ haben. Somit muß jede gemeinsame Nullstelle von $h_1, \ldots, h_k$ auch eine Nullstelle von g sein, sonst gibt es einen Widerspruch. Daher muß die Formel $\forall x_1 \ldots \forall x_n \, h_1 = 0 \wedge \ldots \wedge h_k = 0 \longrightarrow g = 0$ insbesondere für $\mathbf{K}$ gelten.

q.e.d.

Somit kann der Test auf Gültigkeit in diesem Fall durch das Berechnen einer Gröbnerbasis durchgeführt werden. Beschäftigt man sich etwas näher mit dem hier vorgestellten Ansatz, so stellt man fest, daß für viele herkömmliche Sätze diese Methode im naiven Ansatz fehlschlägt, d.h. in der Regel liegt für die gewählte Übersetzung des Problems in Algebra die 1 nicht in dem entspechenden Ideal. Dies liegt daran, daß je nach der gewählten Übersetzung verschiedenes geometrisches Wissen einfließt oder man einfach zusätzliche Bedingungen vergißt. Daher enthält der Ansatz von Wen-tsün eine Idee, wie man in einem solchen Fall die „vergessenen” Bedingungen finden kann. Wir wollen hier nur kurz die Gröbnerbasenvariante von Chou für diese Problematik vorstellen und an unserem Parallelogrammbeispiel erläutern. Sie basiert auf einer Erweiterung der ursprünglichen Frage zu folgendem Problem:

Gegeben: Eine Menge von Polynomen $h_1, \ldots, h_k, g$ aus $\mathbf{K}[x_1, \ldots, x_n]$.

Frage: Gibt es ein weiteres Polynom s aus $\mathbf{K}[x_1, \ldots, x_n]$ so daß $V_{\mathbf{K}}(h_1, \ldots, h_k) \backslash V_{\mathbf{K}}(s) \subseteq V_{\mathbf{K}}(g)$?

Natürlich ist dieses Problem algebraisch immer lösbar indem man z.B. $s = h_1$ wählt und $V_{\mathbf{K}}(h_1, \ldots, h_k) \backslash V_{\mathbf{K}}(s) = \emptyset \subseteq V_{\mathbf{K}}(g)$ erhält. Wen-tsün und Chou geben nun geeignete Einschränkungen an s an, die garantieren, daß s eine „sinnvolle" geometrische Bedingung ist. Hier kommt die Unterscheidung der zur Koordination gewählten Variablen in unabhängige u_i und abhängige x_i zum Tragen. Als sinnvolle Einschränkungen werden nur Polynome in den freien Variablen angesehen, und ob solche existieren und wie sie aussehen, kann man durch Gröbnerbasen bezüglich Eliminationsordnungen erfahren. Wir gehen davon aus, daß die geometrische Situation durch Polynome $h_1, \ldots, h_k, g \in \mathbf{K}[X, U]$ beschrieben wird, wobei $X = \{x_1, \ldots, x_n\}$ die abhängigen und $U = \{u_1, \ldots, u_m\}$ die freien Variablen in der Koordinatisierung sind. Weiter sei G eine Gröbnerbasis des von den Polynomen $h_1, \ldots, h_k, g * z - 1$ in $\mathbf{K}[X, U, z]$ erzeugten Ideals bezüglich einer lexikographischen Ordnung mit $z > X > U$. Dann sind alle Polynome aus $G \cap \mathbf{K}[U]$ Kandidaten für zusätzliche geometrische Bedingungen.

Zum Abschluß wollen wir uns noch einmal mit unserem Parallelogrammbeispiel beschäftigen. Als beschreibende Polynome hatten wir die Hypothesen

$$\begin{aligned}
h_1 &= u_1x_1 - u_1u_3 = 0\\
h_2 &= u_3x_2 - (u_2 - u_1)x_1 = 0\\
h_3 &= x_1x_4 - (x_2 - u_1)x_3 - u_1x_1 = 0\\
h_4 &= u_3x_4 - u_2x_3 = 0
\end{aligned}$$

und die Behauptung

$$g = 2 \cdot u_2x_4 + 2 \cdot u_3x_3 - u_3^2 - u_2^2 = 0.$$

Berechnet man nun in $\mathbf{Q}[X, U, z]$ die Gröbnerbasis von $h_1, h_2, h_3, h_4, g * z - 1$ mit der rein-lexikographischen Ordnung mit Präzedenz $z \succ x_4 \succ \ldots \succ x_1 \succ u_3 \succ u_2 \succ u_1$ so erhält man die reduzierte normierte Gröbnerbasis

$$\begin{aligned}
&2 \cdot zx_3u_3 + 2 \cdot zx_4u_2 - zu_2^2 - zu_3^2 - 1,\\
&x_1x_4 - x_2x_3,\\
&x_1u_1,\\
&x_3u_2 - x_4u_3,\\
&x_1u_2 - x_2u_3,\\
&2 \cdot zx_4u_2^2 + 2 \cdot zx_4u_3^2 - zu_2^3 - zu_2u_3^2 - u_2,\\
&2 \cdot zx_4u_1u_2 - zu_1u_2^2 - u_1,\\
&u_1u_3,\\
&x_3u_1.
\end{aligned}$$

Diese Menge enthält nur ein Polynom aus $\mathbf{Q}[U]$, nämlich u_1u_3. Was bedeutet nun die Bedingung $u_1u_3 \neq 0$? Die Variablen u_1 und u_3 werden durch die Koordinatisierung der Punkte $B = (u_1, 0)$ und $C = (u_2, u_3)$ eingeführt. Gilt $u_1 = 0$, so fällt der Punkt B mit dem Punkt A zusammen, gilt hingegen $u_3 = 0$, so liegt C auf der Geraden durch A und B, d.h. durch eine zusätzliche Hypothese $u_1u_3z_1 - 1$, wobei z_1 eine neue Variable ist, werden gerade diese degenerierten Fälle eines Parallelogramms ausgeschlossen, und die Behauptung kann gezeigt werden. Denkt man an einen „natürlichen" Beweis dieses Satzes, so fällt auf, daß man unbewußt davon ausgehen würde, daß ein nicht-degeneriertes Parallelogramm vorliegt. Es wurde im Prinizip also nur vergessen, diese Information in die Hypothesen aufzunehmen.

3.5 Das 3-Farbenproblem für Graphen

In diesem Abschnitt wollen wir zeigen, wie ein wichtiges graphentheoretisches Problem sich mit Hilfe von Gröbnerbasen lösen läßt.

Gegeben sei ein ungerichteter Graph $\mathcal{G}$ mit n Knoten und maximal einer Kante zwischen je zwei Knoten. Die Frage ist nun, ob sich die Knoten des Graph mit 3 verschiedenen Farben so einfärben lassen, daß nie zwei Knoten, die mit einer Kante verbunden sind, die gleiche Farbe haben. Dieses Problem läßt sich natürlich auch für $k > 3$ Farben formulieren und ähnlich lösen.

Es stellt sich nun die Frage, wie man dieses graphentheoretische Problem in eine idealtheoretische Formulierung übersetzen kann. Hierzu repräsentieren wir unsere 3 Farben durch dritte Einheitswurzeln $1, \epsilon, \epsilon^2$ aus $\mathbf{C}$ mit $\epsilon = e^{\frac{2\pi i}{3}}$. Die Knoten des Graphen werden durch Variablen $x_1, \ldots, x_n$ dargestellt. Ziel ist es nun, die möglichen Einfärbungen des Graphen als Lösungen eines Gleichungssystems zu kodieren.

Jeder Knoten kann nun auf drei Arten „gefärbt" werden, was durch die Gleichungen

$$f_i = x_i^3 - 1 = 0, 1 \leq i \leq n$$

ausgedrückt wird. Weiterhin sollen Knoten, die durch eine Kante verbunden sind, verschieden eingefärbt werden. Für zwei beliebige Knoten x_i und x_j gilt immer $x_i^3 = x_j^3$ und diese Gleichung kann auch geschrieben werden als $(x_i - x_j) * (x_i^2 + x_i x_j + x_j^2) = 0$. Somit haben die Knoten x_i und x_j genau dann verschiedene Farben, wenn

$$g_{ij} = x_i^2 + x_i x_j + x_j^2 = 0.$$

Nun können wir unseren Graphen $\mathcal{G}$ durch Polynome in $\mathbf{C}[x_1, \ldots, x_n]$ wie folgt beschreiben:

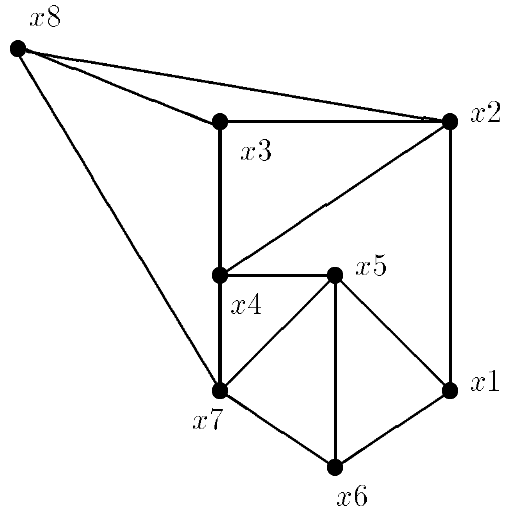
$$F_{\mathcal{G}} = \{f_1, \ldots, f_n\} \cup \{g_{ij} \mid 1 \leq i < j \leq n, \text{ es gibt Kante zwischen } x_i \text{ und } x_j \text{ in } \mathcal{G}\}.$$

Dann gilt für das von $F_{\mathcal{G}}$ in $\mathbf{C}[x_1, \ldots, x_n]$ erzeugte Ideal folgender wichtige Satz:

Satz 3.5.1 *Der Graph $\mathcal{G}$ kann mit 3 Farben gefärbt werden genau dann, wenn $V(\langle F_{\mathcal{G}} \rangle) \neq \emptyset$.*

Wie im vorherigen Abschnitt können nun Gröbnerbasen benutzt werden, um zu entscheiden, ob $V(\langle F_{\mathcal{G}} \rangle) \neq \emptyset$. Man berechnet einfach zu $F_{\mathcal{G}}$ eine Gröbnerbasis $G_{\mathcal{G}}$ und testet, ob diese Menge ein konstantes Element enthält.

Betrachten wir ein einfaches Beispiel.



Die Polynome, die diesen Graphen $\mathcal{G}$ beschreiben, sind

$$f_i = x_i^3 - 1, 1 \le i \le 8,$$

und

$$g_{ij} = x_i^2 + x_i x_j + x_j^2, (i,j) \in B,$$

wobei $B = \{(1,2),(1,5),(1,6),(2,3),(2,4),(2,8),(3,4),(3,8),(4,5),(4,7),(5,6),(5,7),(6,7),(7,8)\}$. Die reduzierte normierte Gröbnerbasis des von diesen Polynomen erzeugten Ideals bezüglich länge-lexikographischer Ordnung mit Präzedenz $x_1 > \ldots > x_8$ ist $G_{\mathcal{G}} = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8, x_6 - x_8, x_7^2 + x_7x_8 + x_8^2, x_8^3 - 1\}$. Da diese Menge kein konstantes Element enthält, gilt $V(\langle F_{\mathcal{G}}\rangle) \neq \emptyset$, und wir können sogar eine konkrete Färbung des Graphen berechnen. Hierzu beginnen wir mit dem Knoten x_8, da es nur ein Polynom $x_8^3 - 1$ in nur einer Variablen gibt. Wir nehmen an, unsere drei Farben sind rot, gelb und blau, und wir färben x_8 rot ein. Danach können wir x_7 färben, da das Polynom $x_7^2 + x_7x_8 + x_8^2$ in $G_{\mathcal{G}}$ ist, und x_7 muß eine neue Farbe bekommen, zum Beispiel blau. Dann müssen jedoch auch x_1 und x_3 blau sein, da die Polynome $x_1 - x_7$ und $x_3 - x_7$ in $G_{\mathcal{G}}$ sind. Ebenso müssen die Knoten x_4 und x_6 rot sein, da die Polynome $x_4 - x_8$ und $x_6 - x_8$ in $G_{\mathcal{G}}$ sind. Es verbleiben die Knoten x_2 und x_5, welche die gleiche Farbe haben müssen, aber verschieden von x_7 und x_8, da $x_2 + x_7 + x_8$ und $x_5 + x_7 + x_8$ in $G_{\mathcal{G}}$ sind. Wir erhalten also folgende Färbung:

Knoten	Farbe
x_1	blau
x_2	gelb
x_3	blau
x_4	rot
x_5	gelb
x_6	rot
x_7	blau
x_8	rot

Die Gröbnerbasis $G_{\mathcal{G}}$ gibt uns in diesem Beispiel nicht nur die Möglichkeit, eine Färbung auszurechnen, sondern wir sehen an der einfachen Struktur sogar, daß dieses Färbungsschema im Wesentlichen das einzig mögliche ist[3]. Zur Erinnerung: Die vorkommenden Kopfterme x_1, x_2, x_3, x_4, x_5, x_6, x_7^2 und x_8^3 bestimmen die Anzahl der möglichen Lösungen.

Für andere Graphen kann die dazugehörige Gröbnerbasis komplizierter aussehen, und somit ist das Berechnen einer konkreten Färbung nicht immer so einfach.

3.6 Polynomiale Abbildungen und lineare Optimierung

In diesem Abschnitt wollen wir eine weitere Anwendung von Gröbnerbasen kennenlernen, die sich mit sogenannten **K**-Algebra-Homomorphismen zwischen Polynomringen beschäftigt, d.h. mit Abbildungen

$$\phi : \mathbf{K}[y_1, \ldots, y_m] \longrightarrow \mathbf{K}[x_1, \ldots, x_n],$$

die durch ihr Verhalten auf den Variablen eindeutig bestimmt sind:

$$\phi : y_i \longmapsto f_i$$

mit f_i aus $\mathbf{K}[x_1, \ldots, x_n]$, $1 \leq i \leq m$. Für ein Polynom h aus $\mathbf{K}[y_1, \ldots, y_m]$ der Gestalt $h = \sum_{\nu=(\nu_1,\ldots,\nu_m)\in\mathbf{N}^m} c_\nu \cdot y_1^{\nu_1} \ldots y_m^{\nu_m}$ mit nur endlich vielen c_ν ungleich der Null ergibt sich dann

$$\phi(h) = \sum_{\nu=(\nu_1,\ldots,\nu_m)\in\mathbf{N}^m} c_\nu \cdot f_1^{\nu_1} \ldots f_m^{\nu_m} = h(f_1, \ldots, f_m),$$

und dieses Polynom liegt in $\mathbf{K}[x_1, \ldots, x_n]$. Der Kern dieser Abbildung ist ein Ideal, nämlich

$$\mathsf{ker}(\phi) = \{h \in \mathbf{K}[y_1, \ldots, y_m] \mid h(f_1, \ldots, f_m) = 0\}.$$

Das Bild dieser Abbildung ist eine K-Unteralgebra von $\mathbf{K}[x_1, \ldots, x_n]$

$$\mathsf{im}(\phi) = \{f \in \mathbf{K}[x_1, \ldots, x_n] \mid \phi(h) = f \text{ für ein } h \in \mathbf{K}[y_1, \ldots, y_m]\}.$$

Diese Unteralgebra wird oft auch mit $\mathbf{K}[f_1, \ldots, f_m]$ bezeichnet. Es gilt (erster Isomorphismensatz für K-Algebren)

$$\mathbf{K}[y_1, \ldots, y_m]/\mathsf{ker}(\phi) \cong \mathbf{K}[f_1, \ldots, f_m]$$

vermöge der Abbildung

$$g + \mathsf{ker}(\phi) \longmapsto \phi(g).$$

Im Folgenden benutzen wir unsere Sätze aus der Eliminationstheorie, um

[3]Es können natürlich die einzelnen Farben noch miteinander vertauscht werden.

1. den Kern von ϕ mit einer Gröbnerbasis zu beschreiben und

2. für das Bild von ϕ einen Entscheidungsalgorithmus zu bestimmen.

Dazu benötigen wir ein einfaches technisches Lemma.

Lemma 3.6.1 *Sind $a_1, \ldots, a_n, b_1, \ldots, b_n$ Elemente aus einem kommutativen Ring, so liegt $a_1 * \ldots * a_n - b_1 * \ldots * b_n$ im Ideal $\langle a_1 - b_1, \ldots, a_n - b_n \rangle$.*

Beweis :
Der Beweis erfolgt durch Induktion nach n und benutzt die Tatsache, daß

$$a_1 * \ldots * a_n - b_1 * \ldots b_n = a_1 * (a_2 * \ldots * a_n - b_2 * \ldots b_n) + b_2 * \ldots * b_n * (a_1 - b_1).$$

q.e.d.

Wenden wir uns nun unserer ersten Aufgabe zu. Den Kern der Abbildung ϕ können wir algebraisch wie folgt charakterisieren.

Satz 3.6.2 *Es seien $f_1, \ldots, f_m$ die wie oben zu ϕ assoziierten Polynome aus $\mathbf{K}[x_1, \ldots, x_n]$ und $\mathfrak{i} = \langle y_1 - f_1, \ldots, y_m - f_m \rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$. Dann gilt*

$$\mathsf{ker}(\phi) = \mathfrak{i} \cap \mathbf{K}[y_1, \ldots, y_m].$$

Beweis :
Ist g aus $\mathfrak{i} \cap \mathbf{K}[y_1, \ldots, y_m]$, so gilt $g = \sum_{i=1}^{m} (y_i - f_i) * h_i$, wobei die Polynome h_i aus $\mathbf{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ sind. Daher ist $g(f_1, \ldots, f_m)$ Null und somit g aus $\mathsf{ker}(\phi)$. Umgekehrt hat ein Polynom g aus $\mathsf{ker}(\phi)$ eine Darstellung $g = \sum_{\nu=(\nu_1,\ldots,\nu_m)\in\mathbf{N}^m} c_\nu \cdot y_1^{\nu_1} \ldots y_m^{\nu_m}$ mit nur endlich vielen c_ν ungleich der Null. Da $g(f_1, \ldots, f_m) = 0$, können wir auch schreiben

$$\begin{aligned} g &= g - g(f_1, \ldots, f_m) \\ &= \textstyle\sum_{\nu=(\nu_1,\ldots,\nu_m)\in\mathbf{N}^m} c_\nu \cdot y_1^{\nu_1} \ldots y_m^{\nu_m} - \sum_{\nu=(\nu_1,\ldots,\nu_m)\in\mathbf{N}^m} c_\nu \cdot f_1^{\nu_1} \ldots f_m^{\nu_m} \\ &= \textstyle\sum_{\nu=(\nu_1,\ldots,\nu_m)\in\mathbf{N}^m} c_\nu \cdot (y_1^{\nu_1} \ldots y_m^{\nu_m} - f_1^{\nu_1} \ldots f_m^{\nu_m}), \end{aligned}$$

und jedes $y_1^{\nu_1} \ldots y_m^{\nu_m} - f_1^{\nu_1} \ldots f_m^{\nu_m}$ liegt nach Lemma 3.6.1 in $\mathfrak{i}$. Somit liegt g auch in $\mathfrak{i} \cap \mathbf{K}[y_1, \ldots, y_m]$.

q.e.d.

Dieser Satz ist die Grundlage für die konkretere Bestimmung des Kerns von ϕ. Man berechnet eine Gröbnerbasis G von $\{y_1 - f_1, \ldots, y_m - f_m\}$ bezüglich einer Eliminationsordnung mit $X > Y$, und die Elemente aus $G \cap \mathbf{K}[y_1, \ldots, y_m]$ sind eine Gröbnerbasis des Ideals $\mathsf{ker}(\phi)$.

Machen wir uns dieses Vorgehen an einem kleinen Beispiel deutlich. Es sei die Abbildung $\phi : \mathbf{Q}[r,u,v,w] \longrightarrow \mathbf{Q}[x,y]$ bestimmt durch

$$\begin{array}{rcr} r & \longmapsto & x^4 \\ u & \longmapsto & x^3y \\ v & \longmapsto & xy^3 \\ w & \longmapsto & y^4. \end{array}$$

Dann bestimmen wir bezüglich der Eliminationsordnung, welche die länge-lexikographische Ordnung mit Präzedenz $y > x$ auf $\mathbf{Q}[x,y]$ mit der umgekehrt-länge-lexikographischen Ordnung $r > u > v > w$ auf $\mathbf{Q}[r,u,v,w]$ verbindet, die reduzierte normierte Gröbnerbasis von $\langle r - x^4, u - x^3y, v - xy^3, w - y^4\rangle$: $G = \{x^4 - r, x^3y - u, y^4 - w, yv - xw, yr - xu, y^2u - x^2v, x^2y^2w - v^2, uv - rw, v^3 - uw^2, rv^2 - u^2w, yuw - xv^2, u^3 - r^2v, yu^2 - xrv\}$. Dann ist $G \cap \mathbf{Q}[r,u,v,w] = \{uv - rw, v^3 - uw^2, rv^2 - u^2w, u^3 - r^2v\}$ eine Gröbnerbasis von $\mathsf{ker}(\phi)$.

Wenden wir uns nun dem Bild der Abbildung ϕ zu.

Satz 3.6.3 *Es sei $\mathfrak{i} = \langle y_1 - f_1, \ldots, y_m - f_m\rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ wie in Satz 3.6.2 und G eine normierte reduzierte Gröbnerbasis dieses Ideals bezüglich einer Eliminationsordnung mit $X > Y$. Dann liegt ein Polynom f aus $\mathbf{K}[x_1,\ldots,x_n]$ genau dann im Bild von ϕ, wenn es ein h aus $\mathbf{K}[y_1,\ldots,y_m]$ gibt mit $f \overset{*}{\longrightarrow}_G h$. Es gilt dann $f = \phi(h) = h(f_1,\ldots,f_m)$.*

Beweis :
Zuerst nehmen wir an, f sei aus dem Bild von ϕ, d.h. es gibt ein Polynom g aus $\mathbf{K}[y_1,\ldots,y_m]$ mit $f = g(f_1,\ldots,f_m)$. Dann liegt die Differenz $f - g$ in $\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]$, und es gilt $f - g = g(f_1,\ldots,f_m) - g$, und wie im vorherigen Satz kann man mit Hilfe von Lemma 3.6.1 zeigen, daß $f - g$ in $\mathfrak{i}$ liegt. Daher gilt $f - g \overset{*}{\longrightarrow}_G 0$, und nach Lemma 2.3.2 gibt es ein h mit $f \overset{*}{\longrightarrow}_G h$ und $g \overset{*}{\longrightarrow}_G h$. Letztere Reduktionskette erlaubt zur Reduktion von g aus $\mathbf{K}[y_1,\ldots,y_m]$, da G mit einer Eliminationsordnung berechnet wurde, nur die Anwendung von Polynomen aus $G \cap \mathbf{K}[y_1,\ldots,y_m]$. Insbesondere muß dann auch h aus $\mathbf{K}[y_1,\ldots,y_m]$ sein.
Umgekehrt impliziert $f \overset{*}{\longrightarrow}_G h$ nach Lemma 2.3.2 $f - h \in \mathfrak{i}$, d.h.

$$f - h = \sum_{i=1}^{m} g_i * (y_i - f_i)$$

mit Polynomen g_i aus $\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]$. Ersetzt man f_i für y_i, so erhält man wie gewünscht $f = h(f_1,\ldots,f_m) = \phi(h)$.

q.e.d.

Somit kann aus folgendem Korollar ein Algorithmus abgeleitet werden, um zu entscheiden, ob ein Polynom im Bild von ϕ liegt.

Korollar 3.6.4 *Es sei* $\mathfrak{i} = \langle y_1 - f_1, \ldots, y_m - f_m\rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ *wie in Satz 3.6.2 und* G *eine normierte reduzierte Gröbnerbasis dieses Ideals bezüglich einer Eliminationsordnung mit* $X > Y$. *Dann liegt ein Polynom* f *aus* $\mathbf{K}[x_1, \ldots, x_n]$ *genau dann im Bild von* ϕ, *wenn* NORMALFORM(f, G) *ein Polynom aus* $\mathbf{K}[y_1, \ldots, y_m]$ *liefert.*

Dieser Algorithmus soll wieder an einem Beispiel verdeutlicht werden. Wir betrachten die Abbildung $\phi : \mathbf{Q}[u, v] \longrightarrow \mathbf{Q}[x]$ definiert durch

$$\begin{array}{ll} u & \longmapsto x^4 + x \\ v & \longmapsto x^3. \end{array}$$

Liegt x^5 im Bild dieser Abbildung? Um dies zu beantworten, berechnen wir die reduzierte normierte Gröbnerbasis des Ideals $\langle u-x^4-x, v-x^3\rangle$ bezüglich der lexikographischen Ordnung mit Präzedenz $x > u > v$. Wir erhalten $G = \{u^3 - v^4 - 3\cdot v^3 - 3\cdot v^2 - v, xv + x - u, xu^2 - v^3 - 2\cdot v^2 - v, x^2u - v^2 - v, x^3 - v\}$. Reduktion von x^5 mit G ergibt

$$x^5 \longrightarrow_{x^3-v} x^2v \longrightarrow_{xv+x-u} -x^2 + xu.$$

Da dies eine Normalform ist und nicht in $\mathbf{Q}[u, v]$ liegt, impliziert Korollar 3.6.4, daß x^5 nicht im Bild von ϕ liegt.

Dieser Algorithmus kann auch benutzt werden, um zu testen, ob ϕ surjektiv ist, d.h. jedes Element aus $\mathbf{K}[x_1, \ldots, x_n]$ hat ein Urbild in $\mathbf{K}[y_1, \ldots, y_m]$. Man braucht nur zu testen, ob die Variablen $x_1, \ldots, x_n$ im Bild von ϕ liegen. Der nächste Satz besagt, daß man dies direkt an der Gröbnerbasis ablesen kann.

Satz 3.6.5 *Es sei* $\mathfrak{i} = \langle y_1 - f_1, \ldots, y_m - f_m\rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ *wie in Satz 3.6.2 und* G *eine normierte reduzierte Gröbnerbasis dieses Ideals bezüglich einer Eliminationsordnung mit* $X > Y$. *Dann ist* ϕ *surjektiv genau dann, wenn es zu jedem* $1 \le i \le n$ *ein Polynom* g_i *in* G *gibt der Gestalt* $g = x_i - h_i$ *mit* $h_i \in \mathbf{K}[y_1, \ldots, y_m]$. *Insbesondere gilt* $x_i = h_i(f_1, \ldots, f_m)$.

Beweis :
Nehmen wir zuerst an, ϕ sei surjektiv. Als Präzedenz auf den Variablen X setzen wir $x_1 < \ldots < x_n$ voraus. Dann existiert nach Satz 3.6.3, da x_1 im Bild von ϕ liegt, ein Polynom h_1' aus $\mathbf{K}[y_1, \ldots, y_m]$ mit $x_1 \xrightarrow{*}_G h_1'$, und es gilt $x_1 - h_1' \in \mathfrak{i}$. Daher muß insbesondere ein Polynom g_1 aus G existieren, dessen Kopfterm $\mathsf{HT}(x_1) = x_1$ teilt, also, da G nicht die 1 enthält, gilt $\mathsf{HT}(g_1) = x_1$. Weiter sind alle Terme, die kleiner als x_1 sind, Terme aus $\mathsf{T}^m(Y)$, d.h. $g_1 = x_1 - h_1$ mit h_1 aus $\mathbf{K}[y_1, \ldots, y_m]$. Ebenso folgt, da x_2 im Bild von ϕ liegt, die Existenz eines Polynoms h_2' mit $x_2 \xrightarrow{*}_G h_2'$. Es existiert somit ein Polynom g_2 in G mit Kopfterm $\mathsf{HT}(g_2) = x_2$, dessen weitere Terme alle kleiner als x_2 sind, also in $\mathsf{T}^{m+1}(\{x_1\} \cup Y)$ liegen. Da jedoch G reduziert ist und das Polynom $g_1 = x_1 - h_1$ enthält, folgt, daß die Variable x_1 in den Termen von g_2 nicht vorkommt. Daher gibt es ein Polynom h_2 aus $\mathbf{K}[y_1, \ldots, y_m]$ mit $g_2 = x_2 - h_2$. Ähnlich können wir nun für die Variablen $x_3, \ldots, x_n$ vorgehen.

Um umgekehrt zu zeigen, daß ϕ surjektiv ist, benutzen wir, daß dies genau dann der Fall ist, wenn jedes x_i im Bild von ϕ liegt, $1 \leq i \leq n$. Da $x_i - h_i$ in G liegt, gilt $x_i \longrightarrow_G h_i$ für alle $1 \leq i \leq n$. Da h_i aus $\mathbf{K}[y_1, \ldots, y_m]$ folgt mit Satz 3.6.3, daß x_i im Bild von ϕ liegt.

q.e.d.

Diese Resultate können nun auf Quotienten von Polynomringen übertragen werden.

Definition 3.6.6 *Eine $\mathbf{K}$-Algebra heißt affin, falls sie isomorph (als K-Algebra) zu einem Quotienten $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{k}$ mit Ideal $\mathfrak{k}$ ist.*

Der Polynomring $\mathbf{K}[x_1, \ldots, x_n]$ selbst ist affin. Ebenso ist für $f_1, \ldots, f_m$ wie oben $\mathbf{K}[f_1, \ldots, f_m]$ affin. Wir betrachten nun Homomorphismen zwischen solchen affinen K-Algebren

$$\phi : \mathbf{K}[y_1, \ldots, y_m]/\mathfrak{j} \longrightarrow \mathbf{K}[x_1, \ldots, x_n]/\mathfrak{k},$$

die wie folgt eindeutig bestimmt sind:

$$\phi : y_i + \mathfrak{j} \longmapsto f_i + \mathfrak{k}.$$

Eine solche Abbildung ist genau dann wohldefiniert, wenn für $\mathfrak{j} = \langle g_1, \ldots, g_t \rangle$ gilt, daß für alle $1 \leq i \leq t$, $g_i(f_1, \ldots, f_m) \in \mathfrak{k}$. Dies kann natürlich mittels Gröbnerbasen überprüft werden. Als Verallgemeinerungen der obigen Sätze erhalten wir

Satz 3.6.7 *Es sei $\mathfrak{i} = \langle \mathfrak{k}, y_1 - f_1, \ldots, y_m - f_m \rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$. Dann gilt $\mathsf{ker}(\phi) = \mathfrak{i} \cap \mathbf{K}[y_1, \ldots, y_m]$ (modulo $\mathfrak{j}$), d.h. falls $\mathfrak{i} \cap \mathbf{K}[y_1, \ldots, y_m] = \langle g_1, \ldots, g_s \rangle$, so ist $\mathsf{ker}(\phi) = \langle g_1 + \mathfrak{j}, \ldots, g_s + \mathfrak{j} \rangle$.*

Satz 3.6.8 *Es sei $\mathfrak{i} = \langle \mathfrak{k}, y_1 - f_1, \ldots, y_m - f_m \rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ und G eine Gröbnerbasis von $\mathfrak{i}$ bezüglich einer Eliminationsordnung mit $X > Y$. Dann liegt $f + \mathfrak{k}$ aus $\mathbf{K}[x_1, \ldots, x_n]/\mathfrak{k}$ genau dann im Bild von ϕ, wenn es ein h aus $\mathbf{K}[y_1, \ldots, y_m]$ gibt mit $f \overset{*}{\longrightarrow}_G h$. Insbesondere gilt $f + \mathfrak{k} = \phi(h + \mathfrak{j}) = h(f_1, \ldots, f_m) + \mathfrak{j}$.*

Wieder kann dies durch das Berechnen der Normalform bezüglich G entschieden werden.

Satz 3.6.9 *Es sei $\mathfrak{i} = \langle \mathfrak{k}, y_1 - f_1, \ldots, y_m - f_m \rangle_{\mathbf{K}[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ und G eine normierte reduzierte Gröbnerbasis von $\mathfrak{i}$ bezüglich einer Eliminationsordnung mit $X > Y$. Die Abbildung ϕ ist genau dann surjektiv, wenn es für jedes $1 \leq i \leq n$ ein Polynom $g_i = x_i - h_i$ in G gibt mit h_i aus $\mathbf{K}[y_1, \ldots, y_m]$.*

Bisher haben wir kennengelernt, wie Gröbnerbasen eingesetzt werden können, um das Enthaltenseinsproblem für Ideale in $\mathbf{K}[x_1, \ldots, x_n]$ zu entscheiden. Eine weitere interessante Unterstruktur von Polynomringen haben wir in diesem Abschnitt kennengelernt — Unteralgebren. Im Gegensatz zu Idealen sind Unteralgebren nur abgeschlossen bezüglich Multiplikation mit Elementen aus $\mathbf{K}$ und sich selbst. Eine Menge

$\mathcal{A} \subseteq \mathbf{K}[x_1, \ldots, x_n]$ heißt Unteralgebra genau dann, wenn $\mathbf{K} \subseteq \mathcal{A}$ und f, g aus $\mathcal{A}$ gilt: $f - g$ und $f * g$ sind auch aus $\mathcal{A}$. Das Enthaltenseinproblem für Unteralgebren läßt sich wie folgt formulieren.

Enthaltenseinproblem für Unteralgebren

Gegeben:	Eine Erzeugendenmenge F und ein Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$.
Frage:	Liegt f in $\mathbf{K}[F]$?

Wir können nun für endlich erzeugte Unteralgebren von $\mathbf{K}[x_1, \ldots, x_n]$ die hier vorgestellten Techniken benutzen, um dieses Problem zu entscheiden. Ist $\mathcal{A}$ erzeugt von den Polynomen $F = \{f_1, \ldots, f_k\}$, so schreiben wir wieder $\mathbf{K}[f_1, \ldots, f_k]$. Berechnet man die zu

$$\begin{array}{rcl} \phi : \mathbf{K}[y_1, \ldots, y_m] & \longrightarrow & \mathbf{K}[x_1, \ldots, x_n], \\ y_i & \longmapsto & f_i \end{array}$$

assoziierte Gröbnerbasis G von $\{y_i - f_i \mid 1 \leq i \leq k\}$ wie oben beschrieben, so gilt für f aus $\mathbf{K}[x_1, \ldots, x_n]$, daß f auch in $\mathbf{K}[f_1, \ldots, f_k]$ liegt, genau dann, wenn die Normalform h von f bezüglich G in $\mathbf{K}[y_1, \ldots, y_k]$ liegt. Es gilt dann sogar $\phi(f) = h(f_1, \ldots f_k)$, und das Polynom h gibt uns f als Algebralinearkombination der Elemente aus F. Dieses Entscheidungsverfahren kann auch für Ideale in $\mathbf{K}[f_1, \ldots, f_k]$ ausgedehnt werden.

Abschließend wollen wir nun sehen, wie Gröbnerbasen eingesetzt werden können, um lineare Optimierungsprobleme zu lösen.

Gegeben seien Elemente a_{ij}, b_i aus $\mathbf{Z}$ und c_j aus $\mathbf{R}$ mit $1 \leq i \leq n$ und $1 \leq j \leq m$. Gesucht wird eine Lösung in $\mathbf{N}^m$ des Gleichungssystems

$$\begin{array}{ccccccc} a_{11} \cdot z_1 & + & \ldots & + & a_{1m} \cdot z_m & = & b_1 \\ a_{21} \cdot z_1 & + & \ldots & + & a_{2m} \cdot z_m & = & b_2 \\ \\ a_{n1} \cdot z_1 & + & \ldots & + & a_{nm} \cdot z_m & = & b_n, \end{array}$$

welches folgende Kostenfunktion minimiert

$$c(z_1, \ldots, z_m) = \sum_{j=1}^{m} c_j \cdot z_j.$$

Es gibt verschiedene Ansätze, solch ein Problem zu lösen, z.B. die Simplexmethode. Wir wollen hier jedoch wieder versuchen, Gröbnerbasen einzusetzen. Hierbei wollen wir wie folgt vorgehen:

1. Übersetze das gegebene Optimierungsproblem in ein algebraisches Problem
2. Löse das algebraische Problem mit Gröbnerbasen.
3. Übersetze diese Lösung in den ursprünglichen Kontext.

Zuerst wollen wir uns mit dem Spezialfall beschäftigen, daß alle a_{ij} und b_i aus $\mathbf{N}$ sind und die Kostenfunktion vernachlässigt wird. Dann können wir unser Gleichungssystem in speziellen Polynomen kodieren. Wir führen für jede Gleichung eine Variable x_i ein und schreiben

$$x_i^{a_{i1}\cdot z_1+\ldots+a_{im}\cdot z_m} = x_i^{b_i}$$

für $1 \leq i \leq n$. Das ganze Gleichungssystem kann dann in einer Gleichung zusammengefaßt werden

$$x_1^{a_{11}\cdot z_1+\ldots+a_{1m}\cdot z_m} \ldots x_n^{a_{n1}\cdot z_1+\ldots+a_{nm}\cdot z_m} = x_1^{b_1} \ldots x_n^{b_n}$$

oder anders geschrieben

$$(x_1^{a_{11}} x_2^{a_{21}} \ldots x_n^{a_{n1}})^{z_1} \ldots (x_1^{a_{1m}} x_2^{a_{2m}} \ldots x_n^{a_{nm}})^{z_m} = x_1^{b_1} \ldots x_n^{b_n}.$$

Dann kann die linke Seite dieser Gleichung als Bild des Produktes $y_1^{z_1} \ldots y_m^{z_m}$ folgender Abbildung aufgefaßt werden:

$$\begin{array}{rlcl} \phi: & \mathbf{K}[y_1, \ldots, y_m] & \longrightarrow & \mathbf{K}[x_1, \ldots, x_n] \\ & y_i & \longmapsto & x_1^{a_{1i}} x_2^{a_{2i}} \ldots x_n^{a_{ni}} \end{array}$$

Lemma 3.6.10 *Im oben beschriebenen Spezialfall, daß alle a_{ij} und b_i aus $\mathbf{N}$ sind, gilt: Es gibt eine Lösung $(\sigma_1, \ldots, \sigma_m)$ aus $\mathbf{N}^m$ genau dann, wenn $x_1^{b_1} \ldots x_n^{b_n}$ Bild eines Termes aus $\mathsf{T}^m(Y)$ unter der Abbildung ϕ ist. Insbesondere folgt aus $x_1^{b_1} \ldots x_n^{b_n} = \phi(y_1^{\sigma_1} \ldots y_m^{\sigma_m})$, daß $(\sigma_1, \ldots, \sigma_m)$ eine Lösung des Gleichungssystems ist.*

In Satz 3.6.3 haben wir gesehen, unter welchen Bedingungen ein Element Bild eines Polynoms unter einer solchen Abbildung ϕ ist. In unserem Lemma wird gefordert, daß das Element sogar Bild eines Termes sein soll. Da ϕ die Variablen y_i jedoch auf Terme in $\mathsf{T}^n(X)$ abbildet, können wir Satz 3.6.3 verschärfen.

Lemma 3.6.11 *Wir setzen wieder voraus, daß alle a_{ij} und b_i aus $\mathbf{N}$ sind. Ist $x_1^{b_1} \ldots x_n^{b_n}$ im Bild von ϕ, so ist es Bild eines Termes aus $\mathsf{T}^m(Y)$.*

Beweis :
Wir benutzen Satz 3.6.3. Es sei $\mathfrak{i} = \langle \{y_i - x_1^{a_{1i}} x_2^{a_{2i}} \ldots x_n^{a_{ni}} \mid 1 \leq i \leq m\} \rangle$ und G eine normierte reduzierte Gröbnerbasis dieses Ideals bezüglich einer Eliminationsordnung mit $X > Y$. Dann ist $x_1^{b_1} \ldots x_n^{b_n}$ im Bild von ϕ genau dann, wenn $x_1^{b_1} \ldots x_n^{b_n} \xrightarrow{*}_G h$ für ein Polynom h aus $\mathbf{K}[y_1, \ldots, y_m]$. Insbesondere folgt aus $x_1^{b_1} \ldots x_n^{b_n} \xrightarrow{*}_G h$ dann auch $x_1^{b_1} \ldots x_n^{b_n} = \phi(h)$. Da G nur Polynome bestehend aus Differenzen zweier Terme enthält, folgt sofort, daß h ein Term aus $\mathsf{T}^m(Y)$ sein muß.

q.e.d.

Somit können wir Gröbnerbasen wieder einsetzen, um zu entscheiden, ob in unserem Spezialfall das Gleichungssystem eine ganzzahlige Lösung hat.

1. Berechne eine reduzierte Gröbnerbasis des Ideals $\langle \{y_i - x_1^{a_{1i}} x_2^{a_{2i}} \ldots x_n^{a_{ni}} \mid 1 \leq i \leq m\} \rangle$ bezüglich einer Eliminationsordnung mit $X > Y$.

2. Berechne die Normalform h von $x_1^{b_1} \ldots x_n^{b_n}$.

3. Ist h nicht aus $\mathsf{T}^m(Y)$, so existiert keine nicht-negative Lösung. Gilt jedoch $h = y_1^{\sigma_1} \dots y_m^{\sigma_m}$, so ist $(\sigma_1, \dots, \sigma_m)$ eine Lösung des Gleichungssystems.

Dies soll nun an einem Beispiel illustriert werden. Wir betrachten das Gleichungssystem

$$\begin{array}{ccccccccc} 3 \cdot z_1 & + & 2 \cdot z_2 & + & z_3 & + & z_4 & = & 10 \\ 4 \cdot z_1 & + & z_2 & + & z_3 & & & = & 5. \end{array}$$

Dann erhalten wir für jede Gleichung eine Variable, also x_1 und x_2. Die entsprechende Abbildung ist

$$\begin{array}{cccc} \phi: & \mathbf{Q}[y_1, y_2, y_3, y_4] & \longrightarrow & \mathbf{Q}[x_1, x_2] \\ & y_1 & \longmapsto & x_1^3 x_2^4 \\ & y_2 & \longmapsto & x_1^2 x_2 \\ & y_3 & \longmapsto & x_1 x_2 \\ & y_4 & \longmapsto & x_1, \end{array}$$

und das dazugehörige Ideal ist $\mathfrak{i} = \langle y_1 - x_1^3 x_2^4, y_2 - x_1^2 x_2, y_3 - x_1 x_2, y_4 - x_1 \rangle$. Die reduzierte normierte Gröbnerbasis dieses Ideals bezüglich der lexikographischen Ordnung mit Präzedenz $x_1 > x_2 > y_1 > y_2 > y_3 > y_4$ ist $G = \{x_1 - y_4, x_2 y_4 - y_3, x_2 y_3^3 - y_1, y_2 - y_3 y_4, y_1 y_4 - y_3^4\}$. Wir erhalten somit für den Term $x_1^{10} x_2^5$, der die rechten Seiten des Gleichungssystems kodiert,

$$\begin{array}{ccc} x_1^{10} x_2^5 & \longrightarrow_{x_1 - y_4} & x_1^9 x_2^5 y_4 \\ & \overset{9}{\longrightarrow}_{x_1 - y_4} & x_2^5 y_4^{10} \\ & \longrightarrow_{x_2 y_4 - y_3} & x_2^4 y_3 y_4^9 \\ & \overset{4}{\longrightarrow}_{x_2 y_4 - y_3} & y_3^5 y_4^5 \end{array}$$

und $y_3^5 y_4^5$ ist in Normalform. Dann ist $(0, 0, 5, 5)$ eine ganzzahlige Lösung unseres Gleichungssystems.

Als nächstes wollen wir uns dem allgemeineren Fall mit a_{ij} und b_i aus $\mathbf{Z}$ zuwenden. Da wir nun bei einer Kodierung des Gleichungssystems auch negative Exponenten erhalten würden, können wir nicht mehr in einem Polynomring $\mathbf{K}[x_1, \dots, x_n]$ arbeiten. Statt dessen wählen wir eine zusätzliche Variable w und arbeiten in dem affinen Quotientenring $\mathbf{K}[x_1, \dots, x_n, w]/\mathfrak{k}$ mit $\mathfrak{k} = \langle x_1 x_2 \dots x_n w - 1 \rangle$. Dann können wir nicht-negative Elemente a'_{ji} und d_i, $1 \leq i \leq m$, $1 \leq j \leq n$ finden, so daß für alle $1 \leq i \leq m$ gilt

$$(a_{1i}, \dots, a_{ni}) = (a'_{1i}, \dots, a'_{ni}) + d_i \cdot (-1, \dots, -1).$$

Im affinen Quotientenring $\mathbf{K}[x_1, \dots, x_n, w]/\mathfrak{k}$ gilt dann, da $x_1^{d_i} \dots x_n^{d_i} w^{d_i} - 1 \in \mathfrak{k}$ und somit auch $x_1^{a_{1i}} x_2^{a_{2i}} \dots x_n^{a_{ni}} * (x_1^{d_i} \dots x_n^{d_i} w^{d_i} - 1) \in \mathfrak{k}$,

$$\begin{array}{rcl} x_1^{a_{1i}} x_2^{a_{2i}} \dots x_n^{a_{ni}} + \mathfrak{k} & = & x_1^{a_{1i}} x_2^{a_{2i}} \dots x_n^{a_{ni}} + x_1^{a_{1i}} x_2^{a_{2i}} \dots x_n^{a_{ni}} * (x_1^{d_i} \dots x_n^{d_i} w^{d_i} - 1) + \mathfrak{k} \\ & = & x_1^{a'_{1i}} x_2^{a'_{2i}} \dots x_n^{a'_{ni}} w^{d_i} + \mathfrak{k}. \end{array}$$

Analog kann man auch $b'_1, \dots, b'_n, d \in \mathbf{N}$ finden, so daß $(b_1, \dots, b_n) = (b'_1, \dots, b'_n) + d \cdot (-1, \dots, -1)$ und man erhält

$$x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} + \mathfrak{k} = x_1^{b'_1} x_2^{b'_2} \dots x_n^{b'_n} w^d + \mathfrak{k}.$$

Wieder können wir eine Abbildung definieren wie folgt

$$\begin{array}{rlcl}\phi: & \mathbf{K}[y_1,\ldots,y_m] & \longrightarrow & \mathbf{K}[x_1,\ldots,x_n,w]/\mathfrak{k} \\ & y_i & \longmapsto & x_1^{a'_{1i}}x_2^{a'_{2i}}\ldots x_n^{a'_{ni}}w^{d_i}+\mathfrak{k}.\end{array}$$

Analog zu vorher erhält man:

Lemma 3.6.12 *Es gibt eine Lösung* $(\sigma_1,\ldots,\sigma_m)$ *aus* $\mathbf{N}^m$ *für das oben beschriebene Gleichungssystem genau dann, wenn* $x_1^{b'_1}\ldots x_n^{b'_n}w^d+\mathfrak{k}$ *Bild eines Termes aus* $\mathsf{T}^m(Y)$ *unter der Abbildung* ϕ *ist. Insbesondere folgt aus* $x_1^{b'_1}\ldots x_n^{b'_n}w^d+\mathfrak{k}=\phi(y_1^{\sigma_1}\ldots y_m^{\sigma_m})$*, daß* $(\sigma_1,\ldots,\sigma_m)$ *eine Lösung des Gleichungssystems ist.*

Nun können wir Satz 3.6.3 anwenden, da die besondere Gestalt der Gröbnerbasis es wieder garantiert, daß beim Test, ob ein Element im Bild der Funktion ϕ liegt, im positiven Fall auch ein Term geliefert wird. Dies folgt, da wie in Lemma 3.6.11 gilt:

Lemma 3.6.13 *Ist* $x_1^{b'_1}\ldots x_n^{b'_n}w^d+\mathfrak{k}$ *im Bild von* ϕ*, so gibt es einen Term aus* $\mathsf{T}^m(Y)$ *als Urbild.*

Somit haben wir die Grundlagen geschaffen, unsere spezielle Lösung auf Gleichungssysteme mit Koeffizienten a_{ij} und b_i aus $\mathbf{Z}$ zu erweitern.

Schauen wir uns ein Beispiel an. Wir betrachten das Gleichungssystem

$$\begin{array}{rcrcrcrcr} 3\cdot z_1 & - & 2\cdot z_2 & + & z_3 & - & z_4 & = & -1 \\ 4\cdot z_1 & + & z_2 & - & z_3 & & & = & 5.\end{array}$$

Wieder erhalten wir für jede Gleichung eine Variable, also x_1 und x_2, und für jede Unbekannte eine Variable, also y_1, y_2, y_3 und y_4. Unser Ideal $\mathfrak{k}$ ist $\langle x_1x_2w-1\rangle$. Die entsprechende Abbildung ist

$$\begin{array}{rccc}\phi: & \mathbf{Q}[y_1,y_2,y_3,y_4] & \longrightarrow & \mathbf{Q}[x_1,x_2,w]/\mathfrak{k} \\ & y_1 & \longmapsto & x_1^3x_2^4+\mathfrak{k} \\ & y_2 & \longmapsto & x_2^3w^2+\mathfrak{k} \\ & y_3 & \longmapsto & x_1^2w+\mathfrak{k} \\ & y_4 & \longmapsto & x_2w+\mathfrak{k}.\end{array}$$

Das dazugehörige Ideal ist $\mathfrak{i}=\langle y_1-x_1^3x_2^4, y_2-x_2^3w^2, y_3-x_1^2w, y_4-x_2w, x_1x_2w-1\rangle$. Die reduzierte normierte Gröbnerbasis dieses Ideals bezüglich der lexikographischen Ordnung mit Präzedenz $x_1>x_2>w>y_1>y_2>y_3>y_4$ ist $G=\{x_1-y_1y_3^4y_4^6, x_2-y_1y_3^3y_4^6, w-y_3y_4^2, y_1y_3^4y_4^7-1, y_1y_3^3y_4^8-y_2, y_1y_3^2y_4^9-y_2^2, y_1y_3y_4^{10}-y_2^3, y_1y_4^{11}-y_2^4, y_2y_3-y_4\}$. Da gilt $x_1^{-1}x_2^5+\mathfrak{k}=x_2^6w+\mathfrak{k}$, reduzieren wir den Term x_2^6w und erhalten

$$\begin{array}{rll} x_2^6w & \longrightarrow_{x_2-y_1y_3^3y_4^6} & x_2^5wy_1y_3^6y_4^6 \\ & \overset{5}{\longrightarrow}_{x_2-y_1y_3^3y_4^6} & wy_1^6y_3^{18}y_4^{36} \\ & \longrightarrow_{w-y_3y_4^2} & y_1^6y_3^{19}y_4^{38} \\ & \longrightarrow_{y_1y_3^4y_4^7-1} & y_1^5y_3^{15}y_4^{31} \\ & \overset{3}{\longrightarrow}_{y_1y_3^4y_4^7-1} & y_1^2y_3^3y_4^{10} \\ & \longrightarrow_{y_1y_3^3y_4^8-y_2} & y_1y_2y_4^2,\end{array}$$

und der Term $y_1y_2y_4^2$ ist in Normalform. Außer der Lösung $(1, 1, 0, 2)$ erhalten wir durch Inspektion des Reduktionsprozesses jedoch noch weitere Lösungen des Gleichungssystems. Jeder Term aus $\mathsf{T}^m(Y)$ aus obiger Reduktionskette beschreibt nämlich eine Lösung.

Nun wollen wir zur Lösung unseres eigentlichen Problems zurückkehren, d.h. wir wollen eine Lösung des Gleichungssystems bestimmen, für die auch noch die gegebene Kostenfunktion $c(z_1, \ldots, z_m) = \sum_{j=1}^{m} c_j \cdot z_j$ minimal ist. Diese zusätzliche Einschränkung werden wir in die Gröbnerbasenberechnung kodieren. Bisher haben wir nur benötigt, daß die Gröbnerbasis bezüglich einer Eliminationsordnung mit $X > w > Y$ bestimmt wurde. Wir werden nun unsere Kostenfunktion benutzen, um spezielle solche Termordnung auszuzeichnen.

Definition 3.6.14 *Eine Termordnung $<_Y^c$ auf den Variablen Y heißt* **kompatibel mit der Kostenfunktion** c **und der Abbildung** ϕ, *falls aus $\phi(y_1^{\sigma_1} \ldots y_m^{\sigma_m}) = \phi(y_1^{\sigma'_1} \ldots y_m^{\sigma'_m})$ und $c(\sigma_1, \ldots, \sigma_m) < c(\sigma'_1, \ldots, \sigma'_m)$ folgt, daß $y_1^{\sigma_1} \ldots y_m^{\sigma_m} <_Y^c y_1^{\sigma'_1} \ldots y_m^{\sigma'_m}$.*

Diese speziellen Termordnungen werden genau die Lösungen mit minimaler Kostenfunktion liefern.

Satz 3.6.15 *Es sei G eine Gröbnerbasis des zu unserem Gleichungssystem wie oben beschriebenen Ideals bezüglich einer Eliminationsordnung mit $X > w > Y$, wobei die Ordnung auf Y mit c und ϕ kompatibel ist. Dann folgt aus $x_1^{b'_1} \ldots x_n^{b'_n} w^d \xrightarrow{*}_G y_1^{\sigma_1} \ldots y_m^{\sigma_m}$ mit irreduziblem $y_1^{\sigma_1} \ldots y_m^{\sigma_m}$, daß die Lösung $(\sigma_1, \ldots, \sigma_m)$ die Kostenfunktion minimiert.*

Beweis :
Sei also $x_1^{b'_1} \ldots x_n^{b'_n} w^d \xrightarrow{*}_G y_1^{\sigma_1} \ldots y_m^{\sigma_m}$ mit irreduziblem $y_1^{\sigma_1} \ldots y_m^{\sigma_m}$. Dann ist sicherlich $(\sigma_1, \ldots, \sigma_m)$ eine Lösung unseres Gleichungssystems. Nehmen wir an, es gäbe eine weitere Lösung $(\sigma'_1, \ldots, \sigma'_m)$ mit $c(\sigma'_1, \ldots, \sigma'_m) < c(\sigma_1, \ldots, \sigma_m)$ und $y_1^{\sigma'_1} \ldots y_m^{\sigma'_m}$ sei die entsprechende Kodierung als Term. Dann gilt $\phi(y_1^{\sigma_1} \ldots y_m^{\sigma_m}) = \phi(y_1^{\sigma'_1} \ldots y_m^{\sigma'_m}) = x_1^{b'_1} \ldots x_n^{b'_n} w^d + \mathfrak{k}$. Somit liegt $y_1^{\sigma_1} \ldots y_m^{\sigma_m} - y_1^{\sigma'_1} \ldots y_m^{\sigma'_m}$ im Kern von ϕ, und dieser Kern liegt in dem von der Abbildung beschriebenen Ideal. Also muß gelten

$$y_1^{\sigma_1} \ldots y_m^{\sigma_m} - y_1^{\sigma'_1} \ldots y_m^{\sigma'_m} \xrightarrow{*}_G 0.$$

Da wir annehmen, daß $y_1^{\sigma_1} \ldots y_m^{\sigma_m} >_Y^c y_1^{\sigma'_1} \ldots y_m^{\sigma'_m}$ ist $y_1^{\sigma_1} \ldots y_m^{\sigma_m}$ also der Kopfterm dieses Polynoms und somit mit G reduzibel im Widerspruch zu der Annahme, daß er irreduzibel war.

q.e.d.

Natürlich können abhängig von der gewählten Termordnung verschiedene minimale Lösungen berechnet werden. Leider ist es im Allgemeinen nicht so einfach, eine geeignete kompatible Termordnung zu bestimmen. Sind jedoch alle Koeffizienten der Kostenfunktion nicht-negativ, so ist folgende Termordnung immer mit c und ϕ kompatibel: Ordne zuerst die Terme bezüglich der Kostenfunktion, und falls diese Werte übereinstimmen, benutze eine beliebige Ordnung.

Dies soll nun als Erweiterung unseres vorherigen Beispiels kurz skizziert werden. Als Kostenfunktion wählen wir $c(z_1, z_2, z_3, z_4) = 1000 \cdot z_1 + z_2 + z_3 + 100 \cdot z_4$. Als Ordnung benutzen wir die lexikographische Ordnung auf den Variablen X und w mit Präzedenz $x_1 > x_2 > w$ und auf Y eine Kombination der Kostenfunktion mit der lexikographischen Ordnung mit Präzedenz $y_1 > y_2 > y_3 > y_4$, d.h. $y_1^{\sigma_1} \dots y_m^{\sigma_m} <_c y_1^{\sigma'_1} \dots y_m^{\sigma'_m}$ genau dann, wenn $c(y_1^{\sigma_1} \dots y_m^{\sigma_m}) < c(y_1^{\sigma'_1} \dots y_m^{\sigma'_m})$ oder $c(y_1^{\sigma_1} \dots y_m^{\sigma_m}) = c(y_1^{\sigma'_1} \dots y_m^{\sigma'_m})$ und $y_1^{\sigma_1} \dots y_m^{\sigma_m} <_{lex} y_1^{\sigma'_1} \dots y_m^{\sigma'_m}$. Dann erhält man als Gröbnerbasis $G = \{w - y_2^2 y_4^3, y_4 - y_2 y_3, x_1 - y_1 y_2^6 y_3^{10}, x_2 - y_1 y_2^6 y_3^9, y_1 y_2^7 y_3^{11} - 1\}$. Reduziert man nun den Term $x_2^6 w$, so erhält man als Normalform $x_2^6 w \xrightarrow{*}_G y_1 y_2^3 y_3^2$, und wir erhalten somit eine Lösung $(1, 3, 2, 0)$ mit minimalen Kosten.

Übungen

1. Lösen Sie folgendes Gleichungssystem:

$$\begin{array}{rcrcrcr} 3 \cdot z_1 & + & 2 \cdot z_2 & + & z_3 & = & 10 \\ 4 \cdot z_1 & + & 3 \cdot z_2 & + & z_3 & = & 12. \end{array}$$

2. Lösen Sie folgendes Gleichungssystem:

$$\begin{array}{rcrcrcrcr} 2 \cdot z_1 & + & z_2 & - & 3 \cdot z_3 & + & z_4 & = & 4 \\ -3 \cdot z_1 & + & 2 \cdot z_2 & - & 2 \cdot z_3 & - & z_4 & = & -3. \end{array}$$

Kapitel 4

Verbesserungen von Buchbergers Algorithmus

Die Müh' ist klein, der Spaß ist groß.

Goethe

Will man Gröbnerbasen zum Lösen von algebraischen Problemen einsetzen, so ist es wichtig, Buchbergers Algorithmus möglichst effizient zu implementieren. Daher gilt es, unnötige Berechnungen zu erkennen und zu vermeiden. Da Buchbergers Algorithmus zur Berechnung einer Gröbnerbasis die Charakterisierung über s-Polynome benutzt, fällt die Hauptarbeit des Algorithmus beim Reduzieren von s-Polynomen zur Normalform an. In diesem Kapitel werden wir Kriterien kennenlernen, die es erlauben, gewisse s-Polynome, die sich auf jeden Fall zu Null reduzieren lassen, zu erkennen, ohne die Reduktion durchführen zu müssen. Somit kann man Normalformbestimmungen einsparen. Dies ist insbesondere von Bedeutung, da die Tatsache, daß ein s-Polynom zu Null reduzibel wäre, noch lange nicht impliziert, daß die Normalformberechnung im Algorithmus selbst die Null liefert. Die Null muß nämlich nicht bezüglich jeder Reduktionsstrategie die Normalform sein (wir haben unter Umständen ja noch keine Konfluenz).

4.1 Buchbergers erstes Kriterium

Erinnert man sich an spezielle Reduktionssysteme, die sogenannten Wortersetzungssysteme, so sind dort solche kritischen Situationen immer zusammenführbar, die aus sogenannten disjunkten Überlappungen entstehen. Etwas ähnliches kann man auch für Polynomreduktionen aufzeigen.

Satz 4.1.1 *Es sei F eine endliche Menge von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$ und f, g zwei Polynome aus F, so daß*

$$\mathsf{kgV}(\mathsf{HT}(f), \mathsf{HT}(g)) = \mathsf{HT}(f) \circ \mathsf{HT}(g),$$

d.h. die Kopfterme der beiden Polynome haben keinen echten gemeinsamen Teiler außer der 1*. Dann ist die Null eine Normalform des s-Polynoms* $\mathsf{spol}(f,g)$ *bezüglich Reduktion mit* F*.*

Beweis :
O.B.d.A. können wir annehmen, daß $\mathsf{HC}(g) = \mathsf{HC}(g) = 1$. Dann gilt:

$$\begin{aligned}
\mathsf{spol}(f,g) &= \mathsf{HT}(g) * f - \mathsf{HT}(f) * g \\
&= (g - \mathsf{RED}(g)) * f - (f - \mathsf{RED}(f)) * g \\
&= g * f - \mathsf{RED}(g) * f - f * g + \mathsf{RED}(f) * g \\
&= -\mathsf{RED}(g) * f + \mathsf{RED}(f) * g
\end{aligned}$$

Wir werden nun zeigen, daß für alle Terme $s \in \mathsf{T}(\mathsf{RED}(g))$ und $t \in \mathsf{T}(\mathsf{RED}(f))$ gilt $s \circ \mathsf{HT}(f) \neq t \circ \mathsf{HT}(g)$. Dies impliziert, daß sich das s-Polynom $\mathsf{spol}(f,g)$ durch $|\mathsf{RED}(g)|$ Anwendungen von f und $|\mathsf{RED}(f)|$ Anwendungen von g zu Null reduzieren läßt. Nehmen wir also an, es gäbe $s \in \mathsf{T}(\mathsf{RED}(g))$ und $t \in \mathsf{T}(\mathsf{RED}(f))$ mit $s \circ \mathsf{HT}(f) = t \circ \mathsf{HT}(g)$. Dann ist jedoch $t \circ \mathsf{HT}(g)$ ein gemeinsames Vielfaches von $\mathsf{HT}(f)$ und $\mathsf{HT}(g)$. Da $\mathsf{kgV}(\mathsf{HT}(f), \mathsf{HT}(g)) = \mathsf{HT}(f) \circ \mathsf{HT}(g)$, muß somit $\mathsf{HT}(f)$ den Term t teilen im Widerspruch zu $\mathsf{HT}(f) > t$.

q.e.d.

Machen wir uns die Argumentation aus diesem Beweis noch einmal an einem Beispiel deutlich.

Betrachten wir die Polynommenge $F = \{f_1 = yz + y, f_2 = x^3 + y, f_3 = y^2 + z\}$ aus $\mathbf{Q}[x,y,z]$, und als Termordnung wählen wir die länge-lexikographische Ordnung mit Präzedenz $x > y > z$. Dann erfüllt das s-Polynom zu f_1 und f_2 die Bedingung des Lemmas. Wir erhalten $\mathsf{spol}(f_1, f_2) = x^3y - y^2z$, und dies läßt sich mit den Polynomen f_1 und f_2 zu Null reduzieren. Daß jedoch nicht jede beliebige Reduktionskette die Null als Normalform liefern muß sehen wir, wenn wir $x^3y - y^2z$ wie folgt reduzieren:

$$x^3y - y^2z \longrightarrow_{f_2} -y^2z - y^2 \longrightarrow_{f_3} -y^2 + z^2 \longrightarrow_{f_3} z^2 + z.$$

Satz 4.1.1 bieten also eine erste Möglichkeit, unsere Charakterisierung von Gröbnerbasen über s-Polynome einzuschränken auf s-Polynome von Polynomen, deren Kopfterme einen echten gemeinsamen Teiler haben. Um noch weitere s-Polynome als überflüssig zu erkennen, wollen wir uns mit den s-Polynomen etwas näher beschäftigen. Wir haben sie kennengelernt als Resultat einer Reduktion eines Termes mit zwei verschiedenen Polynomen, also als eine sogenannte kritische Situation einer Reduktionsrelation, die aufgelöst werden muß, um lokale Konfluenz zu erreichen. Im nächsten Abschnitt wollen wir nun eine algebraische Motivation von s-Polynomen kennenlernen, die auch ein weiteres Kriterium zur Erkennung von Nullreduktionsketten liefern wird.

4.2 Syzygien und ein zweites Kriterium

Der Begriff Syzygie kommt aus der Astronomie.

> SYZYGIE [grch. Verbindung, Paar] Konjunktion[1] und Opposition[2] von Sonne und Mond.

Im Folgenden sei $F = \{f_1, \ldots, f_k\}$ immer eine Menge von Polynomen aus $\mathbf{K}[x_1, \ldots, x_n]$.

Definition 4.2.1 *Eine* **Syzygie der Kopfmonome** $\mathsf{HM}(f_1), \ldots, \mathsf{HM}(f_k)$ *von F ist ein k-Tupel von Polynomen $S = (h_1, \ldots, h_k)$ aus $\mathbf{K}[x_1, \ldots, x_n]^k$ so daß*[3]

$$\sum_{i=1}^{k} h_i * \mathsf{HM}(f_i) = 0.$$

Mit $S(F)$ bezeichnen wir die Menge aller solchen Syzygien.

Als Beispiel betrachten wir die Polynome $f_1 = yz + y$, $f_2 = x^3 + y$ und $f_3 = z^4$ aus $\mathbf{Q}[x, y, z]$, und als Termordnung wählen wir wieder die länge-lexikographische Ordnung mit Präzedenz $x > y > z$. Dann ist $S = (z^3, z^4, -x^3 - y)$ eine Syzygie von $\mathsf{HM}(f_1)$, $\mathsf{HM}(f_2)$ und $\mathsf{HM}(f_3)$, da

$$z^3 * \mathsf{HM}(f_1) + z^4 * \mathsf{HM}(f_2) + (-x^3 - y) * \mathsf{HM}(f_3) = yz^4 + x^3z^4 - x^3z^4 - yz^4 = 0.$$

Da für zwei Syzygien $S_1 = (h_1, \ldots, h_k)$ und $S_2 = (g_1, \ldots, g_k)$ aus $S(F)$ die Summe $S_1 + S_2 = (h_1 + g_1, \ldots, h_k + g_k)$ auch wieder eine Syzygie aus $S(F)$ ist und für ein Polynom f aus $\mathbf{K}[x_1, \ldots, x_n]$ das (Skalar-)Produkt $f \star S_1 = (f * h_1, \ldots, f * h_k)$ auch wieder eine Syzygie aus $S(F)$ ist, bildet diese Menge $S(F)$ einen Modul über $\mathbf{K}[x_1, \ldots, x_n]$. Zur Erinnerung heißt eine Menge $\mathcal{M}$ ein **Modul**[4] über einem kommutativen Ring $\mathbf{R}$ mit Eins, falls $\mathcal{M}$ eine additive Gruppe mit Skalarmultiplikation mit Elementen aus $\mathbf{R}$ ist, für die folgende Axiome gelten:

1. Für alle a aus $\mathbf{R}$ und m aus $\mathcal{M}$ gilt $a \cdot m$ aus $\mathcal{M}$.
2. Für alle a aus $\mathbf{R}$ und m_1, m_2 aus $\mathcal{M}$ gilt $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$.
3. Für alle a_1, a_2 aus $\mathbf{R}$ und m aus $\mathcal{M}$ gilt $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$.
4. Für alle a_1, a_2 aus $\mathbf{R}$ und m aus $\mathcal{M}$ gilt $a_1 \cdot (a_2 \cdot m) = (a_1 \cdot a_2) \cdot m$.
5. Für alle m aus $\mathcal{M}$ gilt $1 \cdot m = m$.

---

[1] Konjunktion findet statt, wenn zwei Gestirne auf dem gleichen Längenkreis stehen.

[2] Opposition tritt ein, wenn der Längenunterschied 180° beträgt.

[3] In der Literatur findet sich auch die Definition von Syzygien von Polynomen $f_1, \ldots, f_k$ mittels der Summe $\sum_{i=1}^{k} h_i * f_i = 0$.

[4] Moduln unterscheiden sich insofern von Vektorräumen, als die Skalare nur aus einem Ring und nicht aus einem Körper sein müssen.

Ein Beispiel eines Moduls haben wir bereits kennengelernt – Ideale sind $\mathbf{K}[x_1, \ldots, x_n]$-Moduln. Im Folgenden werden wir uns mit einem weiteren $\mathbf{K}[x_1, \ldots, x_n]$-Modul, der Menge $\mathbf{K}[x_1, \ldots, x_n]^k$ beschäftigen[5]. Als (freie) Basis wählen wir die Vektoren

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \mathbf{e}_k = (0, \ldots, 0, 1).$$

Die Menge der Syzygien $S(F)$ ist ein sogenannter **Untermodul** von $\mathbf{K}[x_1, \ldots, x_n]^k$, und jedes Element $S = (h_1, \ldots, h_k)$ dieser Menge läßt sich schreiben als Summe $\sum_{i=1}^k h_i \star \mathbf{e}_i$. Für Syzygien, die zu s-Polynomen korrespondieren, erhält man somit folgende Schreibweise: Es seien f_i und f_j zwei Polynome aus F mit $i < j$ und $t = \mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j)) = \mathsf{HT}(f_i) \circ s_i = \mathsf{HT}(f_j) \circ s_j$ mit Termen s_i, s_j aus T^n. Dann ist

$$S_{ij} = \mathsf{HC}(f_i)^{-1} \cdot s_i \star \mathbf{e}_i - \mathsf{HC}(f_j)^{-1} \cdot s_j \star \mathbf{e}_j$$

eine Syzygie, die auch als

$$S_{ij} = (\underbrace{0, \ldots, 0}_{i-1}, \mathsf{HC}(f_i)^{-1} \cdot s_i, \underbrace{0, \ldots, 0}_{j-i}, \mathsf{HC}(f_j)^{-1} \cdot s_j, \underbrace{0, \ldots, 0}_{k-j})$$

geschrieben werden kann. Eine Interpretation des Namens s-Polynom ergibt sich durch „Syzygien-Polynom". Es wird in der Literatur jedoch auch die Interpretation „substraction-polynomial" angeboten, die wohl mehr der ursprünglichen Idee Buchbergers entspricht.

Ähnlich wie Ideale kann man Untermodule auch über Erzeugendensysteme definieren, und da Ideale ein Spezialfall der Untermoduln waren, benutzen wir die gleiche Notation für ein solches Erzeugnis, nämlich für eine Menge von Vektoren $\{\mathbf{a}_1, \ldots, \mathbf{a}_s\}$ aus $\mathbf{K}[x_1, \ldots, x_n]^k$ schreiben wir

$$\langle \mathbf{a}_1, \ldots, \mathbf{a}_s \rangle = \{\sum_{i=1}^k h_i \star \mathbf{a}_i \mid h_1, \ldots, h_s \in \mathbf{K}[x_1, \ldots, x_n]\}.$$

Wichtig ist nun, daß wiederum alle Untermodule von $\mathbf{K}[x_1, \ldots, x_n]^k$ endlich erzeugt sind und daher insbesondere die Menge der Syzygien $S(F)$. Wir werden zeigen, daß die zu den s-Polynomen von F korrespondierenden Syzygien S_{ij} gerade eine solche endliche Basis bilden. Hierzu benötigen wir den Begriff der homogenen Syzygien.

Definition 4.2.2 *Eine Syzygie der Gestalt* $S = (a_1 \cdot t_1, \ldots, a_k \cdot t_k)$ *aus* $S(F)$ *mit* $a_i \in \mathbf{K}$, $t_i \in \mathsf{T}^n$, $1 \leq i \leq k$ *heißt* **homogen vom Grade** $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$, *falls für alle* $1 \leq j \leq n$, $1 \leq i \leq k$ *gilt* $\mathsf{grad}_{x_j}(t_i * f_i) = \alpha_j$.

Die Syzygien, welche zu den s-Polynomen korrespondieren, sind homogen.

Lemma 4.2.3 *Jedes Element aus* $S(F)$ *kann (sogar eindeutig) als Summe homogener Elemente aus* $S(F)$ *dargestellt werden.*

[5] Der Exponent k korrepondiert zu der Anzahl der Polynome in unserer Menge F.

Beweis :
Es sei $S = (h_1, \ldots, h_k)$ eine beliebige Syzygie aus $S(F)$. Für ein festes Tupel $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$ bezeichnen wir mit $t_{j\alpha}$ den Term aus $\mathsf{T}(h_j)$ (falls es ihn gibt), für den gilt $\mathsf{grad}_{x_i}(t_{j\alpha} * f_j) = \alpha_i$ für alle $1 \leq i \leq n$. Dann muß gelten $\sum_{j=1}^{s} a_{j\alpha} \cdot t_{j\alpha} * f_j = 0$, wobei $a_{j\alpha}$ der Koeffizient von $t_{j\alpha}$ in h_j ist. Somit ist $S_\alpha = (a_{1\alpha} \cdot t_{1\alpha}, \ldots, a_{k\alpha} \cdot t_{k\alpha})$ eine homogene Syzygie in $S(F)$, und wir können S schreiben als $S = \sum_{\alpha \in \mathbf{N}^n} S_\alpha$.

q.e.d.

Dieses Lemma kann nun benutzt werden, um zu zeigen, daß für die Elemente S_α sogar die Syzygien S_{ij} benutzt werden können.

Satz 4.2.4 *Jede Syzygie S aus $S(F)$ kann dargestellt werden als Summe*

$$\sum_{i<j} h_{ij} \star S_{ij}$$

wobei die h_{ij} Polynome aus $\mathbf{K}[x_1, \ldots, x_n]$ und die S_{ij} die zu f_i, f_j assoziierten Syzygien sind.

Beweis :
Nach Lemma 4.2.3 läßt sich S als Summe von homogenen Syzygien schreiben. Es genügt also zu zeigen, daß sich eine homogene Syzygie als Summe in den S_{ij} darstellen läßt. O.B.d.A sei also $S = (a_1 \cdot t_1, \ldots, a_k \cdot t_k)$ homogen vom Grade $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$ und nicht der Nullvektor. Dann enthält S mindestens zwei Komponenten $a_i \cdot t_i$ und $a_j \cdot t_j$ beide ungleich Null mit $i < j$. Weiter sei $\mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j)) = \mathsf{HT}(f_i) \circ s_i = \mathsf{HT}(f_j) \circ s_j$ mit s_i, s_j aus T^n. Da $\mathsf{grad}_{x_l}(t_i * f_i) = \mathsf{grad}_{x_l}(t_j * f_j) = \alpha_l$ für $1 \leq l \leq n$ teilt $\mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j))$ den Term $\mathsf{HT}(t_i * f_i) = \mathsf{HT}(t_j * f_j)$ und für den Teiler $s \in \mathsf{T}^n$ gilt, daß die i-te Komponente in der Syzygie $S - a_i \cdot \mathsf{HC}(f_i) \cdot s \star S_{ij}$ Null sein muß, da

$$\begin{aligned}
& S - a_i \cdot \mathsf{HC}(f_i) \cdot s \star S_{ij} \\
= \; & S - a_i \cdot \mathsf{HC}(f_i) \cdot s \star (\mathsf{HC}(f_i)^{-1} \cdot s_i \star \mathbf{e}_i - \mathsf{HC}(f_j)^{-1} \cdot s_j \star \mathbf{e}_j) \\
= \; & S - a_i \cdot \mathsf{HC}(f_i) \cdot (\mathsf{HC}(f_i)^{-1} \cdot s_i \circ s \star \mathbf{e}_i - \mathsf{HC}(f_j)^{-1} \cdot s_j \circ s \star \mathbf{e}_j) \\
= \; & S - a_i \cdot t_i \star \mathbf{e}_i + a_i \cdot \mathsf{HC}(f_i) \cdot \mathsf{HC}(f_j)^{-1} \cdot t_j \star \mathbf{e}_j.
\end{aligned}$$

Diese neue Syzygie ist wiederum homogen vom Grade α und hat mindestens eine Komponente weniger, die ungleich Null ist. Auf diese Art kann man also eine gewünschte Darstellung für S finden.

q.e.d.

Es stellt sich nun die Frage, ob man wirklich alle S_{ij} als Basis für $S(F)$ braucht. Zur Illustration betrachten wir folgendes Beispiel:

Es sei $F = \{f_1 = x^2y^2 + z, f_2 = xy^2 + y^2, f_3 = x^2y + z^2\}$ wieder eine Menge von Polynomen aus $\mathbf{Q}[x, y, z]$, und als Termordnung wählen wir die länge-lexikographische

Ordnung mit Präzedenz $x > y > z$. Dann erhalten wir folgende zu den s-Polynomen korrespondierenden Syzygien

$$\begin{aligned} S_{12} &= (1, -x, 0) \\ S_{13} &= (1, 0, -y) \\ S_{23} &= (0, x, -y). \end{aligned}$$

Da jedoch $S_{13} = S_{12} + S_{23}$ gilt, ist diese Syzygie überflüssig, da bereits S_{12} und S_{23} eine Basis von $S(F)$ bilden.

Wir werden nun eine Charakterisierung von Gröbnerbasen über Syzygien vornehmen, um daraus ein zweites Kriterium zur Verbesserung von Buchbergers Algorithmus abzuleiten.

Satz 4.2.5 *Eine Menge $F = \{f_1, \ldots, f_k\}$ aus $\mathbf{K}[x_1, \ldots, x_n]$ ist eine Gröbnerbasis (des Ideals $\langle F \rangle$) genau dann, wenn für alle Syzygien $S = (h_1, \ldots, h_k)$ einer homogenen Basis von $S(F)$ gilt, daß*

$$\sum_{i=1}^{k} h_i * f_i \xrightarrow{*}_F 0.$$

Setzt man als Basis gerade die Menge der Syzygien S_{ij} ein, so erhält man Buchbergers Charakterisierung einer Gröbnerbasis über die s-Polynome. Der nächste Satz zeigt nun, wann man Elemente aus dieser speziellen homogenen Basis von $S(F)$ streichen kann.

Satz 4.2.6 *Für eine Polynomemenge $F = \{f_1, \ldots, f_s\}$ aus $\mathbf{K}[x_1, \ldots, x_n]$ sei B eine Teilmenge von $\{S_{ij} \mid 1 \leq i < j \leq s\}$, welche eine Basis von $S(F)$ ist. Nehmen wir an es gäbe Polynome f_i, f_j, f_k aus F, so daß $\mathsf{HT}(f_k)$ den Term $\mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j))$ teilt. Dann ist, falls S_{ik} und S_{jk} in B liegen, $B \backslash \{S_{ij}\}$ auch eine Basis von $S(F)$.*

Beweis :
O.B.d.A. nehmen wir an, daß $i < j < k$ und $k_{ij} = \mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j))$, $k_{ik} = \mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_k))$ und $k_{jk} = \mathsf{kgV}(\mathsf{HT}(f_j), \mathsf{HT}(f_k))$. Weiter gilt, da t_k den Term k_{ij} teilt $k_{ij} = t_i \circ s_i = t_j \circ s_j = t_k \circ s$. Somit teilen jedoch auch k_{ik} und k_{jk} den Term k_{ij}. Für das zu f_i und f_j assoziierte Polynom S_{ij} gilt nun

$$\begin{aligned} S_{ij} &= \mathsf{HC}(f_i)^{-1} \cdot \frac{k_{ij}}{\mathsf{HT}(f_i)} \star \mathbf{e}_i - \mathsf{HC}(f_j)^{-1} \cdot \frac{k_{ij}}{\mathsf{HT}(f_j)} \star \mathbf{e}_j \\ &= \frac{k_{ij}}{k_{ik}} \star (\mathsf{HC}(f_i)^{-1} \cdot \frac{k_{ik}}{\mathsf{HT}(f_i)} \star \mathbf{e}_i - \mathsf{HC}(f_k)^{-1} \cdot \frac{k_{ik}}{\mathsf{HT}(f_k)} \star \mathbf{e}_k) \\ &\quad - \frac{k_{ij}}{k_{jk}} \star (\mathsf{HC}(f_j)^{-1} \cdot \frac{k_{jk}}{\mathsf{HT}(f_j)} \star \mathbf{e}_j - \mathsf{HC}(f_k)^{-1} \cdot \frac{k_{jk}}{\mathsf{HT}(f_k)} \star \mathbf{e}_k) \\ &= \frac{k_{ij}}{k_{ik}} \star S_{ik} - \frac{k_{ij}}{k_{jk}} \star S_{jk}, \end{aligned}$$

und somit kann S_{ij} als Linearkombination von S_{ik} und S_{jk} ausgedrückt werden.

q.e.d.

Dieser Satz liefert somit ein zweites Kriterium, um s-Polynome ohne Reduktion abzuhandeln. Im nächsten Abschnitt soll nun eine verbesserte Version von Buchbergers Algorithmus vorgestellt werden.

4.3 Noch einmal Buchbergers Algorithmus

Im Folgenden wollen wir die beiden aufgezeigten Kriterien benutzen, um Buchbergers ursprünglichen Algorithmus zu verbessern. Um Satz 4.2.6 anwenden zu können, benötigen wir zusätzlich eine Menge geordneter Paare (i,j) mit $i<j$. Da wir nicht immer wissen werden, ob bei einem Paar von Indizes $i \neq j$, $i>j$ oder $j>i$ gilt, werden wir folgende Notation benutzen:

$$[i,j] = \begin{cases} (i,j) & \text{falls } i<j \\ (j,i) & \text{falls } j<i \end{cases}$$

Weiterhin sei $\textsc{Syzygienkriterium}(f_i, f_j, B)$ eine boolsche Funktion, die testet, ob für zwei Polynome f_i und f_j aus F das in Satz 4.2.6 beschriebene Kriterium bezüglich einer aus geordneten Paaren von Indizes bestehenden Menge B gilt. Diese Funktion liefert **wahr** genau dann, wenn es einen von i und j verschiedenen Index k gibt, für den beide Paare $[i,k]$ und $[j,k]$ in B sind und $\mathsf{HT}(f_k)$ den Term $\mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j))$ teilt.

Verbesserter Buchberger Algorithmus

Eingabe: Eine endliche Menge von Polynomen $F = \{f_1, \ldots, f_k\}$ aus $\mathbf{K}[x_1, \ldots, x_n]$.
Ausgabe: Eine Gröbnerbasis G von $\langle F \rangle$.

$t := k$;
$G := F$;
$B := \{(i,j) \mid 1 \le i < j \le t\}$;
while $B \neq \emptyset$ **do**
  wähle ein Paar (i,j) aus B;
  $B := B \backslash \{(i,j)\}$;
  if $\mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j)) \neq \mathsf{HT}(f_i) \circ \mathsf{HT}(f_j)$ **und**
    $\textsc{Syzygienkriterium}(f_i, f_j, B) \neq$ **wahr then**
    $h := \mathsf{spol}(f_i, f_j)$;
    $h := \textsc{Normalform}(h, G)$;
    if $h \neq 0$ **then**
      $t := t+1$;
      $f_t := h$;
      $G := G \cup \{f_t\}$;
      $B := B \cup \{(i,t) \mid 1 \le i \le t-1\}$;
    endif
  endif
endwhile

Es bleibt zu zeigen, daß dieser Algorithmus eine Gröbnerbasis berechnet.

Die Idee dieses Algorithmus ist es, in der Menge B diejenigen Paare (i,j) zu speichern, für die noch die s-Polynome getestet werden müssen. Bevor dann zu einem Paar aus B wirklich ein s-Polynom berechnet wird, wird zuerst überprüft, ob eines unserer Kriterien benutzt werden kann, um die Berechnung des s-Polynom zu vermeiden.

Termination folgt nach Dicksons Lemma ähnlich wie für den ursprünglichen Algorithmus von Buchberger.

Sei also $G_a = \{f_1, \ldots, f_s\}$ die Ausgabe und $B_a = \{(i,j) \mid 1 \leq i < j \leq s\}$. Wir wollen zeigen, daß für jedes Paar (i,j) aus B_a entweder $\mathsf{spol}(f_i, f_j) \xrightarrow{*}_{G_a} 0$ gilt oder das Prädikat $\textsc{Syzygienkriterium}(f_i, f_j, B_a)$ hält. Da nämlich nach Satz 4.2.6 auch die Menge $B_a \backslash \{(i,j) \mid \textsc{Syzygienkriterium}(f_i, f_j, B_a) = \text{wahr}, 1 \leq i < j \leq s\}$ eine homogene Basis von $S(G_a)$ ist, folgt somit die Korrektheit.

Offensichtlich ist nach Konstruktion der Menge B im Algorithmus jedes (i,j) aus B_a irgendwann einmal in B enthalten. Wird es aus B entfernt und es gilt $\textsc{Syzygienkriterium}(f_i, f_j, B)$, wobei die zu dem Zeitpunkt im Algorithmus bestehende Menge B Teilmenge von B_a ist, so gilt auch unsere Behauptung. Gilt hingegen für die Kopfterme der Polynome f_i und f_j $\mathsf{kgV}(\mathsf{HT}(f_i), \mathsf{HT}(f_j)) = \mathsf{HT}(f_i) \circ \mathsf{HT}(f_j)$, so impliziert Satz 4.1.1 sofort, daß sich $\mathsf{spol}(f_i, f_j)$ mit der aktuellen Menge G nach Null reduzieren läßt, also insbesondere mit der Ausgabemenge G_a. Es bleibt der Fall, daß tatsächlich das s-Polynom berechnet wird, und entweder wird dieses zu Null reduziert, oder aber die Normalform f_t wird G hinzugefügt, und da sicherlich $\mathsf{spol}(f_i, f_j) \xrightarrow{*}_{G \cup \{f_t\}} 0$ gilt, gilt dies auch für die Ausgabemenge, und wir sind fertig.

Es zeigt sich, daß es sinnvoll ist, solche Früherkennung von überfüssigen s-Polynomen einzubauen. Experimente zeigen, daß man bei eigentlich N zu betrachtenden s-Polynomen mit diesen beiden Kriterien unter Umständen mit $\sqrt{N}$ s-Polynomen auskommt.

Ebenfalls von großer Bedeutung für die Komplexität des Gröbnerbasenalgorithmus ist die gewählte Termordnung. Schauen wir uns z.B. das Ideal $\langle x^2 + xy + y, y^2 + yz + z, z^2 + z + 1 \rangle$ aus $\mathbf{Q}[x,y,z]$ an. Dann ist diese Basis bereits eine reduzierte Gröbnerbasis bezüglich allen Termordnungen, für die x^7, y^5 beziehungsweise z^2 die jeweiligen Kopfterme sind. Wählt man jedoch die lexikographische Ordnung mit Präzedenz $z > y > x$ als Termordnung, so werden die Polynome wie folgt umsortiert: $xy + y + x^2$, $yz + z + y^2$ und $z^2 + z + 1$. Man sieht sofort, daß die drei Polynome miteinandner s-Polynome bilden, von denen nur eines durch unsere Kriterien ausgeschlossen werden kann. Wir erhalten in einem ersten Schritt zusätzlich die Polynome $\mathsf{spol}(xy + y + x^2, yz + z + y^2) = yz + x^2 z - xz - xy^2 \longrightarrow_{yz+z+y^2} x^2 z - xz - z - xy^2 - y^2$, $\mathsf{spol}(yz + z + y^2, z^2 + z + 1) = z^2 + y^2 z - yz - y \longrightarrow_{z^2+z+1} y^2 z - yz + z - y \longrightarrow_{yz+z+y^2} -2 \cdot yz + z - y^3 - y \longrightarrow_{yz+z+y^2} 3 \cdot z - y^3 + 2 \cdot y^2 - y$. Eine Gröbnerbasis mit dieser Ordnung zu berechnen, wird eine ganz andere Komplexität haben.

Wie wir in Kapitel 3 gesehen haben, schreiben häufig die Anwendungen die Ordnung, bezüglich der die Gröbnerbasis berechnet werden muß, vor. In der Regel sind dies Eliminationsordnungen, und häufig ist es aufwendig, eine Gröbnerbasis bezüglich einer solchen Ordnung zu berechnen. Daher stellt sich die Frage, ob man nicht ausgehend von einer Gröbnerbasis bezüglich einer beliebigen Ordnung eine Gröbnerbasis bezüglich einer neuen Ordnung berechnen kann. Solche Basiskonversionen werden in der Literatur vorgestellt, sprengen jedoch den Rahmen dieser Vorlesung.

Ein weiteres Feld für Optimierungsmöglichkeiten bieten die Auswahlmöglichkeiten der Paare (i, j) aus B und die Auswahlmöglichkeiten der Polynome aus G bei der Normalformbildung. Auch hier gibt es in der Literatur Vorschläge, Untersuchungen und Beispiele, die einen Einblick in das Verhalten des Algorithmus geben.

Literaturverzeichnis

[AdLo94] W.W. Adams und P. Loustaunau. *An Introduction to Gröbner Bases.* American Mathematical Society. 1994.

[BeWe92] T. Becker und V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer Verlag. 1992.

[Bu65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* Dissertation. Universität Innsbruck. 1965.

[CoLiOS92] D. Cox, J. Little und D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer Verlag. 1992.

[Ch88] S.C. Chou. *Mechanical Geometry Proving.* D. Reidel Publishing Company. Dordrecht. 1988.

[GeCzLa92] K.O. Geddes, S.R. Czapor and G. Labahn. *Algorithms for Computer Algebra.* Kluwer Academic Publishers. Massachusetts. 1992.

[Ya96] C.K. Yap. *Fundamental Problems in Algorithmic Algebra.* Princeton University Press. 1996.