Notizen zur Vorlesung
Konstruktive Nichtlineare Algebra

H.-G. Gräbe

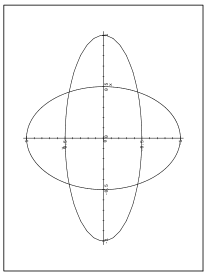
14. Juli 1997

1 Einführung

1.1 Besonderheiten bei nichtlinearen Gleichungssystemen

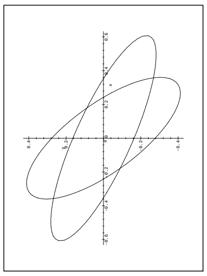
Bsp: Pseudolineares Gl.-S.

$$
\begin{aligned}
x^2 + 4y^2 &= 1\\
y^2 + 4x^2 &= 1
\end{aligned}
$$



Gleichungssystem nach Koordinatentransformation $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$:

$$
\begin{aligned}
17x^2 + 22xy + 13y^2 &= 1\\
8x^2 + 28xy + 37y^2 &= 1
\end{aligned}
$$



Klassisches Eliminationsverfahren der linearen Algebra hilft nicht mehr weiter. Was müßte ein korrektes Eliminationsverfahren im nichtlinearen Fall alles leisten?

Lösungsmenge hat paarweise verschiedene x-Werte, die wir wegen der obigen Transformation in unserem Beispiel kennen: $x \in \{\frac{-4}{5\sqrt{5}}, \frac{-2}{5\sqrt{5}}, \frac{2}{5\sqrt{5}}, \frac{4}{5\sqrt{5}}\}$

Das sind die Nullstellen des Polynoms

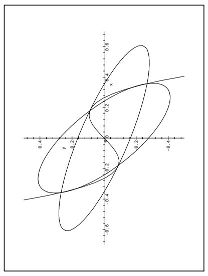
$$(x^2 - \frac{16}{125})(x^2 - \frac{4}{125}) = x^4 - \frac{4}{25}x^2 + \frac{2^6}{5^6}$$

Es gibt genau eine polynomiale Funktion 3. Grades, die durch die vier Lösungen geht (Interpolationsaufgabe):

$$y = -\frac{625}{48}x^3 + \frac{11}{12}x$$

D.h., eine allgemeine Theorie müßte die Polynome

$$\begin{aligned} f_1 &:= 17\,x^2 + 22\,x\,y + 13\,y^2 - 1 \\ f_2 &:= 8\,x^2 + 28\,x\,y + 37\,y^2 - 1 \end{aligned}$$



umwandeln in

$$\begin{aligned} g_1 &:= x^4 - \frac{4}{25}x^2 + \frac{2^6}{5^6} \\ g_2 &:= y + \frac{625}{48}\,x^3 - \frac{11}{12}\,x \end{aligned}$$

Beide Gleichungssysteme sind sogar äquivalent:

$$\begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = M_1 \cdot \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = M_2 \cdot \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$$

mit

$$M_1 := \begin{pmatrix} \left(-\frac{74}{625}\,y\,x + \frac{91}{1875}\,x^2 - \frac{296}{46875}\right) & \left(\frac{26}{625}\,y\,x + \frac{41}{1875}\,x^2 + \frac{104}{46875}\right) \\ \left(-\frac{37}{24}\,y + \frac{91}{144}\,x\right) & \left(\frac{13}{24}\,y + \frac{41}{144}\,x\right) \end{pmatrix}$$

und

$$M_2 := \begin{pmatrix} \left(-\frac{5078125}{2304}\left(x^2 - \frac{36}{325}\right)\right) & \left(\frac{8125}{48}\left(x^3 - \frac{1628}{8125}\,x - \frac{48}{625}\,y\right)\right) \\ \left(-\frac{14453125}{2304}\left(x^2 - \frac{36}{925}\right)\right) & \left(\frac{23125}{48}\left(x^3 - \frac{2972}{23125}\,x - \frac{48}{625}\,y\right)\right) \end{pmatrix}$$

Allerdings gilt nicht wie im linearen Fall $M_1 M_2 = E$, sondern nur $M_1 M_2\,\mathbf{g} = \mathbf{g}$ und $M_2 M_1\,\mathbf{f} = \mathbf{f}$

1.2 Folgerungen

Wir benötigen

- polynomiale statt skalarer Linearkombinationen
- Ringe statt Vektorräume
- Ideale statt Unterräume

Außerdem ist die Nullstellenbestimmung univariater Polynome eine Unteraufgabe der allgemeinen Fragestellung, die für algebraisch nicht abgeschlossene Körper zusätzliche Schwierigkeiten bereithält.

Aufgabe: Man versuche dasselbe Programm mit

$$\begin{aligned} y^2 - x^2 &= 1 \\ y^2 + x^2 &= 5 \end{aligned}$$

und der Koordinatentransformation $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$

Einige Worte zur Literatur.

2 Affine Varietäten

2.1 Situation und Bezeichnungen

$S = k[x_1, \ldots, x_n]$ Polynomring über einem Körper $k, \overline{k}$ dessen algebraischer Abschluß (in den meisten Fällen stelle man sich $k = \overline{k} = \mathbf{C}$ vor).

$\mathbf{A}^n := \{(a_1, \ldots, a_n) \ : \ a_i \in \overline{k}\}$ n-dim. affiner Raum

$B = \{f_1, \ldots, f_s\} \subset S$ (endliches) System von Polynomen

$V = V(B) := \{(a_1, \ldots, a_n) \ : \ f_i(\mathbf{a}) = 0 \ \forall\, i\}$ gemeinsame Nullstellenmenge.

Mengen $V \subset \mathbf{A}^n$, die sich auf diese Weise darstellen lassen, heißen *affine Varietäten.*

$I = I(B)$ das von B erzeugte Ideal in S

$V(B) = V(I(B))$

$I(V) := \{f \in S \ : \ f(\mathbf{a}) = 0 \ \forall\, \mathbf{a} \in V\}$ Menge der auf $V \subset \mathbf{A}^n$ verschwindenden polynomialen Funktionen

2.2 Beispiele

Affine Varietäten in der Ebene:

$V(F(x,y))$ beschreibt normalerweise eine Kurve in der Ebene. Ein besonders einfaches Beispiel sind Kurven $C = \{(x,y) \ : \ y = f(x)\}$, die sich durch einen expliziten funktionalen Zusammenhang angeben lassen. Ist f ein Polynom, so entspricht dem die Bestimmungsgleichung $V = V(y - f(x))$. Ist dagegen $f(x) = \frac{p(x)}{q(x)}$ eine rationale Funktion mit teilerfremden $p(x), q(x)$, so ist $V = V(q(x) \cdot y - p(x))$. In der Tat, $\mathbf{a} \in V$ wenn entweder $q(\mathbf{a}) \neq 0$ oder $p(\mathbf{a}) = q(\mathbf{a}) = 0$. Letzteres ist für univariate Polynome aber nicht möglich, da p und q teilerfremd sind, es also eine Darstellung $1 = u\,p + v\,q$ gibt.

Oftmals läßt sich aber $F(x,y)$ nicht nach einer der beiden Variablen auflösen, z.B. in $V(x^2 + y^2 - 1)$. Dies stellt einen Kreis dar und zu einem vorgegebenen y-Wert gibt es zwei Punkte mit dieser y-Koordinate, aber verschiedenen x-Koordinaten, und umgekehrt. Allerdings läßt diese Varietät eine rationale Parametrisierung zu

$$V := \left\{ \left(\frac{1 - r^2}{1 + r^2}, \frac{2r}{1 + r^2} \right) \ : \ r \in \overline{k} \right\}$$

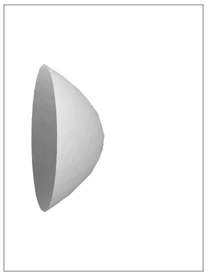
Diese erhält man durch folgende Überlegung: Wir betrachten die Schar der Gearden durch den Punkt $P := (-1, 0) \in V$, die durch deren Anstieg r parametrisiert seien. Eine solche Gerade ist also durch die Gleichung $y = r(x+1)$ gegeben und schneidet den Kreis außer in P in einem weiteren Punkt, dessen Koordinaten folglich durch r eindeutig bestimmt sind und umgekehrt. Durch Substitution in die Kreisgleichung erhalten wir

$$x^2 + r^2 x^2 + 2\,r^2 x + r^2 - 1 = (x+1)\left(x + r^2 x - 1 + r^2\right)$$

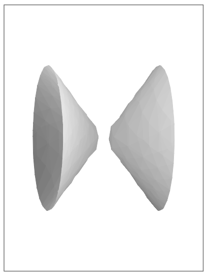
Daß sich dieses durch Elimination entstandene Polynom zweiten Grades in zwei Linearfaktoren zerlegen läßt, entspricht der Tatsache, daß wir einen seiner Faktoren, der P entspricht, vorab kannten. Der zweite Faktor beschreibt die x-Koordinate des zweiten Schnittpunkts, die Geradengleichung daraus die zugehörige y-Koordinate. Bemerkenswert ist, daß in Wirklichkeit alle Punkte bis auf P auf diese Weise (eindeutig) gewonnen werden können. P erhält man auf formale Weise, wenn man $r \to \infty$ streben läßt.

Aufgabe: Betrachten Sie auf analoge Weise die Kurve $V = V(y^2 - x^2 - x^3)$ und versuchen Sie, eine (rationale) Parametrisierung zu finden. Eine solche Kurve nennt man eine *elliptische Kurve.* Hinweis: Betrachten Sie Geraden durch $(0,0)$. Das erlaubt sogar eine reguläre Parametrisierung, d.h. eine solche durch polynomiale Ausdrücke.

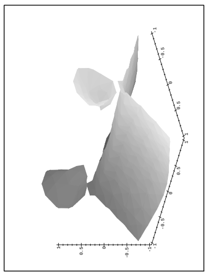
Affine Varietäten im Raum: Sind diese wiederum von der Gestalt $V = V(F(x,y,z))$, so handelt es sich um Flächen im Raum wie etwa die folgenden.



$V(x^2 + y^2 - z)$



$V(x^2 + y^2 - z^2)$



$V(x^2 - y^2z^2 + z^3)$
"Schweinsohrfläche"

Lassen sie sich durch zwei Gleichungen beschreiben, so erhalten wir im Normalfall eine Kurve im Raum:

$$V = V(\{y - x^2, z - x^3\}) = \{(t, t^2, t^3) \ : \ t \in \overline{k}\}$$

Diese Kurve nennt man die *getwistete Kubik*.

Das führt uns auf einen *intuitiven Dimensionsbegriff*: Die Dimension $dim\ V$ einer affinen Varietät V ist gleich der Anzahl der freien Parameter in den sie definierenden Gleichungen. Normalerweise ist zu erwarten, daß jede Gleichung eine Variable bindet, d.h. daß $dim\ V = n - m$ gilt, wenn V durch m Gleichungen im $\mathbf{A}^n$ gegeben werden kann. Dies ist allerdings bereits im Fall der linearen Algebra falsch, wo m durch den Rang der entsprechenden Matrix ersetzt werden muß. Im nichtlinearen Fall wird es noch komplizierter. Betrachten wir die ebene Varietät $V(\{y(x + y - 1), x^2 - x - y^2 + y\})$, die sich aus den beiden Teilvarietäten $V(\{x + y - 1\})$ und $V(\{x, y\})$ zusammensetzt, d.h. aus einem Punkt und einer Geraden besteht.

Polynomiale Gleichungssysteme entstehen aus den verschiedensten Anwendungen heraus. Hier z.B. eine Anwendung aus der Analysis:

Bestimme $max\,\{f = x^2 + y^2 \mid (x, y) \in C\}$ wobei C die Kurve $C = \{(x, y) \ : \ x^3 - x\,y + y^3 = 1\}$ ist.

Lösung mit der Methode der Lagrange-Faktoren ($\nabla f = \lambda \nabla g$) liefert das Gleichungssystem

$$\begin{aligned} 2\,x &= \lambda\,(\,3\,x^2 - y\,) \\ 2\,y &= \lambda\,(\,3\,y^2 - x\,) \\ x^3 - x\,y + y^3 &= 1 \end{aligned}$$

===> Weitere Beispiele, wo polynomiale Gleichungssysteme auf natürliche Weise auftreten.

2.3 Erste Eigenschaften affiner Varietäten

Beschreibung affiner Varietäten im $\mathbf{A}^1$:

Satz 1 *Eine affine Varietät $V \subset \mathbf{A}^1$ besteht aus dem ganzen $\mathbf{A}^1$ oder endlich vielen Punkten.*

Damit bekommen wir ein notwendiges Kriterium

Satz 2 *Ist V eine affine Varietät und g eine Gerade, so gilt $g \subset V$ oder $g \cap V$ ist endlich.*

Beweis: Betrachte die Geradengleichung $(c_1, \ldots, c_n) + t \cdot (v_1, \ldots, v_n)$ von g. Setzt man diese Punkte in die Bestimmungsgleichungen von V ein, so erhält man univariate Polynome in t, die eine Untervarietät im $\mathbf{A}^1$ beschreiben.

Beispiele nichtalgebraischer Mengen, basierend auf diesem Satz: Ein Intervall in der Ebene, eine Kreisscheibe, $\mathbf{A}^2 \setminus \{(0, 0)\}$.

Satz 3 *(1) $\emptyset$ und $\mathbf{A}^n$ sind affine Varietäten*

(2) *Sind V und W affine Varietäten im $\mathbf{A}^n$, so ist auch $V \cup W$ eine affine Varietät.*

(3) *Ist $V_\alpha \subset \mathbf{A}^n$ eine Familie affiner Varietäten, so auch ihr Durchschnitt.*

Beweis von (2+3): Ist $V = V(B)$ und $W = V(C)$, so gilt $V \cap W = V(B \cup C)$ und $V \cup W = V(\{fg : f \in B, g \in C\})$. Analog unendlicher Durchschnitt.

Die affinen Teilvarietäten des $\mathbf{A}^n$ erfüllen damit die Axiome eines Systems abgeschlossener Mengen und definieren somit eine Topologie, die sogenannte *Zariski-Topologie*. Begriff des topologischen Abschlusses $\overline{V}$ einer beliebigen Teilmenge $V \subset \mathbf{A}^n$: Dies ist die kleinste affine Varietät, die V umfaßt. Äquivalent:

$$\overline{V} = \bigcap \{W \ : W \supset V,\ W\ affin\}$$

AUFGABE:

(1) Zeige, daß (2) auch für endliche Vereinigungen affiner Varietäten gilt.

(2) Zeige an einem Beispiel, daß die unendliche Vereinigung affiner Varietäten nicht unbedingt eine affine Varietät sein muß.

(3) Zeige, daß $V \setminus W$ nicht unbedingt eine affine Varietät sein muß.

(4) Zeige, daß für affine Varietäten $V \subset \mathbf{A}^m$ und $W \subset \mathbf{A}^n$ das karthesische Produkt $V \times W \subset \mathbf{A}^{m+n}$ eine Varietät ist.

2.4 Parametrisierung affiner Varietäten

Im linearen Fall ist eine solche immer möglich:

$$\begin{array}{rcl} x+y+z &=& 1 \\ x+2y-z &=& 3 \end{array} \qquad \Leftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} -3 \\ 2 \\ 1 \end{pmatrix} \cdot t$$

Die Parametrisierung erfaßt alle Punkte der Varietät genau einmal.

Betrachten wir den nichtlinearen Fall, z.B. obige Parametrisierung der Kreislinie $C = V(x^2 + y^2 - 1)$

$$C' = \left\{ (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \ : \ t \in \mathbf{C}, t^2+1 \neq 0 \right\}$$

Hier kann man ebenfalls aus vorgegebenen Koordinaten $P = (x,y) \in C$ den Parameterwert $t = \frac{1-x}{y}$ eindeutig rekonstruieren, jedoch erfaßt C' den Punkt $(-1,0)$ auf der Kreislinie nicht. Eine vollständige Parametrisierung wäre etwa die trigonometrische

$$C'' = \{(\sin(t), \cos(t)) \ : \ t \in \mathbf{C}\},$$

die jedoch transzendente Funktionen verwendet und außerdem C mehrfach überdeckt. Wegen $cos(t) = \frac{e^{it}+e^{-it}}{2}$ und $sin(t) = \frac{e^{it}-e^{-it}}{2i}$ kann man daraus eine rationale Version mit komplexen Koeffizienten

$$C'' = \left\{ \left(\frac{t+\frac{1}{t}}{2}, \frac{t-\frac{1}{t}}{2i} \right) = \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2it} \right) \ : \ t \in \mathbf{C}, t \neq 0 \right\}$$

herleiten, die eine 1-1-Abbildung ist, aber zwei Ausnahmepunkte hat.

Sei nun V eine affine Varietät.

DEFINITION: Als *rationale Parameterdarstellung* (der Dimension d) von V bezeichnet man eine Darstellung durch rationale Funktionen $r_i = \frac{p_i}{q_i} \in k(t_1, \ldots, t_d)$, $i = 1, \ldots, n$, so daß

$$V' := \left\{ \left(\frac{p_i(\mathbf{a})}{q_i(\mathbf{a})}, i = 1, \ldots, n \right) \; : \; \mathbf{a} \in \mathbf{A}^d, \forall\, i\, q_i(\mathbf{a}) \neq 0 \right\}$$

V so weit wie möglich ausschöpft, d.h.

(1) $V' \subset V$ und

(2) $V = \overline{V'}$

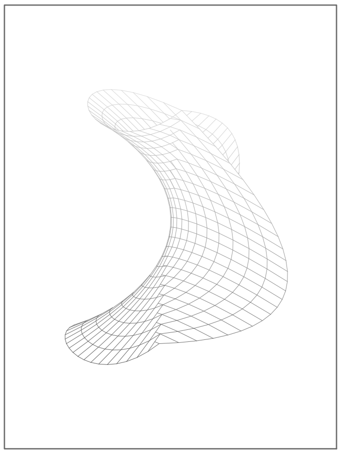
Normierung auf gemeinsamen Nenner möglich:

$$r_i = \frac{p_i}{q} \quad \text{mit} \quad gcd(p_1, \ldots, p_n, q) = 1$$

DEFINITION: Eine Parameterdarstellung heißt *polynomial* oder *regulär*, wenn $q(t) = 1$ gewählt werden kann, d.h. die $r_i(t)$ polynomiale Funktionen sind.

DEFINITION: Die Darstellung $V = V(f_1, \ldots, f_m)$ heißt *implizite Darstellung* von V.

Vorteile einer Parameterdarstellung: Man kann die Punkte auf V besser generieren. Bsp: Die “Schweinsohrfläche” $V = V(x^2 - y^2z^2 + z^3) = \{t(u^2 - t^2, u, t^2 - u^2) \; : \; (u, t) \in C^2\}$



Vorteile impliziter Darstellung für Test, ob Punkt auf Varietät liegt.

Damit entstehen folgende weiteren Fragen:

(1) Umrechnung einer impliziten in eine Parameterdarstellung

(2) Implizitierung einer Parameterdarstellung

Bei der zweiten Fragestellung entsteht wieder auf natürliche Weise ein Eliminationsproblem. Betrachten wir etwa die Kurve

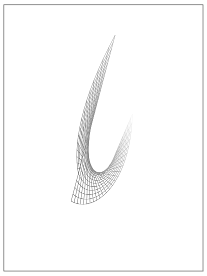
$$C := \{(1 - t, 1 - t^2) \; : \; t \in \overline{k}\},$$

so ist für eine implizite Darstellung aus dem Gleichungssystem

$$x = 1 - t, \; y = 1 - t^2$$

die Variable t zu eliminieren, was hier auf einfache Weise möglich ist und auf die implizite Gleichung $C = V(x^2 - 2x + y)$ führt.

Betrachten wir ein etwas komplizierteres Beispiel, die Tangentialfläche an die getwistete Kubik $C := \{(t, t^2, t^3) \ : \ t \in \overline{k}\}$



Der Tangentialvektor an den Punkt $(t, t^2, t^3) \in C$ hat die Koordinaten $(1, 2t, 3t^2)$. damit kann man jeden Punkt auf der Tangentialfläche durch zwei Parameter t und u beschreiben:

$$S := \{(t + u, t^2 + 2\,u\,t, t^3 + 3\,u\,t^2) \ : \ t, u \in \overline{k}\}$$

oder explizit

$$x = t + u, \ y = t^2 + 2\,u\,t, \ z = t^3 + 3\,u\,t^2$$

Implizitierung unter Verwendung der Lösungsformel für quadratische Gleichungen ergibt $u = x - t, t = x \pm \sqrt{x^2 - y}$ und insgesamt

$$S = V(z^2 - 6\,x\,y\,z + 4\,x^3\,z - 3\,x^2\,y^2 + 4\,y^3)$$

Aufgabe: Finden Sie eine Parametrisierung der linearen Varietät

$$V(x + 2y - 2z + w + 1, x + y + z - w - 2).$$

Aufgabe: Betrachten Sie die Kurve $C = \{(\frac{t}{1+t}, 1 - \frac{1}{t^2}) \ : \ t \in C\}$.
(a) Finden Sie die Gleichung der affinen Varietät $V = \overline{C}$.
(b) Zeigen Sie, daß $C = V \setminus \{(1,1)\}$ gilt.

Wir wollen diesen Abschnitt mit einem Beispiel aus dem CAGD, dem computergestützten Geometrie-Design beenden. Wenn man komplexe Formen wie etwa Autokarosserien oder Flugzeugflügel entwerfen will, brauchen die Ingenieure Kurven und Flächen, die variabel in ihrer Form, aber einfach zu beschreiben und schnell zu zeichnen sind. Dafür sind rational parametrisierte Kurven und Flächen bestens geeignet.

Nehmen wir der Einfachheit halber an, daß ein solcher Design-Ingenieur Kurven in der Ebene entwerfen will. Komplizierte Kurven werden gewöhnlich aus einfacheren Stücken zusammengesetzt, wobei man für deren glatte Komposition übereinstimmende Tangentialrichtungen an den Endpunkten benötigt. Der Designer muß also vier Größen kontrollieren können, nämlich Lage und Tagentialrichtung für den Start- und den Endpunkt.

Die *Bézier-Kurven*, benannt nach dem Renault Autodesigner P. Bézier, ist dafür besonders gut geeignet. Es handelt sich dabei um Kurven, die parametrisch gegeben sind durch die Gleichungen

$$\begin{aligned} x &= (1-t)^3 x_1 + 3t(1-t)^2 x_2 + 3t^2(1-t)x_3 + t^3 x_4 \\ y &= (1-t)^3 y_1 + 3t(1-t)^2 y_2 + 3t^2(1-t)y_3 + t^3 y_4 \end{aligned}$$

für $0 \le t \le 1$, wobei $x_1, \ldots, y_4$ die zu spezifizierenden Designkonstanten sind. Für $t = 0$ bzw. $t = 1$ bekommen wir

$$\begin{aligned} (x(0), y(0)) &= (x_1, y_1) \\ (x(1), y(1)) &= (x_4, y_4) \end{aligned}$$

und für die Tangentialrichtungen in den Endpunkten mit

$$x' = -3(1-t)^2 x_1 + 3(3t^2 - 4t + 1)x_2 + 3(2t - 3t^2)x_3 + 3t^2 x_4$$

schließlich

$$\begin{aligned}(x'(0), y'(0)) &= (3(x_2 - x_1), 3(y_2 - y_1))\\ (x'(1), y'(1)) &= (3(x_4 - x_3), 3(y_4 - y_3)).\end{aligned}$$

Die zu manipulierenden Parameter sind also durch die Lage der vier Punkte (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) eindeutig bestimmt. Diese vier Punkte heißen die *Kontrollpunkte* der Bézier-Kurve, das daraus zu bildende Viereck das *Kontroll-Polygon*. Durch die Lage der beiden mittleren Punkte kann man nicht nur die Tangentialrichtung, sondern auch die Tangentialgeschwindigkeit der Kurve variieren und so verschiedene Kurven mit denselben Tangentialrichtungen und denselben Endpunkten konstruieren.

Bézier-Kurven kommen ebenfalls in der Postscript-Sprache vor. Mit dem Kommando `curveto` kann man die vier Kontrollpunkte eingeben.

Aufgabe: Zeigen Sie, daß die Bézier-Kurve immer vollständig innerhalb ihres Kontrollpolygons verläuft.

Aufgabe: Eine andere interessante Kurve ist die *Strophoide*, die durch folgende trigonometrische Parametrisierung gegeben werden kann:

$$\begin{aligned}x &= a\ \sin(t)\\ y &= a\ \tan(t)(1 + \sin(t)),\end{aligned}$$

wobei a eine Konstante ist.

- Lassen Sie sich von einem CAS ein Bild einer Strophoide erzeugen.
- Zeigen Sie, daß eine Strophoide eine affine Varietät ist, indem Sie die beschreibende Gleichung finden. (Hinweis: $(a^2 - x^2)y^2 = x^2(a + x)^2$ ist nicht die richtige Antwort, da die entsprechende Varietät noch eine Komponente $\{(-a, y)\ :\ y \in \mathbf{C}\}$ enthält.
- Finden Sie eine rationale Parametrisierung für die Strophoide.

3 Ideale und Faktorringe

Sei wie oben $\mathbf{A}^n$ der affine n-dimensionale Raum und $R = k[x_1, \ldots, x_n]$ der Ring der polynomialen Funktionen auf $\mathbf{A}^n$. Zur Beschreibung affiner Varietäten spielen Ideale und Faktorringe von R als grundlegende algebraische Begriffe eine zentrale Rolle.

Definition: Eine Teilmenge $I \subset R$ heißt *Ideal*, wenn

- $0 \in I$,
- $f, g \in I\ \ =>\ \ f + g \in I$ und
- $f \in I,\ h \in R\ \ =>\ \ h \cdot f \in I$

gilt.

Mit einer endlichen Menge $B = \{f_1, f_2, \ldots, f_m\}$ von Polynomen muß also auch jede polynomiale Linearkombination zu I gehören.

Definition: Wir bezeichnen die Menge

$$I(B) = \{\sum h_i\, f_i\ \ :\ \ h_i \in R\}$$

als das von B *erzeugte* Ideal.

Man überzeugt sich leicht davon, daß es sich tatsächlich um ein Ideal handelt und daß dieses Ideal das kleinste Ideal ist, das B umfaßt. Ist $B = \{f\}$ eine einelementige Menge, so schreiben wir auch $I(f)$ statt $I(\{f\})$.

Jeder Ring enthält zwei triviale Ideale, das nur aus dem Nullelement bestehende *Nullideal* $I(0)$ und das aus dem ganzen Ring bestehende *Einsideal* $I(1)$.

DEFINITION: Ist umgekehrt ein Ideal I gegeben, so bezeichnet man eine (endliche) Teilmenge $B \subset I$ mit $I = I(B)$ als *(endliche) Basis* oder *Erzeugendensystem* von I. Eine Teilmenge, die minimal mit dieser Eigenschaft bzgl. der Inklusionsrelation ist, heißt *Minimalbasis*.

Es stellt sich heraus, daß dieser Begriff nicht die guten Eigenschaften von Vektorraumbasen hat. Insbesondere ist die Anzahl der Elemente in einer solchen Minimalbasis nicht eindeutig bestimmt. Betrachten wir dazu als Beispiel das Ideal $I_1 = I(x_1, x_2, x_3)$ aller Polynome in $k[x_1, x_2, x_3]$ ohne Absolutglied.

$$B_2 = \{x_1 + x_3\,,\ x_1^2 + x_2\,,\ x_1\,x_2\,,\ x_1^3 + x_1\}$$

und

$$B_3 = \{x_1 + x_3\,,\ x_1^2 + x_2\,,\ x_1\,x_2\,,\ x_1\,(x_1^2\,x_3 + x_1^2 + x_3 + 1)\,,\ x_1\,x_3\,(x_1^2 + 1)\}$$

erzeugen alle dasselbe Ideal, denn z.B. gilt

$$(x_1^2 + x_2)\,x_1 - x_1\,x_2 = x_1^3$$

AUFGABE: Zeigen Sie

(1) $I(x + x\,y, y + x\,y, x^2, y^2) = I(x, y)$

(2) $I(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = I(x^2 - 4, y^2 - 1)$

Insbesondere kann es schwierig zu erkennen sein, ob ein gegebenes Ideal das Einsideal ist.

Bsp.: $I = I(x_1^2 - x_2, x_2^2 - x_3, x_1 + x_3, x_1^3 - 1) = I(1)$

3.1 Restklassen und Faktorring bzgl. eines Ideals

Bisher hatten wir Ideale stets durch Angabe einer Basis beschrieben. Sei nun $V \subset \mathbf{A}^n$ eine Teilmenge des n-dimensionalen affinen Raums.

DEFINITION:

$$I(V) := \{f(x) \in R\ :\ f(a_1, \ldots, a_n) = 0 \text{ für alle } (a_1, \ldots, a_n) \in V\}$$

ist ein Ideal, das *Ideal der auf V verschwindenden Polynome*.

So ist etwa $I_1 = I(\,(0,0,0)\,)$ das Ideal der im Ursprung des $\mathbf{A}^3$ verschwindenden Polynome.

Etwas komplizierter ist es, das Verschwindungsideal $I_2 := I(V)$ der getwisteten Kubik $C_2 = \{(a, a^2, a^3)\ :\ a \in \mathbf{C}\}$ zu finden. Wir zeigen, daß dieses Ideal von der Basis $B_{2,1} = \{y - x^2, z - x^3\}$ erzeugt wird.

AUFGABE: CALI produziert für dieses Beispiel die Idealbasis $B_{2,2} = \{-xz + y^2, xy - z, x^2 - y\}$. Zeigen Sie, daß $I(B_{2,1}) = I(B_{2,2})$ gilt und daß $B_{2,2}$ keine Minimalbasis ist.

Der Beweis, daß $I(C_2) = I(B_{2,1})$ gilt, läßt sich am besten mit Restklassen modulo eines Ideals führen. Ähnlich wie für den Ring der ganzen Zahlen definieren wir dazu für ein Ideal $I \subset R$

$$f \equiv g\ (mod\ I)\ \ :<=>\ f - g \in I.$$

Bsp: Für $J := I(B_{2,1})$ gilt $xyz \equiv x^3 z \equiv x^4 y \equiv x^6\ (mod\ J)$

AUFGABE: Zeigen Sie, daß diese Relation eine Äquivalenzrelation ist, die außerdem Summen und Produkte respektiert, d.h. daß mit

$$\begin{array}{c} f_1 \equiv g_1\ (mod\ I) \\ f_2 \equiv g_2\ (mod\ I) \end{array}$$

auch

$$\begin{array}{c} f_1 \pm f_2 \equiv g_1 \pm g_2\ (mod\ I) \\ f_1 \cdot f_2 \equiv g_1 \cdot g_2\ (mod\ I) \end{array}$$

gilt. Dies bedeutet, daß es sich sogar um eine Kongruenzrelation handelt.

Offensichtlich ist $I(C_2) \supset J$. Für die umgekehrte Inklusion betrachten wir $f(x, y, z) \in I(V)$. Wegen $y \equiv x^2, z \equiv x^3\ (mod\ J)$ gilt $f(x, y, z) \equiv f(x, x^2, x^3) =: g(x)\ (mod\ J)$. Mit $f \in I(C_2)$ und $f - g \in J \subset I(C_2)$ folgt $g(x) \in I(C_2)$, also $g = 0$ und damit $f \equiv 0\ (mod\ J)$, d.h. $f \in J$.

Noch etwas komplizierter wird die Bestimmung der Idealbasis für das Verschwindungsideal I_3 der Kurve $C_3 := \{(a^2, a^3, a^5) \ : \ a \in \mathbf{C}\}$. Man überzeugt sich leicht, daß $B_3 := \{xy - z, x^3 - y^2\}$ in I_3 enthalten ist.

AUFGABE: Weitere Elemente des Verschwindungsideals sind etwa $x^5 - z^2$ oder $y^5 - z^3$. Zeigen Sie, daß diese Polynome in $I(B_3)$ liegen, für eine Minimalbasis also überflüssig sind.

Setzen wir wieder $J := I(B_3)$, so können wir mit den Beziehungen $z \equiv xy, \ y^2 \equiv x^3 \ (mod\ J)$ nur bis zu einer Darstellung $f(x,y,z) \equiv g_1(x) + g_2(x) \cdot y \ (mod\ J)$ reduzieren. Ist $g_i(x) = \sum c_{i,k} x^k$ so gilt allerdings $g_1(x) + g_2(x) y \in I(C_3)$ nur, wenn

$$g_1(a^2) + g_2(a^2) a^3 = \sum c_{1,k} a^{2k} + \sum c_{2,k} a^{2k+3} = 0$$

für alle $a \in \mathbf{C}$, also *identisch* in a gilt. Dafür müssen aber sowohl g_1 als auch g_2 identisch verschwinden, denn die erste Summe enthält nur gerade a-Potenzen, die zweite dagegen nur ungerade. Weiter argumentieren wir wie oben.

AUFGABE: Finden Sie das Verschwindungsideal der Kurve $C_4 := \{(a^3, a^4, a^5) \ : \ a \in \mathbf{C}\}$ und beweisen Sie die Richtigkeit Ihrer Aussage.

Wegen der Repräsentantenunabhängigkeit der Addition und Multiplikation der Restklassen modulo eines Ideals I bilden diese einen Ring, den *Restklassen-* oder *Faktorring* $S = R/I$ des Polynomrings R nach dem Ideal I. Für Verschwindungsideale $I(V)$ affiner Varietäten V hat dieser Ring eine direkte geometrische Interpretation. Sind nämlich $f, g \in R$ zwei Polynome, die als Funktionen auf V zusammenfallen, so gilt $f - g \in I(V)$ und umgekehrt. $k[V] := S/I(V)$ ist also der Ring der polynomialen Funktionen auf V. Diesen Ring bezeichnet man auch als den *Koordinatenring* von V.

3.2 Verschwindungsideal und affine Varietät

Betrachten wir nun die Beziehung zwischen einer affinen Varietät V und ihrem Verschwindungsideal $I(V)$ genauer. Die Überlegungen, die uns zur Basis des Verschwindungsideals in obigen Beispielen führten, kann man auch wie folgt beschreiben: $f(x,y,z)$ verschwindet genau dann auf der durch $(x,y,z) = (t, t^2, t^3)$ gegebenen Kurve, wenn das durch die entsprechenden Substitutionen aus f erzeugte Polynom identisch, d.h. als Element des Polynomrings $k[t]$, verschwindet. Die Ersetzung $x \to t, y \to t^2, z \to t^3$ induziert dabei einen Ringhomomorphismus $k[x,y,z] \longrightarrow k[t]$. $k[t]$ ist dabei der Koordinatenring des $\mathbf{A}^1$, der affinen Geraden. Identifiziert man $\mathbf{A}^1$ mit $\mathbf{C}$, so kann man die Darstellung $C_2 = \{(a, a^2, a^3) \ : \ a \in \mathbf{C}\}$ ebenfalls als Abbildung auffassen, nämlich als

$$\phi : \mathbf{A}^1 \longrightarrow \mathbf{A}^3 \qquad via \qquad a \mapsto (a, a^2, a^3),$$

deren Bild gerade die betrachtete Kurve ist.

In diesem Licht kann man jede reguläre Parametrisierung einer d-dimensionalen Varietät im n-dimensionalen Raum als Abbildung

$$\phi : \mathbf{A}^d \longrightarrow \mathbf{A}^n$$

betrachten, die einem Parametertupel $a = (a_1, \ldots, a_d) \in \mathbf{A}^d$ den Punkt $c = (\phi_1(a), \ldots, \phi_n(a)) \in \mathbf{A}^n$ zuordnet.

Eine solche Abbildung induziert eine dazu duale Abbildung zwischen den Koordinatenringen

$$\phi^* : R := k[x_1, \ldots, x_n] \longrightarrow R' := k[t_1, \ldots, t_d] \qquad via \qquad f \mapsto f \circ \phi,$$

die in die andere Richtung zeigt, also *kontravariant* wirkt. $f(x_1, \ldots, x_n) \in R$ verschwindet auf der durch ϕ parametrisierten Varietät $V := im(\phi) = \{(\phi_1(a), \ldots, \phi_n(a)) \ : \ a \in \mathbf{A}^d\}$ genau dann, wenn $f(\phi_1(a), \ldots, \phi_n(a)) = f(\phi(a)) = 0$, d.h. wenn $f \in ker(\phi^*)$. Hierbei steht $ker(\psi) = \{u \in R \ : \ \psi(u) = 0\}$ für den *Kern* des Ringhomomorphismus $\psi : R \longrightarrow R'$.

AUFGABE: Sei $\psi : R \longrightarrow R'$ ein Ringhomomorphismus.

(1) Zeigen Sie, daß der Kern eines beliebigen Ringhomomorphismus ein Ideal in R ist und sein Bild

$im(\psi)$ ein Unterring von R'.
(2) Zeigen Sie die Gültigkeit des ersten Isomorphiesatzes

$$im(\psi) \cong R/ker(\psi).$$

Damit bekommen wir die folgende Beschreibung des Verschwindungsideals einer durch eine reguläre Parametrisierung gegebenen affinen Varietät:

Satz 4 *Ist $V = im(\phi)$ eine regulär parametrisierte Varietät im $\mathbf{A}^n$ und $\phi : \mathbf{A}^d \longrightarrow \mathbf{A}^n$ die zugehörige Parametrisierung, so gilt $I(V) = ker(\phi^*)$ und $k[V] = R/I(V) = im(\phi^*)$.*

Betrachten wir nun die Beziehung zwischen den Operatoren $I()$ und $V()$, die einer gegebenen Teilmenge $V \subset \mathbf{A}^n$ das Ideal der auf ihr verschwindenden Polynome bzw. einem gegebenen Ideal $I \subset R$ die Menge seiner gemeinsamen Nullstellen zuordnet.

Starten wir bei einer Teilmenge V, bilden das Ideal $I = I(V)$ und davon die zugehörige Varietät, so enthält diese neben den Punkten von V noch all jene Punkte, die gemeinsame Nullstellen aller Funktionen sind, die auch auf ganz V verschwinden. Das ist offensichtlich die kleinste affine Varietät, die V umfaßt, also deren Abschluß. Ist insbesondere V bereits eine affine Varietät, so gilt $V(I(V)) = V$.

Starten wir dagegen mit einem Ideal I, bilden die gemeinsame Nullstellenmenge $V = V(I)$ und davon wieder das Ideal, so erhalten wir nicht notwendig I zurück, da jedes Polynom $f \in R$, für welches ein k existiert, so daß $f^k \in I$ gilt, ebenfalls auf V verschwindet. Ideale enthalten also neben der Information über die Nullstellen selbst weitere Information über die “Vielfachheit” der Nullstellen.

Definition: Für ein Ideal $I \subset R$ bezeichnen wir die Menge

$$rad(I) := \{f \in R \ : \ \exists\, k \ f^k \in I\}$$

als das *Radikal* von I.

Aufgabe: Zeigen Sie, daß $rad(I)$ wiederum ein Ideal ist.

Es stellt sich heraus, daß dies im Falle eines algebraisch abgeschlossenen Grundkörpers bereits alle Funktionen sind, die auf einer gegebenen Varietät V verschwinden. Betrachten wir dafür zunächst $V = \emptyset$. Es ist offensichtlich, daß die Frage nach Funktionen, deren Nullstellenmenge leer ist, ganz wesentlich vom Grundkörper abhängt. Im Fall eines algebraisch abgeschlossenen Körpers wissen wir aus dem Fundamentalsatz der Algebra, daß jedes nichtkonstante univariate Polynom eine (komplexe) Nullstelle besitzt. Ein ähnlicher Satz gilt für Ideale (o. Bew.):

Satz 5 *(Hilberts Nullstellensatz) Ist k ein algebraisch abgeschlossener Körper und $I \subset k[x_1, \ldots, x_n]$ ein Ideal, so gilt*

$$V(I) = \emptyset \quad \Leftrightarrow \quad I = I(1).$$

Äquivalent zu diesem Satz ist die folgende Charakterisierung von $I(V)$:

Satz 6 *Ist k ein algebraisch abgeschlossener Körper, $I \subset R := k[x_1, \ldots, x_n]$ ein Ideal und $V = V(I)$, so gilt $I(V) = rad(I)$.*

Beweis : Wir hatten schon gesehen, daß jede Funktion aus $rad(I)$ auf V verschwindet. Zum Beweis der Umkehrung verwenden wir den sogenannten *Rabinowitsch-Trick*: Sei $h \in I(V)$ und $B = \{f_\alpha\}$ eine Idealbasis von I. Sei weiter t eine neue Variable, $S = R[t]$ und $J \subset S$ das von $f_\alpha \in B$ und $f = 1 - h \cdot t$ erzeugte Ideal. Wegen $V(J) = \emptyset$ folgt $J = I(1)$, also gibt es $r, r_\alpha \in S$ mit

$$1 = \sum r_\alpha(x,t) f_\alpha(x) + r(x,t) \cdot (1 - h(x) \cdot t).$$

Substituieren wir nun überall $t \mapsto \frac{1}{h(x)}$ und multiplizieren mit dem Hauptnenner h^N durch, erhalten wir die Gleichung

$$h(x)^N = \sum \tilde{r}_\alpha(x) f_\alpha(x) + \tilde{r}(x) \cdot 0,$$

also $h^N \in I$. $\square$

DEFINITION: Ein Ideal $I \subset R$ mit $I = rad(I)$ nennen wir *Radikalideal.*

AUFGABE: Zeigen Sie, daß man auch umgekehrt aus diesem Satz den Hilbertschen Nullstellensatz herleiten kann.

Wir haben damit den folgenden Korrespondenzsatz, Teil 1, bewiesen:

Satz 7 *(Korrespondenzsatz, Teil 1) Sei k ein algebraisch abgeschlossener Körper,*
$\mathcal{V}$ die Menge der Teilmengen des $\mathbf{A}^n$,
$\mathcal{I}$ die Menge der Ideale $I \subset R$,
$V : \mathcal{I} \longrightarrow \mathcal{V}$ der Funktor, der einem Ideal J die zugehörige Nullstellenmenge $V(J)$ zuordnet und
$I : \mathcal{V} \longrightarrow \mathcal{I}$ der Funktor, der einer Teilmenge W des $\mathbf{A}^n$ das Ideal $I(W)$ der auf dieser Teilmenge verschwindenden polynomialen Funktionen zuordnet.

V und I sind zueinander inverse, inklusionsumkehrende Korrespondenzen zwischen den affinen Teilmengen des $\mathbf{A}^n$ und den Radikalidealen in R, d.h.

1. *die Bilder unter V sind genau die affinen Teilmengen des $\mathbf{A}^n$,*
2. *die Bilder unter I sind genau die Radikalideale in R,*
3. *für jede Teilmenge $W \in \mathbf{A}^n$ gilt $V(I(W)) = \overline{W}$,*
4. *für jedes Ideal $J \subset R$ gilt $I(V(J)) = rad(J)$,*
5. *$I_1 \subseteq I_2 \Rightarrow V(I_1) \supseteq V(I_2)$,*
6. *$V_1 \subseteq V_2 \Rightarrow I(V_1) \supseteq I(V_2)$.*

BEWEIS : Es sind nur noch die Aussagen 5. und 6. zu zeigen. Deren Gültigkeit ist aber offensichtlich. $\square$

Eine besondere Rolle unter den affinen Varietäten spielen solche, die nur aus einer "Komponente" bestehen. Verschwinden weder f noch g auf V, ist aber $f \cdot g \in I(V)$, so kann man V als (echte) Vereinigung der beiden affinen Teilvarietäten darstellen, auf denen noch f bzw. g verschwindet. Läßt sich umgekehrt V in zwei solche Teile zerlegen, dann gibt es Polynome f, g mit dieser Eigenschaft. Dies führt zur

DEFINITION: Ein Ideal $I \subset R$ heißt *Primideal*, wenn

$$f, g \in R, fg \in I \quad \Rightarrow \quad f \in I \text{ oder } g \in I$$

gilt.

V ist also genau dann unzerlegbar (*irreduzibel*), wenn $I(V)$ ein Primideal ist. Dies kann man auch durch eine Eigenschaft des Koordinatenrings charakterisieren:

AUFGABE: Zeigen Sie, daß I genau dann ein Primideal ist, wenn der Faktorring $S = R/I$ nullteilerfrei ist.

Insbesondere sind die durch reguläre Parametrisierung entstandenen Varietäten irreduzibel, denn $R/I(V) = im(\phi^*) \subset k[t_1, \ldots, t_d]$ ist als Unterring eines (nullteilerfreien) Polynomrings selbst auch nullteilerfrei.

3.3 Idealoperationen

Als nächstes wollen wir untersuchen, welchen Idealoperationen die Bildung (endlicher) Vereinigungen und Durchschnitte von affinen Varietäten unter obiger Korrespondenz entsprechen.

Ein Gleichungssystem, dessen Nullstellenmenge genau dem Durchschnitt zweier vorgegebener Nullstellenmengen entspricht, bekommt man als Vereinigung der beiden Teilsysteme. Auf diese Weise entsteht jedoch kein Ideal. Dafür muß noch die Bildung entsprechender kreuzweiser polynomialer Linerakombinationen zugelsaaen werden.

Beispiel: $I_1 = I(x_1+x_2, x_2x_3, x_3^2 - x_4x_5)$, $I_2 = I(x_1+x_2, x_2x_4, x_4^2 - x_5^2)$
DEFINITION: Als Summe der Ideale $I, J \subset R$ bezeichnet man die Menge

$$I + J := \{i + j \ : \ i \in I, \ j \in J\}$$

Beispiele:
$I_1 + I_2 = I(x_1+x_2, x_2x_3, x_2x_4, x_3^2 - x_4x_5, x_4^2 - x_5^2)$
$J_1 = I(x_1+x_2, x_1x_2)$, $J_2 = I(x_1 - x_2, x_1x_2)$, $J_1 + J_2 = I(x_1, x_2)$.

Satz 8 *Die Summe von zwei Idealen ist wieder ein Ideal. Sind B_i Basen der Ideale $I_i, i = 1, 2$, so ist $B = B_1 \bigcup B_2$ eine Basis von $I_1 + I_2$. Selbst für Minimalbasen muß das aber keine Minimalbasis des Summenideals sein.*

Betrachten wir die analoge Konstruktion für das Produkt statt der Summe.
DEFINITION: Als Produkt der Ideale $I, J \subset R$ bezeichnet man die Menge

$$I \cdot J := \{\sum_k i_k \cdot j_k \ : \ i_k \in I, \ j_k \in J\}$$

Beispiele:
$I_1 \cdot I_2 = I(die\ neun\ paarweisen\ Produkte)$
$J_1 \cdot J_2 = I(x_1^2 - x_2^2, x_2^3, x_1x_2^2)$

Satz 9 *Das Produkt von zwei Idealen ist wieder ein Ideal. Sind B_i Basen der Ideale $I_i, i = 1, 2$, so ist $B = \{f \cdot g \ : \ f \in B_1, \ g \in B_2\}$ eine Basis von $I_1 \cdot I_2$. Selbst für Minimalbasen muß das aber keine Minimalbasis des Produktideals sein.*

Jeder Punkt aus der Vereinigung der Nullstellenmengen der beiden Teilsysteme ist offensichtlich eine gemeinsame Nullstelle der Idealprodukts. In den Beispielen haben wir allerdings gesehen, daß die Multiplizität oftmals nicht die richtige ist.

AUFGABE: Zeigen Sie, daß Summe oder Produkt von Radikalidealen nicht unbedingt wieder Radikalideale sein müssen.

Es zeigt sich, daß noch eine dritte Operation zwischen Idealen von Interesse ist:

Satz 10 *Der Durchschnitt zweier Ideale ist wieder ein Ideal und es gilt stets $I \cdot J \subseteq I \cap J$.*

Die Basis eines Idealdurchschnitts kann jedoch im Allgemeinen nicht nach einer einfachen Vorschrift aus den Basen der Teilideale berechnet werden.

Beispiel: Polynomring in einer Variablen ist Hauptidealring. $R = k[x], I = I(f), J = I(g)$ Dann ist $I \cap J = I(lcm(f, g))$.

Beispiel: Potenzprodukte im Durchschnitt von zwei Potenzproduktidealen

$$I(x^3, xy^2) \cap I(x^2y, y^3) \supseteq I(x^3y, x^2y^2, xy^3)$$

Beispiel $J_1 \cap J_2 = I(x_1^2, x_1x_2, x_2^2)$
Beispiel (o. Bew.) $I_1 \cap I_2 = I(x_2x_3x_5^2, x_2x_4x_5, x_2x_3x_4, x_1 + x_2, (x_4^2 - x_5^2)(x_3^2 - x_4x_5))$
Dafür verhält sich der Durchschnitt zweier Ideale besser bzgl. der Korrespondenz zwischen Idealen und Varietäten.

AUFGABE: Zeigen Sie, daß der Durchschnitt zweier Radikalideale wieder ein Radikalideal ist.

Die eingeführten Idealoperationen hängen eng mit der Bildung von Vereinigungen und Durchschnitten affiner Varietäten zusammen:

Satz 11 *(Korrespondenzsatz, Teil 2) Unter den Voraussetzungen des Korrespondenzsatzes, Teil 1, gilt für Ideale $I_1, I_2 \subset R$ weiterhin*

7. $V(I_1 + I_2) = V(I_1) \bigcap V(I_2)$ *und*

8. $V(I_1 \cdot I_2) = V(I_1 \bigcap I_2) = V(I_1) \bigcup V(I_2)$.

Beweis : Wegen $I_1 \cdot I_2 \subseteq I_1 \cap I_2 \subseteq I_1, I_2$ gilt

$$V(I_1 \cdot I_2) \supseteq V(I_1 \cap I_2) \supseteq V(I_1) \cup V(I_2).$$

Es bleibt also nur $V(I_1 \cdot I_2) \subseteq V(I_1) \cup V(I_2)$ zu zeigen. $a \in V(I_1 \cdot I_2)$ heißt aber insbesondere $f(a)g(a) = 0$ für alle $f \in I_1, g \in I_2$. Ist $a \notin V(I_1)$, so gibt es ein $f \in I_1$ mit $f(a) \neq 0$, was $g(a) = 0$ für alle $g \in I_2$ nach sich zieht. Also wäre dann $a \in V(I_2)$. $\square$

Aufgabe: Seien $a, b, c \subset R$ Ideale. Beweisen Sie die folgenden Relationen

1. $(a + b)c = ac + bc$
2. $(a \cap b) + c \subseteq (a + c) \cap (b + c)$
3. $(a \cap b) \cdot c \supseteq (a \cdot c) \cap (b \cdot c)$
4. $a \cdot b + c \supseteq (a + c) \cdot (b + c)$
5. $a \cap (b + c) \supseteq (a \cap b) + (a \cap c)$
6. $a \cap (b \cdot c) \supseteq (a \cap b) \cdot (a \cap c)$

Zeigen Sie in den Fällen 2.–6., daß im Allgemeinen keine Gleichheit besteht, aber jeweils die Radikale beider Seiten übereinstimmen.

Ein Spezialfall der Relation 5. ist das *Modularitätsgesetz*

$$c \subseteq a \Rightarrow a \cap (b + c) = (a \cap b) + c.$$

Beweisen Sie diese Aussage.

4 Gröbnerbasen

4.1 Monomideale und Dickson-Lemma

Eine wichtige Klasse von Beispielen, die sich einfach beschreiben lassen, aber trotzdem bereits recht komplizierte Ideale enthalten, sind die von Potenzprodukten (PP) erzeugten Ideale. Diese wollen wir in diesem Abschnitt näher untersuchen. Da wir bereits gesehen hatten, daß der Begriff der Idealbasis nicht eindeutig ist und insbesondere etwa bereits für das von einfachsten Potenzprodukten erzeugte Ideal $I(x_1, x_2, x_3)$ selbst *Minimal*basen aus mehrgliedrigen Polynomen angegeben werden können, benötigen wir zunächst eine invariante Definition.

Vereinbarung: Multiexponentenschreibweise $\mathbf{x}^\alpha = x_1^{a_1} \ldots x_n^{a_n}$

Definition: Ein Ideal $I \subset R$ heißt *Monomideal*, wenn

$$f = \sum c_\alpha \mathbf{x}^\alpha \in I, c_\alpha \neq 0 \quad \Rightarrow \mathbf{x}^\alpha \in I$$

gilt.

Offensichtlich besitzt jedes Ideal mit dieser Eigenschaft eine Basis aus PP. Umgekehrt ist auch ein von PP erzeugtes Ideal ein Monomideal: Wird I von den PP $\mathbf{x}^{\beta_i}$ erzeugt, so kann jedes Element $f \in I$ als

$$f = \sum_i \left(\sum_\alpha c_{\alpha,i} \mathbf{x}^\alpha \right) \mathbf{x}^{\beta_i} = \sum c_{\alpha,i} \mathbf{x}^{\alpha+\beta_i}$$

dargestellt werden. Ein PP $\mathbf{x}^\gamma$ tritt in f also nur dann auf, wenn $\gamma = \alpha + \beta_i$ für wenigstens ein Basiselement gilt.

Monomideale sind also genau die Ideale, für die man eine Basis, und damit auch eine Minimalbasis, aus PP angeben kann. Die PP ihrerseits bilden eine eigene mathematische Struktur, das Monoid $T := T(X) = T(x_1, \ldots, x_n)$ der Terme in $x_1, \ldots, x_n$, das wir bzgl. der Abbildung

$$log : T(X) \longrightarrow \mathbf{N}^n \qquad via \qquad \mathbf{x}^\alpha \mapsto \alpha$$

mit dem (additiven) Monoid $\mathbf{N}^n$ identifizieren können.

Die Menge aller in einem Monomidealen enthaltenen PP bildet ein *Monoidideal*, d.h. eine Teilmenge $\Sigma \subset T$ mit

$$\Sigma \cdot T := \{\mathbf{x}^\alpha \cdot \mathbf{x}^\beta \,:\, \mathbf{x}^\alpha \in \Sigma, \mathbf{x}^\beta \in T\} \subset \Sigma.$$

Beispiel: $I = I(x^4y^2, x^3y^4, x^2y^5)$. Graphische Darstellung im $\mathbf{N}^2$.

DEFINITION: Eine Teilmenge $\Sigma_0 = \{\mathbf{x}^{a_1}, \ldots, \mathbf{x}^{a_m}\}$ eines Monoidideals Σ bezeichnet man als *Basis*, wenn $\Sigma_0 \cdot T = \Sigma$ gilt und als *Minimalbasis*, wenn Σ_0 minimal bzgl. Inklusion mit dieser Eigenschaft ist.

Wir schreiben in diesem Fall $\Sigma = \langle \mathbf{x}^{a_1}, \ldots, \mathbf{x}^{a_m}\rangle$.

Satz 12 *Jedes Monoidideal $\Sigma \subset T$ hat eine eindeutig bestimmte Minimalbasis. Diese besteht genau aus den $\mathbf{x}^\alpha \in \Sigma$, die minimal in Σ bzgl. der Teilbarkeitsrelation der PP sind, d.h. für die*

$$\mathbf{x}^\beta \in \Sigma, x^\beta \,|\, \mathbf{x}^\alpha \;\Rightarrow\; x^\beta = \mathbf{x}^\alpha$$

gilt. Für diese Menge schreiben wir $Gen(\Sigma)$.

Wir haben somit eine eindeutige Korrespondenz zwischen den Monomidealen $I \in \mathcal{MI}(R)$ und den Monoididealen $\Sigma \in \mathcal{O}(T)$, gegeben durch die Zuordnungen

$$\begin{array}{lll} \Sigma : \mathcal{MI}(R) \longrightarrow \mathcal{O}(T) & via & I \mapsto \Sigma(I) := \{\mathbf{x}^\alpha \,:\, \mathbf{x}^\alpha \in I\} \\ I : \mathcal{O}(T) \longrightarrow \mathcal{MI}(R) & via & \Sigma \mapsto I(\Sigma) := \{\sum c_\alpha \mathbf{x}^\alpha \,:\, \mathbf{x}^\alpha \in \Sigma\}. \end{array}$$

Satz 13 *Die Abbildungen $\Sigma : \mathcal{MI}(R) \longrightarrow \mathcal{O}(T)$ und $I : \mathcal{O}(T) \longrightarrow \mathcal{MI}(R)$ zwischen der Menge $\mathcal{MI}(R)$ der Monomideale in R und der Menge $\mathcal{O}(T)$ der Monoidideale in T sind zueinander invers, wobei für Monomideale $I_1, I_2 \subset R$*

1. $I_1 + I_2 = I(\Sigma(I_1) \cup \Sigma(I_2))$
2. $I_1 \cdot I_2 = I(\Sigma(I_1) \cdot \Sigma(I_2))$
3. $I_1 \cap I_2 = I(\Sigma(I_1) \cap \Sigma(I_2))$

gilt.

Mit diesem Satz kann also das Rechnen mit Monomidealen auf das Rechnen mit Monoididealen zurückgeführt werden, wobei die Rechnungen für Monoidideale oft rein kombinatorischen Charakter haben.

AUFGABE: Beweisen Sie diesen Satz und leiten Sie daraus her, daß für Monomideale $a, b, c \subset R$

$$\begin{array}{ll} 2. & (a \cap b) + c = (a + c) \cap (b + c) \\ 5. & a \cap (b + c) = (a \cap b) + (a \cap c) \end{array}$$

gilt, es jedoch für die anderen Relationen aus der letzten Aufgabe aus Kap. 3 auch unter den Monomidealen Gegenbeispiele gibt.

Diese strengeren Eigenschaften für Monomideale sind Ausdruck der Tatsache, daß die Menge aller Ideale bzgl. $+, *$ einen modularen Verband, die Menge der Monomideale jedoch einen distributiven Verband bilden.

Man kann auf diese Weise insbesondere für Monomideale den Idealdurchschnitt leicht ausrechnen.

Beispiel: $I(x^3y, y^4) \cap I(x^5, x^2y^2) = I(x^2y^4, x^3y^2, x^5y)$

AUFGABE: Finden Sie eine allgemeine Formel für die Erzeugenden des Durchschnitts zweier Monomideale.

Eine wichtige Eigenschaft von Monomidealen ist die Tatsache, daß jedes von ihnen eine endliche Basis hat. Die entsprechende Aussage für Monoidideale ist Gegenstand des folgenden Satzes.

Satz 14 *(Dickson-Lemma) Jedes Monoidideal $\Sigma \subset T := T(x_1, \ldots, x_n)$ hat eine endliche Basis.*

BEWEIS : Wir führen den Beweis mit Induktion nach n. Für $n = 1$ ist die Aussage offensichtlich. Für den Induktionsschritt sei $T' = T(x_1, \ldots, x_{n-1})$. Nach Induktionsvoraussetzung wissen wir, daß jedes Monoidideal in T' eine endliche Basis besitzt und wir wollen dies für Monoidideale $I \subset T$ zeigen. Mit $\mathbf{x} = (x_1, \ldots, x_{n-1})$ und $y = x_n$ kann jedes PP $M \in T$ (eindeutig) als $M = \mathbf{x}^\alpha y^m$ dargestellt werden.

Betrachten wir zunächst

$$J := \{\mathbf{x}^\alpha \ : \ \exists\, m > 0\ \mathbf{x}^\alpha y^m \in I\}.$$

Diese Menge ist ein Monoidideal (warum?) in T', hat also eine endliche Basis

$$B := \{\mathbf{x}^{\alpha(i)} \ : \ i = 1, \ldots, k\},$$

wobei für geeignete m_i stets $\mathbf{x}^{\alpha(i)} y^{m_i} \in I$ gilt.

Sei $m := max(m_i \ : \ i = 1, \ldots, k)$ und für $l \geq 0$

$$J_l := \{\mathbf{x}^\alpha \ : \ \mathbf{x}^\alpha y^l \in I\}.$$

Diese Mengen, die man als die "Scheiben" von I in y-Richtung verstehen kann, sind ebenfalls Monoidideale in T' (warum?) und es gilt

$$l_1 < l_2 \Rightarrow J_{l_1} \subset J_{l_2}$$

sowie $J_l = J$ für $l \geq m$. Jedes der kleineren ($l \leq m$) Monoidideale hat wiederum eine endliche Basis

$$B_l := \{\mathbf{x}^{\alpha_l(i)} \ : \ i = 1, \ldots, k_l\},$$

so daß nach Definition

$$C_l := \{\mathbf{x}^{\alpha_l(i)} y^l \ : \ i = 1, \ldots, k_l\} \subset I$$

gilt.

Wir behaupten nun, daß die Vereinigung $C := \bigcup_{l \leq m} C_l \subset I$ eine endliche Basis von I ist. Nach der Basiseigenschaft ist dazu nur zu zeigen, daß jedes Monom $M \in I$ durch eines aus C teilbar ist. Das ist nach Konstruktion aber offensichtlich. $\square$

Zum besseren Verständnis des Beweises wollen wir ihn noch einmal an einem Beispiel nachvollziehen:

$I = (x^4y^2, x^3y^4, x^2y^5)$ Dann ist $J = (x^2), m = 5$ und für die einzelnen "Scheiben" erhalten wir $J_0 = J_1 = \{0\}, J_2 = J_3 = (x^4), J_4 = (x^3)$. Nach dem Beweisschema erhalten wir

$$C = \{x^4y^2, x^4y^3, x^3y^4, x^2y^5\}$$

4.2 Normalformen – Teil 1

Zur Bestimmung der Lösungsmenge eines linearen Gleichungssystems können wir den Gauß-Algorithmus oder die Eliminationsmethode verwenden. Beide sind Modifikationen ein und desselben Normalformverfahrens. Betrachten wir etwa das Gleichungssystem

$$\begin{aligned} x + y + 2z &= 1 \\ x + 2y + z &= 2 \\ 2x + y + z &= 5. \end{aligned}$$

Im ersten Verfahren verwenden wir die erste Gleichung, um durch geeignete Zeilentransformationen in den verbleibenden Gleichungen die Koeffizienten vor der Variablen x zu Null umzuformen. Im zweiten Verfahren stellen wir die erste Gleichung nach x um und substituieren in die verbleibenden Gleichungen. Beide Verfahren können wir als *Termersetzungsverfahren* auffassen, das die Regel $x \mapsto 1 - y - 2z$ anwendet. Im Ergebnis erhalten wir die Gleichungen

$$\begin{aligned} y - z &= 1 \\ -y - 3z &= 3, \end{aligned}$$

aus denen wir die nächste (einfachere) Regel $y \mapsto 1 + z$ extrahieren, die uns schließlich

$$4z = -4$$

liefert. Rücksubstitution liefert uns schließlich als Lösungsmenge $L = \{(3, 0, -1)\}$. Die Termination des Verfahrens beruht darauf, daß in jedem Eliminationsschritt eine der (endlich vielen) Variablen verschwindet.

Ähnlich können wir den Euklidschen Algorithmus für Polynome in $k[x]$ interpretieren. Dessen zentrale Konstituente, die Division mit Rest, können wir ebenfalls als Termersetzungsverfahren verstehen. Für $f := x^5 - x + 1$ und $g := x^3 + x^2 - 1$ sind dabei die folgenden Schritte auszuführen:

$$\begin{aligned} f_1 &= f - x^2 g = -x^4 + x^2 - x + 1 \\ f_2 &= f_1 + x\, g = x^3 + x^2 - 2x + 1 \\ r &= f_2 - g = -2x + 2 \end{aligned}$$

Jeder einzelne Schritt kann dabei als algebraische Ersetzungsregel $x^3 \mapsto -x^2 + 1$ aufgefaßt werden, wobei "algebraisch" bedeutet, daß nicht nur die Regel selbst, sondern auch alle daraus ableitbaren monomialen Vielfachen anzuwenden sind. Nach endlich vielen Schritten ist keine dieser Regeln mehr anwendbar; der Rest $r = f mod g$ ist berechnet. Der Euklidsche Algorithmus wird nun mit g und r fortgesetzt, d.h. mit einer "einfacheren" Ersetzungsregel $x \mapsto 1$. Im Gegensatz zum Gauß-Algorithmus gibt es (potentiell) unendlich viele x-Potenzen als linke Seiten unserer Ersetzungsregeln. Die Termination des Verfahrens beruht hier darauf, daß stets nur höhere durch niedrigere Potenzen ersetzt werden.

Ähnliche Überlegungen haben wir auch schon beim Rechnen mit multivariaten Polynomen angetroffen. Um sich etwa zu überzeugen, daß die Polynome $f := -xz + y^2$ und $g := xy - z$ im Ideal $I := I(y - x^2, z - x^3)$ enthalten sind, haben wir aus der Idealbasis die beiden Kongruenzrelationen

$$\begin{aligned} y &\equiv x^2 \ (mod\ I) \\ z &\equiv x^3 \ (mod\ I) \end{aligned}$$

abgeleitet, diese als Ersetzungsregeln aufgefaßt und damit

$$\begin{aligned} f &\equiv -x^4 + (x^2)^2 = 0 \ (mod\ I) \\ g &\equiv x \cdot x^2 - x^3 = 0 \ (mod\ I) \end{aligned}$$

hergeleitet und so $f, g \in I$ geschlossen. Hieraus ein algorithmisches Verfahren zu machen, das immer terminiert, bedarf es einiger Überlegung. Wir wollen uns dabei an der oben entwickelten Vorstellung orientieren, daß wir "größere" durch "kleinere" Terme ersetzen und ein solches Ersetzungsverfahren sich aus noch zu präzisierenden Gründen nach endlich vielen Schritten erschöpft hat.

Eine präzise mathematische Notation für diese Vorstellung ist die einer Ordnungsrelation auf der Menge $T(X)$ der Terme in $k[X] = k[x_1, \ldots, x_n]$. Diese wollen wir zunächst studieren.

4.3 Ordnungen auf $T(X)$

Eine (reflexive, totale) *Ordnungsrelation* $\leq$ auf $T := T(X)$ ist eine reflexive, antisymmetrische und transitive Relation, in der je zwei Elemente miteinander vergleichbar sind. Mit jeder solchen Relation kann man eine irreflexive Ordnungsrelation $<$ verbinden

$$m < n \;:\Leftrightarrow\; m \leq n \textit{ und } m \neq n.$$

In manchen Zusammenhängen spielen auch nicht antisymmetrische Relationen eine Rolle. Derartige (reflexive und transitive) Relationen nennt man *Quasiordnungen.* Elemente $a, b \in T$ mit $a \leq b$ und $b \leq a$ heißen in diesem Fall *zueinander assoziiert.* Wir schreiben dafür $a \equiv b$. Diese Relation ist eine Äquivalenzrelation. Zu einer solchen Quasiordnung kann man ebenfalls eine irreflexive, allerdings nur teilweise Ordnungsrelation definieren durch

$$m < n \;:\Leftrightarrow\; m \leq n \textit{ und } m \not\equiv n.$$

Da wir die zu definierenden Ordnungsrelationen für algebraische Ersetzungsregeln verwenden wollen, müssen sie außerdem kompatibel mit der algebraischen Struktur auf T sein. Wir nennen deshalb eine Ordnungsrelation $\leq$ *monoton*, wenn

$$\forall\, m, n, t \in T \;\; m \leq n \;\Rightarrow\; m \cdot t \leq n \cdot t$$

gilt.

Schließlich soll das Ersetzungsverfahren "große" Terme gegen "kleine" Terme endlich sein. Wir nennen deshalb eine Ordnungsrelation *noethersch*, wenn jede absteigende Kette $m_1 \geq m_2 \geq \ldots$ von Elementen aus T nur endlich viele verschiedene Elemente enthält. Diese Eigenschaft kann man auf unterschiedliche Weise charakterisieren:

Satz 15 *Folgende Bedingungen für eine monotone Ordnungsrelation $\leq$ auf T sind äquivalent:*

1. *$\leq$ ist noethersch.*
2. *$\leq$ ist eine* Wohlordnung, *d.h. jede nichtleere Teilmenge $M \subset T$ besitzt ein kleinstes Element.*
3. *Es gilt $1 \leq m$ für alle $m \in T$.*

Beweis : Wir zeigen die Äquivalenz folgender Aussagen:

1. Es existiert eine unendliche echt absteigende Kette $K = (m_1 > m_2 > \ldots)$.
2. Es existiert eine nichtleere Teilmenge $M \subset T$ ohne kleinstes Element.
3. Es gibt ein $m \in T$ mit $1 > m$.

$1 \Leftrightarrow 2$: M ist sicher unendlich. Wählen wir m_1 beliebig, so folgt aus der Tatsache, daß dies nicht das kleinste Element ist, die Existenz von $m_2 \in M$ mit $m_1 > m_2$. Ausgehend von m_2 kann man analog m_3, m_4 etc. und so $K \subset M$ konstruieren. Umgekehrt nehme man $M = K$.

$1 \Leftrightarrow 3$: Aus der Monotonie und $1 > m$ folgt $m > m^2, m^2 > m^3$ etc., also $1 > m > m^2 > m^3 > \ldots$. Ist umgekehrt K eine unendliche echt absteigende Kette, so wissen wir nach dem Dickson-Lemma, daß das von K erzeugte Monoidideal nur endlich viele Erzeugende $(m_{i_1}, \ldots, m_{i_k})$ mit $i_1 < \ldots < i_k$ hat. Insbesondere gibt es für jedes $j > i_k$ einen Index $i \in \{i_1, \ldots, i_k\}$, so daß m_i ein Teiler von m_j ist, also $m_j = m \cdot m_i$ mit $1 \neq m \in T$ gilt. Es gilt also $m_j = m \cdot m_i < m_i$ und damit $m < 1$, weil $m > 1$ der Monotonie von $\leq$ widersprechen würde. $\square$

Definition: Eine monotone, noethersche Ordnungsrelation $\leq$ auf $T(X)$ nennen wir eine *Termordnung.*

Beispiele für Ordnungsrelationen auf $T(X)$:

Lexikographisch (Lex):

$$x^a <_{lex} x^b \;\Leftrightarrow\; \exists i\, \forall j < i\, (a_j = b_j)\ und\ a_i < b_i$$

Beispiel: Alle Terme in $T(x, y, z)$ vom Grad ≤ 2:

$$x^2 > xy > xz > x > y^2 > yz > y > z^2 > z > 1$$

Diese Ordnung ist eine Termordnung.

Gradweise lexikographisch (DegLex):

$$x^a <_{deglex} x^b \;\Leftrightarrow\; \begin{cases} \sum a_i < \sum b_i \text{ oder} \\ \sum a_i = \sum b_i \text{ und } x^a <_{lex} x^b \end{cases}$$

Beispiel: Alle Terme in $T(x, y, z)$ vom Grad ≤ 2:

$$x^2 > xy > xz > y^2 > yz > z^2 > x > y > z > 1$$

Diese Ordnung ist eine Termordnung.

Revers lexikographisch (RevLex):

$$x^a <_{lex} x^b \;\Leftrightarrow\; \exists i\, \forall j > i\, (a_j = b_j)\ und\ a_i > b_i$$

Beispiel: Alle Terme in $T(x, y, z)$ vom Grad ≤ 2:

$$1 > x > x^2 > y > xy > y^2 > z > xz > yz > z^2$$

Nach dem oben bewiesenen Kriterium ist diese Ordnung auf $T(X)$ allerdings nicht noethersch und damit keine Termordnung.

Gradweise revers lexikographisch (DegRevLex):

$$x^a <_{degrevlex} x^b \;\Leftrightarrow\; \begin{cases} \sum a_i < \sum b_i \text{ oder} \\ \sum a_i = \sum b_i \text{ und } x^a <_{revlex} x^b \end{cases}$$

Beispiel: Alle Terme in $T(x, y, z)$ vom Grad ≤ 2:

$$x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1$$

Diese Ordnung ist eine Termordnung.

Verallgemeinerung: Gewichtete Termordnungen
$0 \neq w \in (\mathbf{R}^n)$ sei ein Vektor mit nichtnegativen reellen Einträgen. Für x^α bezeichnen wir $w \cdot \alpha$ (das übliche Skalarprodukt) als *Gewicht* von x^α. In Verallgemeinerung der gradweisen Termordnungen können wir dann eine *gewichtete Termordnung* mit dem Gewichtsvektor w wie folgt definieren:

$$x^a <_w x^b \;\Leftrightarrow\; \begin{cases} w \cdot a < w \cdot b \text{ oder} \\ w \cdot a = w \cdot b \text{ und } x^a < x^b \end{cases}$$

Dabei ist $<$ eine beliebige andere monotone Ordnungsrelation auf $T(X)$. Haben die Variablen alle positive Gewichte wie im Beispiel der Standardgraduierung, so ist 1 das einzige Monom mit dem Gewicht 0 und wir erhalten in jedem Fall eine Termordnung.

Im allgemeinen Fall kann $<$ selbst wieder eine gewichtete Termordnung mit einem anderen Gewichtsvektor w_1 sein. Eine auf diese Weise durch eine endliche Folge von Gewichtsvektoren gegebene Termordnung bezeichnet man auch als *Matrix-Termordnung*.

AUFGABE: (Charakterisierung von Termordnungen als Matrix-Termordnungen) Zeigen Sie die Gültigkeit der folgenden Aussagen:

1. Jede Termordnung $<$ erfüllt die *Kürzungsregel*

$$\forall m,n,t \in T \; m \cdot t < n \cdot t \;\Rightarrow\; m < n.$$

2. Jede Termordnung $\leq$ wird durch ihren *Positivkegel*

$$C_+(<) := \{\alpha - \beta \in \mathbf{Z}^n \,:\, x^\alpha \geq x^\beta\}$$

eindeutig charakterisiert.

3. Der Abschluß des Positivkegels $C_+(<)$ im $\mathbf{R}^n$ ist ein Halbraum, dessen Stützhyperebene durch einen Gewichtsvektor mit nichtnegativen Einträgen beschrieben wird.

4. Jede Termordnung auf $T(x_1,\ldots,x_n)$ kann man als Matrix-Termordnung mit maximal n Gewichtsvektoren realisieren.

4.4 Normalformen – Teil 2

Kehren wir nun zu unseren Termersetzungsverfahren im Polynomring $R = k[\mathbf{x}]$ zurück. Sei $T(\mathbf{x})$ mit einer Termordnung $<$ versehen, die wir für die folgenden Betrachtungen fixieren wollen, und $0 \neq f(x) = \sum_{i=0}^N c_i x^{\alpha_i} \in R$ ein Polynom, so daß in der fixierten Termordnung $x^{\alpha_i} > x^{\alpha_j}$ für $i < j$ gilt. Bezeichne weiter $T(f) := \{x^{\alpha_i},\, i = 0,\ldots,N\}$ die Menge der in der Darstellung von f auftretenden Terme. Dann können wir die folgenden Begriffe definieren:

- den Leitterm $lt(f) := x^{\alpha_0}$,
- den Leitkoeffizienten $lc(f) := c_0$,
- das Leitmonom $lm(f) := lc(f) \cdot lt(f)$,
- das Reduktum $red(f) := f - lm(f)$.

Beispiel: $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$

$$\begin{array}{llll} <_{lex} & : & lm(f) = -5x^3 & red(f) = 7x^2z^2 + 4xy^2z + 4z^2 \\ <_{deglex} & : & lm(f) = 7x^2z^2 & red(f) = 4xy^2z - 5x^3 + 4z^2 \\ <_{degrevlex} & : & lm(f) = 4xy^2z & red(f) = 7x^2z^2 - 5x^3 + 4z^2 \end{array}$$

Aufgabe:

1. Untersuchen Sie, ob es eine Termordnung gibt, in der $lm(f) = 4z^2$ gilt.

2. Bestimmen Sie den Leitterm der folgenden Polynome bzgl. der drei wichtigsten Termordnungen und ordnen Sie das Reduktum

$$\begin{aligned} f_1 &= 7x^2y^4z - 2xy^6 + x^2y^2 \\ f_2 &= 2x + 3y + z + x^2 - z^2 + x^3 \\ f_3 &= 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4 \end{aligned}$$

Es sei an dieser Stelle bemerkt, daß andere Autoren, insbesondere [1], die Begriffe "Term" und "Monom" in umgekehrter Bedeutung verwenden. Wir folgen hier der Begriffsbildung von [3], die sich in letzter Zeit beginnt durchzusetzen. In dem Zusammenhang sei vermerkt, daß ein Monomideal von Monomen, ein Monoidideal dagegen von Termen erzeugt wird und die in obigem Satz bewiesene 1-1-Korrespondenz zwischen beiden Begriffen ganz wesentlich die Eigenschaft verwendet, daß k ein Körper ist.

Mit der Fixierung eines "größten" Monoms können wir jedes Polynom f als algebraische Ersetzungsregel auffassen, die monomiale Vielfache des Leitterms $lt(f)$ durch geeignete monomiale Vielfache des Reduktums $red(f)$ ersetzt. Genauer gesagt lautet die abzuleitende Ersetzungsregel

$$lt(f) \mapsto -lc(f)^{-1}\, red(f).$$

Entsprechend erhalten wir für eine endliche Menge $B = \{f_1, \ldots, f_m\}$ von Polynomen ein System von Ersetzungsregeln.

Beispiel: $B = \{x^2 + xy + y^2, xz + yz, y^3 - z^3\}$ liefert (bzgl. $<_{lex}$) das Ersetzungssystem

$$x^2 \mapsto -xy - y^2,\ xz \mapsto -yz,\ y^3 \mapsto z^3.$$

Wenden wir die Regeln in der genannten Reihenfolge auf das Polynom $g = x^2y^2 + x^2z^2 + y^2z^2$ an, so erhalten wir nacheinander

$$\begin{aligned} g &\mapsto x^2z^2 - xy^3 - y^4 + y^2z^2 \mapsto -xy^3 - xyz^2 - y^4 \mapsto -xyz^2 - xz^3 - y^4 \\ &\mapsto -xz^3 - y^4 + y^2z^2 \mapsto -y^4 + y^2z^2 + yz^3 \mapsto y^2z^2 \end{aligned}$$

Das aus B abgeleitete Ersetzungssystem erlaubt es also, alle Terme aus dem Monoidideal

$$\Sigma(B) := \{x^\alpha\ :\ \exists\, f \in B : lt(f) \,|\, x^\alpha\}$$

durch eine Linearkombination "kleinerer" Terme zu ersetzen. Diese Terme bezeichnen wir deshalb auch als *Nichtstandardterme*, die verbleibenden Terme $T(X) \setminus \Sigma(B)$ dagegen als die *Standardterme* bzgl. B.

Beispiel, daß es ganz wesentlich auf die Reihenfolge beim Berechnen der Normalform ankommt: $B_1 := \{ux - y^2, uy - z^2, uz - x^2\}$ und Reduktion des Monoms u^2xyz. Zwei verschiedene Pfade liefern die Normalformen y^2z^3 oder x^3z^2.

Begriff der *Reduktionspfades*.

Betrachten wir $u^2xyz - y^2z^3$: Ein Reduktionspfad liefert 0, ein anderer $x^3z^2 - y^2z^3$.

Der folgende Algorithmus **NormalForm** erlaubt es, in einem Polynom $f \in R$ so lange Ersetzungen vorzunehmen, bis der Leitterm des entstehenden Polynoms ein Standardterm bzgl. B ist:

`NF(f:Polynom,B:Basis):Polynom`

Input: `Polynom` $f \in R$, `endliche Menge` $B \subset R$
Output: `Polynom` $f' \in R$ `mit` $f \equiv f' \pmod{I(B)}$ `und` $f' = 0$ `oder` $lt(f') \notin \Sigma(B)$

`while` $(f \neq 0)$ `and` $(M := \{b \in B\ :\ lt(b) \,|\, lt(f)\} \neq \emptyset)$ `do`
  `choose` $b \in M$
  $f := f - \frac{lm(f)}{lm(b)} b$
`return` f

Dieser Algorithmus terminiert offensichtlich, weil die Folge der Leitmonome der in den einzelnen Schritten entstehenden Zwischenergebnisse eine streng monoton fallende Folge von Monomen darstellt, die nach der Definition einer Termordnung endlich sein muß.

Betrachten wir das folgende Gleichungssystem

$$B_2 := \{f_1 = x^2 + y + z - 3,\ f_2 = x + y^2 + z - 3,\ f_3 = x + y + z^2 - 3\},$$

so erkennen wir, daß die daraus ableitbaren Ersetzungsregeln nicht unabhängig voneinander sind. Das liegt daran, daß das Basiselement f_1 dafür verwendet werden kann, die anderen beiden Elemente zu reduzieren. Wir erhalten entsprechend

$$\begin{aligned} f_4 &:= NF(f_1, \{f_3\}) = y^2 + 2yz^2 - 5y + z^4 - 6z^2 + z + 6 \\ f_5 &:= NF(f_2, \{f_3\}) = y^2 - y - z^2 + z \end{aligned}$$

Ähnlich wie im Erweiterten Euklidschen Algorithmus kann man den Normalforn-Algorithmus so modifizieren, daß sogar eine Darstellung von $f' - f \in I(B)$ als polynomiale Kombination der Basiselemente zurückgegeben wird.

```
NFwithRelations(f:Polynom,B:Basis):(Polynom,Vektor)
```

Input: Polynom $f \in R$, endliche Menge $B = \{b_1, \ldots, b_m\} \subset R$
Output: Polynom $f' \in R$ mit $f' = 0$ oder $lt(f') \notin \Sigma(B)$
und Vektor $v = (v_1, \ldots, v_m)$ mit $f = \sum_i v_i\, b_i + f'$.

for $i = 1, \ldots, m$ do $v_i := 0$
while $(f \neq 0)$ and $(M := \{b \in B \ : \ lt(b) \,|\, lt(f)\} \neq \emptyset)$ do
  choose $b_i \in M$
  $f := f - \frac{lm(f)}{lm(b_i)} b_i$
  $v_i := v_i + \frac{lm(f)}{lm(b_i)}$
return (f, v)

In obigem Beispiel etwa erhalten wir bei der Berechnung von $f_4 := NF(f_1, \{f_3\})$ nacheinander

$$\begin{aligned} f_1 &\mapsto f_1 - x\, f_3 = -xy - xz^2 + 3x + y + z - 3 =: f_{11} \\ &\mapsto f_{11} + y\, f_3 = -xz^2 + 3x + y^2 + yz^2 - 2y + z - 3 =: f_{12} \\ &\mapsto f_{12} + z^2\, f_3 = 3x + y^2 + 2yz^2 - 2y + z^4 - 3z^2 + z - 3 =: f_{13} \\ &\mapsto f_{13} - 3\, f_3 = f_4, \end{aligned}$$

also $f_1 = (x - y - z^2 + 3) f_3 + f_4$ und analog $f_2 = 1 \cdot f_3 + f_5$. Mithin erzeugen B_2 und $B_{21} := \{f_3, f_4, f_5\}$ dasselbe Ideal. Analog kann man f_5 verwenden, um aus f_4 ein Polynom mit interessanterem Leitterm zu konstruieren:

$$f_6 := NF(f_4, \{f_5\}) = 2yz^2 - 4y + z^4 - 5z^2 + 6,$$

so daß wir insgesamt aus unserem Polynomsystem B_2 durch *Interreduktion* ein System $B_{22} := \{f_3, f_5, f_6\}$ hergeleitet haben, das dasselbe Ideal wie B_2 erzeugt, in dem aber alle $f \in B_{22}$ in Normalform bzgl. $B_{22} \setminus \{f\}$ sind.

Der bisher betrachtete Normalform-Algorithmus beendet seine Arbeit, wenn ein Standardterm als Leitterm erzeugt worden ist. Dabei kann es sein, daß immer noch Nichtstandardterme im Reduktum des erzeugten Polynoms auftreten, die ebenfalls noch reduziert werden können.

Beispiel: Betrachte $B := \{x^2 - x, y^2 - y\}$ und $f = x^2 + y^2$.

Einen entsprechenden Algorithmus, der **NF** noch rekursiv auf das Reduktum anwendet, bezeichnet man als **totalen Normalform-Algorithmus**.

```
TNF(f:Polynom,B:Basis):Polynom
```

Input: Polynom $f \in R$, endliche Menge $B \subset R$
Output: Polynom $f' \in R$ mit $f \equiv f' \ (mod\ I(B))$ und
$f' = 0$ oder $T(f') \cap \Sigma(B) = \emptyset$

f:=NF(f,B)
if $f = 0$ then return f else return $lm(f) + TNF(red(f), B)$

Für diesen Algorithmus kann man ebenfalls wieder eine Variante angeben, die $f - f'$ als polynomiale Kombination der Basiselemente $b \in B$ darstellt. Fassen wir die letzte Bemerkung in dem folgenden Satz zusammen.

Satz 16 *Sei $R = k[x_1, \ldots, x_n]$ ein Polynomring über einerm Körper k, $<$ eine Termordnung auf $T(x_1, \ldots, x_n)$ und $B = \{b_1, \ldots, b_m\} \subset R$ eine endliche Menge von Polynomen. Dann gibt es einen Algorithmus, der für jedes Polynom $f \in R$ nach endlich vielen Schritten eine Darstellung*

$$f = v_1\, b_1 + \ldots + v_m\, b_m + r$$

mit $v_1, \ldots, v_m, r \in R$ produziert, in der $r = 0$ gilt oder r eine Linearkombination von Standardtermen bzgl. B ist und $lt(f) \geq lt(v_i b_i)$ für alle i gilt.

Aufgabe: Interreduktion einer Basis kann man auch bzgl. der totalen Normalform ausführen. Überführen Sie die Idealbasis

$$B_3 := \{w + x + y + z, wx + xy + yz + zw, wxy + xyz + yzw + zwx, wxyz - 1\}$$

(bzgl. der lexikographischen Ordnung $w > x > y > z$) in eine entsprechende reduzierte Form.

Es gilt also

Satz 17 *Seien R, f und B wie in obigem Satz. Ist $NF(f, B) = 0$, so gilt $f \in I(B)$, aber nicht notwendigerweise umgekehrt.*

Letzteres folgt daraus, daß wir im Beispiel 1) gesehen hatten, daß $NF(f, B) = 0$ von der gewählten Reduktionsstrategie abhängen kann. Allerdings kann $f \in I$, aber $NF(f, B) \neq 0$ unabhängig von der Reduktionsstrategie sein. In obigem Beispiel B_1 gilt

$$u^2xyz - y^2z^3 \equiv x^3z^2 - y^2z^3 \equiv 0 \ (mod\ I(B_1)),$$

je nach Wahl der Reduktionsstrategie. Also ist $f = x^3z^2 - y^2z^3 \in I$, aber jeder seiner Terme ein Standardterm.

4.5 Gröbnerbasen und Hilberts Basissatz

In diesem Abschnitt wollen wir eine Bedingung kennenlernen, unter der das im letzten Satz unbefriedigend beantwortete Idealenthaltenseinsproblem algorithmisch vollständig beantwortet werden kann.

Wir fixieren dazu auf unserem Polynomring $R = k[\mathbf{x}]$ eine Termordnung $<$ und betrachten für ein Ideal $I \subset R$ die Menge $\Sigma(I) := \{lt(f) \,|\, 0 \neq f \in I\} \subset T(X)$. Dies ist eine natürliche Verallgemeinerung dieser oben zunächst für Monomideale eingeführten Bezeichnung. Da $I \cdot R \subseteq I$ gilt, fällt sie außerdem mit der oben für beliebige Mengen B von Polynomen gegebenen zusammen. Ist B eine Basis des Ideals I, so gilt sicher $\Sigma(B) \subseteq \Sigma(I)$, es muß aber nicht unbedingt $\Sigma(B) = \Sigma(I)$ gelten.

Beispiel: $I = I(f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x)$. Dann gilt $B = \{f_1, f_2\}, \Sigma(B) = \langle x^3, x^2y \rangle$, aber wegen $x^2 = x\, f_2 - y\, f_1 \in I$ außerdem wenigstens $x^2 \in \Sigma(I)$.

Das zum Monoidideal $\Sigma(I)$ gehörende Monomideal $Lt(I) \subset R$ wird als linearer Vektorraum also von den Leittermen der Elemente $0 \neq f \in I$ aufgespannt und heißt deshalb das *Leittermideal* von I (bzgl. der festgewählten Termordnung $<$).

Jedes Monoidideal $\Sigma(I)$ hat nach dem Dicksonlemma eine endliche Basis $\{m_1, \ldots, m_r\} \subset T(X)$, zu deren Elementen es also nach Definition Polynome $g_i \in I$ mit $lt(g_i) = m_i$ gibt. Nach Definition ist für eine solche Menge $\Sigma(G) = \Sigma(I)$.

Auf dieser Basis kann man einen der zentralen Sätze der kommutativen Algebra auf sehr einfache Weise konstruktiv beweisen:

Satz 18 *(Hilberts Basissatz) Jedes Ideal $I \subset R$ besitzt eine endliche Basis.*

Beweis : Wir zeigen, daß die gerade gefundene endliche Menge $G = \{g_1, \ldots, g_r\}$ eine solche Basis ist. Wegen $G \subset I$ bleibt dafür nur zu zeigen, daß jedes Element $f \in I$ auch tatsächlich als polynomiale Kombination dieser Polynome darstellbar ist. Berechnen wir die Normalform mit Relationen von f bzgl. G, erhalten wir eine Darstellung

$$f = p_1 g_1 + \ldots + p_r g_r + q$$

mit einem Polynom q, das entweder Null ist oder einen Leitterm $lt(q) \notin \Sigma(G) = \Sigma(I)$ hat. Da letzteres wegen $q \in I$ nicht möglich ist, folgt $f \in I(G)$. □

Dies gibt Anlaß zu folgender

Definition: Eine endliche Menge $G = \{g_1, \ldots, g_r\} \subset I$ heißt *Gröbner-* oder *Standard-Basis*, wenn $\Sigma(G) = \Sigma(I)$ gilt.

Eine Gröbnerbasis eines Ideals I ist also eine solche Menge von Polynomen, daß sich für jedes andere Polynom $f \in I$ ein Basiselement $g \in G$ findet, für welches $lt(g)|lt(f)$ gilt. Wie wir im Beweis des Hilbertschen Basissatzes gesehen haben, ist eine solche Gröbnerbasis zugleich eine Idealbasis im früher definierten Sinne und jedes Ideal besitzt eine endliche solche Gröbnerbasis. Wir sagen deshalb auch ohne Bezug auf ein Ideal, daß G eine Gröbnerbasis ist, wenn G dies bzgl. des Ideals $I = I(G)$ ist.

Da es sich beim Dickson-Lemma, auf dem der obige Beweis beruht, um eine reine Existenzaussage handelt, die uns kein konstruktives Verfahren zum Auffinden einer solchen Gröbnerbasis in die Hand gibt, bleibt die Möglichkeit des praktischen Umgangs mit diesem Begriff zunächst im Dunkeln. Bevor wir dieses aufhellen, wollen wir aber zunächst die Nützlichkeit des eingeführten Begriffs auch für andere konstruktive Fragestellungen zusammentragen.

4.6 Eigenschaften von Gröbnerbasen

Sei auf unserem Polynomring $R = k[\mathbf{x}]$ wiederum eine Termordnung $<$ fixiert.

Gröbnerbasen erlauben eine eindeutige Antwort auf das Idealenthaltenseinsproblem:

Satz 19 *Sei $G = \{g_1, \ldots, g_r\}$ eine Gröbnerbasis des Ideals I. Dann gilt*

$$f \in I \;\Leftrightarrow\; NF(f, G) = 0.$$

Beweis : Wir hatten bereits gesehen, daß $NF(f,G) = 0 \;\Rightarrow f \in I$ für jede Idealbasis von I gilt, so daß die umgekehrte Richtung zu zeigen bleibt. Nehmen wir also an, es gäbe ein $f \in I$ mit $NF(f,G) = r \neq 0$. Dann ist einerseits $lt(r) \notin \Sigma(G) = \Sigma(I)$, andererseits $f \equiv r \ (mod\ I)$, d.h. $r \in I$, ein Widerspruch. □

Korollar 1 *Für eine Gröbnerbasis G eines Ideals I und ein Polynom $f \in R$ ist $TNF(f,G)$ unabhängig vom gewählten Reduktionspfad.*

Beweis : Sind r_1 und r_2 zwei totale Normalformen, die unterschiedlichen Reduktionspfaden entsprechen, so gilt wegen $f \equiv TNF(f,G) \ (mod\ I(G))$ auch $r := r_1 - r_2 \in I$. Da aber beide Normalformen Linearkombinationen aus Standardtermen bzgl. $\Sigma(G) = \Sigma(I)$ sind, so auch r. Also muß $r = 0$ sein, da sonst $lt(r) \in \Sigma(I)$ wäre. □

Bemerkung: Wir hatten oben gesehen, daß wir im Ergebnis des Normalformalgorithmus sogar eine Darstellung

$$f = \sum_{g_i \in G} h_i g_i \quad \text{mit} \quad \forall\, i \ (lt(f) \geq lt(h_i g_i))$$

erhalten.

Wir wollen nun gezielt Beispiele von Polynomen konstruieren, die im von der Basis B erzeugten Ideal liegen, aber deren Leitterm nicht in $\Sigma(B)$ enthalten ist. Einen Weg zur Konstruktion solcher

Polynome hatten wir im Beispiel $B_1 := \{f_1 = ux - y^2, f_2 = uy - z^2, f_3 = uz - x^2\}$ gesehen: u^2xyz läßt sich auf zwei verschiedenen Pfaden jeweils zur Normalform y^2z^3 oder x^3z^2 reduzieren. Demzufolge ist $f = x^3z^2 - y^2z^3 \in I$, aber $lt(f) = x^3z^2 \notin \Sigma(B_1)$. Kleinste Gegenbeispiele können wir auf folgende Weise konstruieren:

$$\begin{aligned} s_{12} &= y \cdot f_1 - x \cdot f_2 = (uxy - y^3) - (uxy - xz^2) = xz^2 - y^3 \\ s_{13} &= z \cdot f_1 - x \cdot f_3 = (uxz - y^2z) - (uxz - x^3) = x^3 - y^2z \\ s_{23} &= z \cdot f_2 - y \cdot f_3 = (uyz - z^3) - (uyz - x^2y) = x^2y - z^3 \end{aligned}$$

In jedem der drei Beispiele kann man dem Ergebnis nicht mehr ansehen, wie es als Linearkombination der Basiselemente entstanden ist, da sich diese Kombination nur durch Hinzufügen zweier gleicher Terme mit entgegengesetztem Vorzeichen ergibt, die in der fixierten Termordnung *größer* als die verbleibenden Terme sind. Ein solches Element hat nur dann eine verschwindende Normalform, wenn es einen zweiten Weg zu seiner Darstellung als Element von I gibt, die *ohne Termüberschreitung* auskommt.

Das allgemeine Schema der Konstruktion solcher Elemente suggeriert die folgende

DEFINITION: Seien $f, g \in R$ zwei nichttriviale Polynome und $m = lcm(lt(f), lt(g))$ das kleinste gemeinsame Vielfache der Leitterme der beiden Polynome. Dann bezeichnen wir das Polynom

$$S(f,g) := \frac{m}{lm(f)}f - \frac{m}{lm(g)}g = \frac{m}{lm(f)}red(f) - \frac{m}{lm(g)}red(g),$$

das die kleinste monomiale Kombination aus f und g ist, in der sich die beiden Kopfterme gegenseitig wegheben, als das *S-Polynom* von f und g.

Ein solches S-Polynom, falls es nicht verschwindet, besitzt einen Leitterm, der echt kleiner als der erwartete Leitterm m ist. Auf diese Weise entstehen Polynome, deren Leitterm möglicherweise nicht in $\Sigma(B)$ enthalten ist. Durch Hinzunahme dieser Polynome in die Basis vergrößern wir also $\Sigma(B)$. Fügen wir etwa im Beispiel B_1 zur Basis die drei neu erzeugten Polynome hinzu, erhalten wir eine neue Basis $B_{11} = \{f_1, f_2, f_3, f_4 := s_{12}, f_5 := s_{13}, f_6 := s_{23}\}$ mit $\Sigma(B_{11}) = \langle ux, uy, uz, xz^2, x^3, x^2y\rangle$. Bzgl. dieser neuen Basis ist offensichtlich $NF(S(f_i, f_j), B_{11}) = 0$ für $(i,j) \in \{(1,2),(1,3),(2,3)\}$. Andererseits können zwischen den neuen und alten Elementen neue S-Polynome konstruiert werden:

$$s_{14} = z^2f_1 - uf_4 = (uxz^2 - y^2z^2) - (uxz^2 - uy^3) = uy^3 - y^2z^2$$

Im Gegensatz zu obigen Polynomen ist dieses Polynom nicht bereits in Normalform bzgl. B_{11}. Es gilt

$$s_{14} \mapsto_{f_2} 0$$

also $NF(s_{14}, B_{11}) = 0$. Damit entsteht aus diesem Polynom kein neues Polynom aus I mit bis dahin unbekanntem Leitterm. Dasselbe gilt für die S-Polynome $s_{ij}, i \in \{1,2,3\}, j \in \{4,5,6\}$. Die restlichen S-Polynome liefern

$$\begin{aligned} s_{45} &= -x^2y^3 + y^2z^3 \mapsto_{f_6} 0 \\ s_{46} &= -xy^4 + z^5 =: f_7 \\ s_{56} &= xz^3 - y^3z \mapsto_{f_4} 0 \end{aligned}$$

Wir erhalten also ein weiteres Polynom $f_7 \in I$ mit bis dahin unbekanntem Leitterm xy^4 und schließlich wegen

$$s_{47} = y^4f_4 + z^2f_7 = -y^7 + z^7 =: f_8$$

ein letztes solches Polynom. Die Normalform aller weiteren S-Polynome verschwindet, so daß wir auf einfachem Wege keine neuen Polynome $f \in I$ mit $lt(f) \notin \Sigma(G)$ für $G = \{f_1, \ldots, f_8\}$ konstruieren können. Weiter unten werden wir sehen, daß G in der Tat bereits eine Gröbnerbasis ist.

Betrachten wir unser zweites Beispiel: Für $I(B_2)$ hatten wir bereits eine neue Idealbasis

$$B_{22} := \{f_3, f_5, f_6\} = \{x + y + z^2 - 3, y^2 - y - z^2 + z, 2yz^2 - 4y + z^4 - 5z^2 + 6\}$$

konstruiert. Hier liefert nur $NF(S(f_5, f_6), B_{22})$ ein neues nichttriviales Polynom f_7:

$$\begin{aligned} S(f_5, f_6) &= z^2 f_5 - 1/2\, y\, f_6 = 2\, y^2 - 1/2\, y\, z^4 + 3/2\, y\, z^2 - 3\, y - z^4 + z^3 \\ &\mapsto_{f_5} -1/2\, y\, z^4 + 3/2\, y\, z^2 - y - z^4 + z^3 + 2\, z^2 - 2\, z \\ &\mapsto_{z^2 f_6} 1/2\, y\, z^2 - y + 1/4\, z^6 - 9/4\, z^4 + z^3 + 7/2\, z^2 - 2\, z \\ &\mapsto_{f_6} f_7 := 1/4(z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6) \end{aligned}$$

Alle S-Polynome, die man seinerseits mit f_7 bilden kann, reduzieren zu Null. Auch hier gilt, wie wir nun zeigen wollen, daß $G := \{f_3, f_5, f_6, f_7\}$ bereits eine Gröbnerbasis ist.

Satz 20 *(Charakterisierungssatz für Gröbnerbasen) Die folgenden Bedingungen an eine Basis G eines Ideals $I \subset R$ sind äquivalent:*

1. *G ist eine Gröbnerbasis von I, d.h. $\Sigma(I) = \Sigma(G)$.*
2. *Für jedes Element $f \in I$ und jede Reduktionsstrategie gilt $NF(f, G) = 0$.*
3. *Für jedes Element $f \in I$ gibt es eine Reduktionsstrategie mit $NF(f, G) = 0$.*
4. *Für jedes Paar $g_1, g_2 \in G$ und jede Reduktionsstrategie gilt $NF(S(g_1, g_2), G) = 0$.*
5. *Für jedes Paar $g_1, g_2 \in G$ gibt es eine Reduktionsstrategie mit $NF(S(g_1, g_2), G) = 0$.*
6. *Jedes Element $f \in I$ hat eine Darstellung*
$$f = \sum_{g_i \in G} h_i g_i \quad mit \quad \forall\, i\ (lt(f) \geq lt(h_i g_i)).$$
7. *Die Standardterme $St(G) := T(X) \setminus \Sigma(G)$ sind linear unabhängig $(mod\ I)$.*
8. *Die Standardterme $St(G)$ bilden eine Vektorraumbasis des Faktorrings R/I, d.h. jedes Element $f \in R$ besitzt eine eindeutige Darstellung*
$$f \equiv \sum_{m \in St(G)} c_m m\ (mod\ I)$$
mit $c_m \in k$.

Beweis : Wir hatten bereits gesehen, daß 1. $\Rightarrow$ 2. gilt. Da S-Polynome spezielle Elemente aus I sind, sind die Implikationen 2. $\Rightarrow$ 3. $\Rightarrow$ 5. und 2. $\Rightarrow$ 4. $\Rightarrow$ 5. trivial, so daß nur noch 5. $\Rightarrow$ 6. und 6. $\Rightarrow$ 1. zu zeigen bleibt.

5. $\Rightarrow$ 6.: Sei $f = \sum h_i g_i \in I$, aber $lt(f) < m := max(lt(h_i g_i))$. Im folgenden bezeichnet $f_1, f_2, \ldots$ Kombinationen $\sum h_i' g_i \in I$ mit $max(lt(h_i' g_i)) < m$. Zunächst ist

$$f = \sum\nolimits^* h_i g_i + f_1 = \sum\nolimits^* (lm(h_i) + red(h_i)) g_i + f_1 = \sum\nolimits^* lm(h_i) g_i + f_2,$$

wobei sich die Summation $\sum^*$ nur über diejenigen Indizes erstreckt, für die $lt(h_i g_i) = m$ gilt. Insbesondere ist $lt(g_i) \,|\, m$ für $i \in *$. Betrachten wir den Ausdruck unter dem Summenzeichen. Für jeden einzelnen Summanden gilt nach Konstruktion $lt(h_i) lt(g_i) = m > lt(f)$, also ist $\sum^* lc(h_i) lc(g_i) = 0$. Sei oBdA ein Summand g_1 in dieser Summe vertreten. Dann gilt $lt(g_1) \,|\, m$ und

$$\sum\nolimits^* lc(h_i) lc(g_i) \tfrac{m}{lm(g_1)} g_1 = 0.$$

m ist ein gemeinsames Vielfaches aller $lt(g_i)$, $i \in *$, also insbesondere ein Vielfaches von $m_i := lcm(lt(g_1), lt(g_i))$. Deshalb ist

$$\sum\nolimits^* lm(h_i) g_i = \sum\nolimits^* lc(h_i) lc(g_i) \tfrac{m}{lm(g_i)} g_i = \sum\nolimits^* lc(h_i) lc(g_i) \tfrac{m}{m_i} S(g_i, g_1),$$

wenn man die oben hergeleitete Null-Summe hinzufügt. Da aber $lt(S(g_i, g_1)) < m_i$ und außerdem $NF(S(g_i, g_1), G) = 0$ gilt, erhalten wir auf diese Weise eine Darstellung von f als Kombination $\sum h'_i g_i$ mit $max(lt(h'_i g_i)) < m$. Noethersche Induktion beweist dann die Aussage 6.

6. $\Rightarrow$ 1.: Aus der Existenz der genannten Darstellung für $f \in I$ folgt $lt(f) = max_i(lt(h_i)lt(g_i))$, also $lt(f) \in \Sigma(G)$.

1. $\Rightarrow$ 7.: Wäre

$$f = \sum_{m \in St(G)} c_m m \equiv 0 \ (mod\ I)$$

eine nichttriviale Linearkombination von Standardmonomen aus I, dann wäre wegen $f \in I$ auch $lt(f) \in \Sigma(I) = \Sigma(G)$.

7. $\Rightarrow$ 8.: Jedes Nichtstandardmonom kann mit Hilfe von $TNF(\_, G)$ als Linearkombination von Standardmonomen dargestellt werden. Also bilden diese auch ein Erzeugendensystem.

8. $\Rightarrow$ 1.: Wäre $m \in \Sigma(I) \setminus \Sigma(G)$ und $f \in I$ mit $lt(f) = m$, so wäre $f' := TNF(f, G) \in I$ eine nichttriviale Linearkombination von Termen aus $St(G)$.

□

Der Charakterisierungssatz zeigt, daß die oben berechnete Menge $G = \{f_1, \ldots, f_8\}$ eine Gröbnerbasis von $I = I(B_1)$ ist, weil sie die Eigenschaft 5. erfüllt.

Wir wollen diesen Abschnitt mit einem Kriterium beschließen, das es erlaubt, manche S-Polynome nicht zu untersuchen.

Satz 21 *(Hauptsyzygienkriterium) Sind $f, g \in R$ nichttriviale Polynome mit teilerfremden Leittermen, so gilt $NF(S(f,g), \{f,g\}) = 0$.*

Beweis : Aus der Teilerfremdheit folgt $m = lcm(lt(f), lt(g)) = lt(f) \cdot lt(g)$ und somit

$$S(f,g) = \frac{m}{lm(f)} red(f) - \frac{m}{lm(g)} red(g) = \frac{1}{lc(f)\, lc(g)} \left(lm(g)\, red(f) - lm(f)\, red(g)\right)$$

Führen wir nun die Substitutionen $lm(f) \mapsto -red(f)$ und $lm(g) \mapsto -red(g)$ aus, so erhalten wir 0.
□

Betrachten wir noch einmal die Rechnungen zum Beispiel

$$B_{22} = \{f_3, f_5, f_6\} = \{x + y + z^2 - 3, y^2 - y - z^2 + z, 2yz^2 - 4y + z^4 - 5z^2 + 6\}.$$

Da die anderen Leittermpaare zueinander teilerfremd sind brauchen wir nach dem Hauptsyzygienkriterium nur $S(f_5, f_6)$ zu untersuchen, was in der Tat ein neues Polynom

$$f_7 := z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6$$

liefert. Von diesem brauchen wir nur $S(f_6, f_7)$ zu untersuchen, was zu 0 reduziert.

4.7 Der Buchberger-Algorithmus

Ähnlich wie oben können wir auch im allgemeinen Fall versuchen, aus einer gegebenen Idealbasis B eine Gröbnerbasis zu konstruieren. Wir versuchen, nacheinander alle S-Polynome $S(f_i, f_j)$, $f_i, f_j \in B$ vermöge B zu reduzieren. Ist $f := NF(S(f_i, f_j), B) \neq 0$, so wissen wir zumindest, daß $lt(f) \in \Sigma(I) \setminus \Sigma(B)$, d.h. $f \in I$ ein Element aus dem Ideal ist, dessen Leitterm man aus den bisher bekannten Basiselementen nicht herleiten kann. Fügen wir andererseits dieses Polynom zur Menge B hinzu, kann $S(f_i, f_j)$ nunmehr trivialerweise zu Null reduziert werden. Durch die Hinzunahme des neuen Basiselements vergrößert sich andererseits die Anzahl der möglichen S-Polynome, so daß die Termination dieses Vorgehens eines Beweises bedarf. Im Beispiel der Menge B_1 jedenfalls terminierte dieses Verfahren.

Die formale Spezifikation des entsprechenden Algorithmus, den man zu Ehren seines Erfinders den **Buchergeralgorithmus** nennt, sieht wie folgt aus:

```
GBasis(B:Basis):Basis
```

Input: `Endliche Menge` $B = \{f_1, \ldots, f_m\} \subset R$.
Output: `Gröbnerbasis` G `des Ideals` $I = I(B)$.

```
G:=B;
P := {(f_i, f_j) | 1 ≤ i < j ≤ m};
While P ≠ ∅ do
    Choose p ∈ P; P := P \ {p};
    f := NF(S(p), G)
    if f ≠ 0 then
        P := P ∪ {(g, f) | g ∈ G};
        G := G ∪ {f};
return G;
```

Satz 22 *Der Algorithmus terminiert nach endlich vielen Schritten.*

Beweis : In jedem Schritt mit $f \neq 0$ wird $\Sigma(G)$ echt vergrößert. Nach dem Dicksonlemma sind aber nur endlich viele solche Schritte möglich. □

Beispiel: Das erste Beispiel in der Vorlesung:

$$B_4 := \{17x^2 + 22xy + 13y^2 - 1,\ 8x^2 + 28xy + 37y^2 - 1\}$$

Betrachten wir die lexikographische Termordnung mit $y > x$. Interreduktion liefert als Augangspunkt für den Gröbneralgorithmus

$$G = \{f_1 = 150\, y\, x + 175\, x^2 - 8,\ f_2 = 75\, y^2 - 50\, x^2 + 1\}$$

Nichttrival reduzierende S-Polynome erhalten wir nacheinander die folgenden:

$$\begin{aligned} f_3 &= NF(S(f_1, f_2), G) = 48\, y + 625\, x^3 - 44\, x \\ f_4 &= NF(S(f_1, f_3), G) = 15625\, x^4 - 2500\, x^2 + 64, \end{aligned}$$

so daß insgesamt $G = \{f_1, f_2, f_3, f_4\}$ eine Gröbnerbasis ist. Allerdings sind $lt(f_1)$ und $lt(f_2)$ für ein minimales Erzeugendensystem von $\Sigma(G)$ und somit für eine Gröbnerbasis nach Definition derselben nicht notwendig. Damit ist in diesem Fall bereits $G' := \{f_3, f_4\}$ eine Gröbnerbasis in Übereinstimmung mit unseren Rechnungen im Abschnitt 1.

Satz 23 *Ist G eine Gröbnerbasis des Ideals I und $G' \subset G$ eine Teilmenge, so daß $Gen(\Sigma(G)) = \{lt(g),\ g \in G'\}$ gilt, so ist auch G' eine Gröbnerbasis von I. Eine solche Gröbnerbasis nennt man* minimal.

Der Beweis dieses Satzes ergibt sich sofort aus der Definition einer Gröbnerbasis. Auf Grund der Eindeutigkeit der Minimalbasis des Monoidideals $\Sigma(I)$ ist die Menge $\{lt(g),\ g \in G'\}$ eindeutig bestimmt. Die Menge

$$\{lt(g) - NF(lt(g), G'),\ g \in G'\} \subset I$$

bezeichnet man schließlich als *minimale reduzierte Gröbnerbasis*. Jedes dieser Polynome ist die Differenz zwischen einem minimalen Nichtstandardterm und dessen eindeutiger Darstellung ($mod\ I$) als Linearkombination von (in der Termordnung kleineren) Standardtermen. Offensichtlich ist eine solche minimale reduzierte Gröbnerbasis eindeutig bestimmt.

4.8 Gröbnerbasisberechnungen in den wichtigsten Computeralgebrasystemen

Alle großen Computeralgebrasysteme allgemeiner Ausrichtung (CAS) erlauben die Berechnung von Gröbnerbasen wenigstens für die lexikographische Termordnung. Die folgenden Ausführungen sollen einen kurzen Überblick über die Möglichkeiten der einzelnen Systeme geben, die in der Vorlesung bisher eingeführten Algorithmen auszuführen. Einen etwas detaillierteren Überblick findet man im Anhang C von [1] sowie in einführender oder Referenzliteratur zu den einzelnen Systemen. Wir setzen bei unserem Ausführungen voraus, daß der Leser mit der Verwendung der genannten CAS im Allgemeinen vertraut ist; dies betrifft insbesondere Grundkenntnisse zur Bedienung und Syntax der einzelnen Systeme.

Maple

Maple verfügt über ein eigenes Gröbnerpaket, das nicht automatisch geladen wird, sondern explizit über den Aufruf

```
> with(grobner);
```

eingebunden werden muß. Als Ergebnis erhält man eine Liste

[finduni, finite, gbasis, gsolve, leadmon, normalf, solvable, spoly]

von Funktionen, die danach zur Verfügung stehen. Hier seien nur zwei von ihnen erläutert.

Die Berechnung einer Gröbnerbasis:

```
gbasis(F, X)
gbasis(F, X, termorder)
gbasis(F, X, termorder, 'Y')

PARAMETERS:
   F         - set or list of polynomials
   X         - set or list of indeterminates (not including parameters)
   termorder - term ordering:
                    'plex' (pure lexicographic) or
                    'tdeg' (total degree is default)
```

Das Manual gibt dazu folgende Beschreibung:

> The command `gbasis(F,X,termorder)` computes the reduced, minimal Grobner basis of the polynomials F with respect to the indeterminates X and the given term ordering. If X is a set, reordering will occur and a fourth argument MUST appear.

Die Berechnung einer Normalform:

```
normalf(poly, F, X)
normalf(poly, F, X, termorder)

PARAMETERS:
   F         - list of polynomials
               (normally, a Grobner basis)
   X         - list of indeterminates
               (not including free parameters)
   poly      - the polynomial to be reduced
   termorder - (optional) term ordering
```

Das Manual gibt dazu folgende Beschreibung:

> The command `normalf(poly,F,X,to)` computes the fully reduced form of poly with respect to the ideal basis F, indeterminates X, and term ordering *to*.

Es folgt eine Beispielrechnung.

```
> with(grobner):

> F := [x^2 - 2*x*z + 5, x*y^2 + y*z^3, 3*y^2 - 8*z^3]:

> vars := [x,y,z]:

> G := gbasis(F,vars);
```

$$[x^2 - 2\,xz + 5, -3\,y^2 + 8\,z^3, 8\,xy^2 + 3\,y^3, 9\,y^4 + 48\,zy^3 + 320\,y^2]$$

Man beachte, daß Maple standardmäßig Gröbnerbasen bzgl. der Ordnung deglex berechnet. Eine Gröbnerbasen bzgl. der rein lexikographischen Ordnung erhält man mit

```
> H := gbasis(F,vars,plex);
```

$$[x^2 - 2\,xz + 5, 640\,z^3x + 9\,z^8 + 120\,z^5 - 96\,z^7, 3\,y^2 - 8\,z^3,$$
$$-40\,z^5 - 3\,z^8 + 32\,z^7 + 80\,yz^3, 1600\,z^3 + 240\,z^6 + 9\,z^9 - 96\,z^8]$$

```
> p := 320*x*y^2 + 9*x*y^4 - 96*z^2*y^4*x + 1600*y^3

>        - 18*y^5*x*z - 592*x*z*y^3 + 45*y^5 + 240*z*y^4:

> normalf(p,G,vars);
```

$$0$$

```
> q:= x^3*y^3*z^3:

> normalf(q,G,vars);
```

$$\frac{7835648\,z^2y^3}{81} - \frac{644560\,zy^3}{27} + \frac{5070080\,y^2z^2}{81} - \frac{10024960\,y^3}{81} + \frac{158556160\,y^2z}{243} - \frac{6481600\,y^2}{81}$$

Mathematica 3.0

Die Möglichkeiten zur Berechnung von Gröbnerbasen sind in der Version 3.0 gegenüber Vorläuferversionen wesentlich flexibler geworden. Während in der Version 2.0 nur die rein lexikographische Termordnung zugänglich war, gibt es nun zwei verschiedene Gröbnerbasisfunktionen:

```
> GroebnerBasis[PolyList, xVars]
```

berechnet die Gröbnerbasis aus der Idealbasis `PolyList` bzgl. der rein lexikographischen Termordnung,

```
> GroebnerBasis[PolyList, xVars, yVars]
```

berechnet die Gröbnerbasis aus der Idealbasis `PolyList` bzgl. einer Ordnung, die `yVars` eliminiert.

Andere Termordnungen kann man über die Option `MonomialOrder` einstellen. Das Handbuch führt dazu aus:

> Valid MonomialOrder options are: Lexicographic (the default), DegreeLexicographic, DegreeReverseLexicographic, EliminationOrder, or a matrix of integers or rationals defining a valid weighting for the variables.

Daneben steht zur Normalformberechnung

```
> PolynomialReduce[Poly,PolyList, xVars]
```

zur Verfügung, das `NFwithRelations` entspricht, d.h. auch noch eine Liste der Kofaktoren für eine Darstellung der (totalen) Normalform von `Poly` bzgl. `PolyList` liefert.

Auch hier wieder eine Beispielrechnung:

```
> F = {x^2 - 2*x*z + 5, x*y^2 + y*z^3, 3*y^2 - 8*z^3};

> vars = {x,y,z};

> G = GroebnerBasis[F,vars]
```

$$\{1600\,z^3 + 240\,z^6 - 96\,z^8 + 9\,z^9, 80\,y\,z^3 - 40\,z^5 + 32\,z^7 - 3\,z^8, 3\,y^2 - 8\,z^3,$$
$$640\,x\,z^3 + 120\,z^5 - 96\,z^7 + 9\,z^8, 5 + x^2 - 2\,x\,z\}$$

Eine Gröbnerbasis unter `deglex` bekommt man aus

```
> H = GroebnerBasis[F,vars,MonomialOrder->DegreeLexicographic]
```

$$\{5 + x^2 - 2\,x\,z, -3\,y^2 + 8\,z^3, 8\,x\,y^2 + 3\,y^3, 320\,y^2 + 9\,y^4 + 48\,y^3\,z\}$$

```
> p = 320*x*y^2 + 9*x*y^4 - 96*z^2*y^4*x + 1600*y^3 - 18*y^5*x*z\

>  - 592*x*z*y^3 + 45*y^5 + 240*z*y^4;
```

Der folgende Aufruf von `PolynomialReduce` liefert nur die Normalform zurück

```
> PolynomialReduce[p,G,vars]//Last
```

$$0$$

```
> q= x^3*y^3*z^3;

> PolynomialReduce[q,G,vars]//Last
```

$$\frac{51276800\,z^3}{243} + \frac{1638400\,z^4}{81} + \frac{51200\,z^5}{27} + \frac{2578240\,z^6}{81} + \frac{81920\,z^7}{27} - \frac{1002496\,z^8}{81}$$

Reduce 3.6

Reduce ist unter den großen Systemen das am schlechtesten dokumentierte. Dafür sind seine Quellen (fast) vollständig zugänglich.

In Reduce stehen zwei größere Pakete zur Berechnung von Gröbnerbasen zur Verfügung, das Paket `groebner` von Melenk, Möller, Neun und das in Leipzig entwickelte Paket `cali`. Beide Pakete sind als Nutzerbeiträge klassifiziert, obwohl das Paket `groebner` auch von Kernfunktionen wie etwa `solve` verwendet wird. Zu jedem der beiden Pakete gibt es im Dokumentationsteil LaTeX-Beschreibungen und ein mehr oder weniger ausführliches Testfile, das die Möglichkeiten der wichtigsten Kommandos erläutert. Wir beschränken uns deshalb hier auch die wichtigsten Funktionalitäten und verweisen für Details auf diese Beschreibungen.

Jedes der beiden Pakete muß vor der Verwendung ähnlich wie in Maple geladen werden. Für das Paket `groebner` stehen folgende wichtige Befehle zur Verfügung.

> `load groebner;`

Laden des Gröbnerpakets

> `groebner(PolyList,VarList);`

Berechnen einer (lex.) Gröbnerbasis

> `preduce(Poly,GBasis);`

Berechnen einer totalen Normalform

Mit dem Befehl

> `torder TO;`

kann explizit von der rein lexikographischen (default) auf andere Termordnungen umgeschaltet werden. Neben `TO=Lex` stehen `TO=GradLex` (unser deglex) und `TO=RevGradLex` (unser degrevlex) zur Auswahl. Man beachte allerdings, daß sich diese Änderung *global* auswirkt, d.h. die gewählte Termordnung bei allen folgenden Rechnungen verwendet wird.

Auch hier folgt eine Beispielrechnung:

```
> load groebner;
> F := {x^2 - 2*x*z + 5, x*y^2 + y*z^3, 3*y^2 - 8*z^3}$
> vars:={x,y,z}$
> G := groebner(F,vars);

  2
{x  - 2*x*z + 5,

        3      8       7        5
 640*x*z  + 9*z  - 96*z  + 120*z ,

    2      3
 3*y  - 8*z ,

      3      8       7       5
 80*y*z  - 3*z  + 32*z  - 40*z ,

    9       8       6        3
 9*z  - 96*z  + 240*z  + 1600*z }
```

```
> p := 320*x*y^2 + 9*x*y^4 - 96*z^2*y^4*x + 1600*y^3 - 18*y^5*x*z
          - 592*x*z*y^3 + 45*y^5 + 240*z*y^4$

> preduce(p,g);
                                        0
```

Und nun dieselben Rechnungen in der Termordnung deglex:

```
> torder gradlex$
> H:=groebner(F,vars);

        4       3          2
h := {9*y  + 48*y *z + 320*y ,

          2      3
      8*x*y  + 3*y ,

        3      2
      8*z  - 3*y ,

       2
      x  - 2*x*z + 5}

> preduce(p,h);
                                        0
```

Das Paket `cali` verfolgt eine detailliertere Strategie bei der Auswahl der entsprechenden Strukturen, in denen die Rechnungen vollzogen werden sollen.

> `load cali;`

Laden des Pakets CALI

> `setring(vars,WeightList,tag);`

Definieren eines Grundrings durch Angabe einer Liste `vars` von Variablen, einer (notfalls leeren) Liste von Gradvektoren (=Listen ganzer Zahlen) `WeightList` für gewichtete Termordnungen und eines Tags `lex` oder `revlex` zur Art der Verfeinerung der gewählten Gradordnung.

> `setideal(Name,PolyList);`

Zuweisung einer Liste `PolyList` von Polynomen an eine Variable `Name`, unter dem bereits berechnete Ergebnisse gespeichert werden. Diese Zuweisung löscht zugleich früher (unter einer anderen Termordnung) berechnete Zwischenergebnisse.

Typische Vereinbarungen sind

```
> setring({x,y,z},{},lex)$
> setideal(f,f)$
```

für die rein lexikographische Termordnung und

```
> setring({x,y,z},{{1,1,1}},lex)$
> setideal(f,f)$
```

für die gradweise lexikographische Termordnung. Der zweite Befehl weist jeweils die unter der Variablen `f` gespeicherte Liste dem Variablennamen `f` zu, d.h. initialisiert den Inhalt der Variablen für die nachfolgende Rechnung neu.

> `gbasis(Name);`

Berechnen einer Gröbnerbasis über dem vereinbarten Grundring.

> `Poly mod GBasis;`

Berechnen einer totalen Normalform

Beispiel:

```
> load cali;
> setring({x,y,z},{},lex)$
> setideal(f,f)$            % F ist die Polynomliste von oben.
> G := gbasis(F);

         2      3
g := {3*y  - 8*z ,

       2
      x  - 2*x*z + 5,

         9       8        6         3
      9*z  - 96*z  + 240*z  + 1600*z ,

            3      8       7       5
      80*y*z  - 3*z  + 32*z  - 40*z ,

             3      8       7        5
      640*x*z  + 9*z  - 96*z  + 120*z }

> p mod g;
                                       0

> setring({x,y,z},{{1,1,1}},lex)$  % deglex. TO.
> setideal(f,f)$            %
> G := gbasis(F);
           2     3
g := {8*x*y  + 3*y ,

         3      2
      8*z  - 3*y ,

         4       3          2
      9*y  + 48*y *z + 320*y ,

       2
      x  - 2*x*z + 5}

> p mod g;
                                       0
```

4.9 Erste Anwendungen von Gröbnerbasen

Wir hatten oben bereits gesehen, daß man mit Gröbnerbasen das Idealenthaltenseinsproblem algorithmisch lösen kann:

Ist G eine Gröbnerbasis des Ideals I, so gilt

$$f \in I \;\Leftrightarrow\; NF(f,G) = 0.$$

Wollen wir etwa prüfen, ob $f = -4x^2y^2z^2 + y^6 + 3z^5$ im von $B = \{xz - y^2, x^3 - z^2\}$ erzeugten Ideal $I = I(B)$ liegt, so berechnen wir zuerst die Gröbnerbasis $G = GBasis(B)$ und prüfen dann, ob $NF(f,G) = 0$ gilt. Bzgl. der lexikographischen Termordnung mit $x > y > z$ erhalten wir etwa

$$G = \{y^6 - z^5,\, xy^4 - z^4,\, x^2y^2 - z^3,\, xz - y^2,\, x^3 - z^2\}$$

und $NF(f,G) = 0$. Verwenden wir dagegen die revers-lexikographische Termordnung, so ist $B = \{-y^2 + xz, x^3 - z^2\}$ bereits selbst Gröbnerbasis und $NF(f,B) = 0$. Wir sehen an diesem Beispiel bereits, daß der Rechenaufwand wesentlich von der gewählten Termordnung abhängen kann.

Auf dieser Basis können wir auch prüfen, ob ein Ideal in einem anderen enthalten ist:

`SubIdeal(A,B:Basis):Boolean`

Input: `Idealbasen` $A, B \subset R$
Output: `true` $\Leftrightarrow$ $I(A) \subseteq I(B)$

```
G:=GBasis(B);
for f in A do
    if NF(f,G) ≠ 0 then return false
return true;
```

Betrachten wir als nächste Fragestellung die Lösbarkeit polynomialer Gleichungssysteme. Nach dem Hilbertschen Nullstellensatz hat ein Gleichungssystem B genau dann eine (über einem algebraisch abgesschlossenen Grundkörper) nichttriviale Nullstellenmenge $V(B) \neq \emptyset$, wenn $I(B)$ nicht das Einsideal $I(1)$ ist. Da sich letzteres aber durch $\Sigma(I(1)) = T(X) = \langle 1 \rangle$ auszeichnet, erhalten wir die folgende Äquivalenz von Aussagen:

Satz 24 *Gegeben sei ein polynomiales Gleichungssystem $B \subset R = k[X]$ mit Koeffizienten aus einem Körper k und ein algebraisch abgeschlossener Erweiterungskörper K von k. Folgende Aussagen sind dann äquivalent:*

1. *$V_K(B) = \emptyset$, d.h. B hat keine gemeinsamen Nullstellen über K.*
2. *$I(B) = I(1)$ ist das Einsideal.*
3. *Jede Gröbnerbasis $G = GBasis(B)$ enthält ein konstantes Polynom.*
4. *$\{1\}$ ist die minimale reduzierte Gröbnerbasis von B.*

Betrachten wir etwa das Gleichungssystem

$$B = \{x^2 + y^2 - 2, x^3 + y^3 - 3, x^4 + y^4 - 4\}.$$

Wir erhalten nacheinander

$$\begin{aligned}
f_4 &= NF\,S(f_1,f_2) = x\,y^2 - 2\,x - y^3 + 3\\
f_5 &= NF\,S(f_1,f_4) = 2\,x\,y - 3\,x + 2\,y^4 - 4\,y^2 - 3\,y + 4\\
f_6 &= NF\,S(f_4,f_5) = x - 4\,y^5 - 6\,y^4 + 4\,y^3 + 18\,y^2 + y\\
f_7 &= NF\,S(f_1,f_6) = 2\,y^6 - 6\,y^4 - 6\,y^3 + 12\,y^2 + 1\\
f_8 &= NF\,S(f_1,f_3) = y^4 - 2\,y^2\\
f_9 &= NF\,S(f_4,f_8) = 2\,y^3 - 3\,y^2\\
f_{10} &= NF\,S(f_8,f_9) = y^2\\
f_{11} &= NF\,S(f_4,f_{10}) = 2y + 3\\
f_{12} &= NF\,S(f_{10},f_{11}) = 1
\end{aligned}$$

Die folgenden Aufgaben sollten Sie mit einem Computeralgebrasystem Ihrer Wahl ausführen, da die damit verbundenen Berechnungen zum Teil beträchtlichen Umfang erreichen können.

AUFGABE: 1.) Untersuchen Sie dasselbe Gleichungssystem bzgl. der gradweise lexikographischen und der gradweise revers lexikographischen Termordnung.
2.) Untersuchen Sie, ob das System

$$\{x^2+y^2+z^2-2, x^3+y^3+z^3-3, x^4+y^4+z^4-4, x^5+y^5+z^5-5\}$$

eine nichttriviale Lösungsmenge besitzt.

Untersuchen wir nun, ob wir für ein Gleichungssystem mit nichttrivialer Lösungsmenge etwas über deren Struktur aussagen können. Wir hatten bereits oben bei der Betrachtung unseres Beispiels B_4 aus der ersten Vorlesung gesehen, daß der Gröbneralgorithmus (bzgl. der lexikographischen Termordnung) das Ausgangssystem

$$B_4 = \{17x^2+22xy+13y^2-1,\, 8x^2+28xy+37y^2-1\}$$

in das System

$$G_4 = \{48\,y + 625\,x^3 - 44\,x,\, 15625\,x^4 - 2500\,x^2 + 64\}$$

überführt. Die zweite Gleichung von G_4 kann zur Ermittlung der 4 Lösungen

$$x \in \{4/(5\sqrt{5}), 2/(5\sqrt{5}), (-2)/(5\sqrt{5}), (-4)/(5\sqrt{5})\}$$

verwendet werden, aus denen sich mit der ersten Gleichung die zugehörigen y-Werte eindeutig ergeben.

Etwas komplizierter sieht die Sache bei dem System

$$B_2 = \{x^2+y+z-3,\, x+y^2+z-3,\, x+y+z^2-3\}$$

aus. Hier hatten wir als Gröbnerbasis

$$G_2 = \{x+y+z^2-3, y^2-y-z^2+z, 2yz^2-4y+z^4-5z^2+6, z^6-10z^4+4z^3+19z^2-8z-6\}$$

gefunden. Aus der letzten Gleichung erhalten wir wiederum

$$z \in \{1+\sqrt{2}, 1-\sqrt{2}, 1, -3, \sqrt{2}, -\sqrt{2}\},$$

jedoch haben wir hier zwei Bestimmungsgleichungen für y. Für die ersten vier Lösungen für z erhalten wir durch Einsetzen in die dritte Gleichung jeweils eine eindeutig bestimmte Lösung für y, die auch Lösung der zweiten Gleichung ist. Für die zwei verbleibenden Werte von z wird dagegen die dritte Gleichung trivial. Die zweite Gleichung liefert dann zu jedem dieser Werte *zwei* verschiedene

Möglichkeiten für den y-Wert. Zu jeder der 8 Möglichkeiten ergibt sich aus der ersten Gleichung eindeutig ein x-Wert, so daß unser Gleichungssystem die folgenden 8 Lösungen besitzt:

$$\begin{aligned}(x,y,z) \in \{&(1,1,1),(-3,-3,-3),\\ &(1-\sqrt{2},\sqrt{2},\sqrt{2}),(1+\sqrt{2},-\sqrt{2},-\sqrt{2}),(\sqrt{2},1-\sqrt{2},\sqrt{2}),\\ &(-\sqrt{2},1+\sqrt{2},-\sqrt{2}),(\sqrt{2},\sqrt{2},1-\sqrt{2}),(-\sqrt{2},-\sqrt{2},1+\sqrt{2})\}\end{aligned}$$

Man beachte, daß die Lösungsmenge die dem Gleichungssystem innewohnende Symmetrie widerspiegelt, indem sie in vier unter zyklischer Vertauschung invariante Teile zerfällt.

Wir sehen an diesem Beispiel, daß bei der Frage nach der Fortsetzbarkeit bzw. Fortsetzung von Teillösungen zu einem Lösungstupel für alle Variablen durchaus nichttriviale Fragestellungen auftreten. Wir wollen deshalb zuerst nach einer Charakterisierung von Gleichungssystemen mit endlich vielen Lösungen fragen.

Satz 25 *Seien $B \subset R = k[X]$ und K wie im vorigen Satz. Folgende Aussagen sind äquivalent:*

1. *$V_K(B)$ ist endlich.*
2. *$I(B)$ enthält für alle $i = 1, \ldots, n$ univariate Polynome $p_i(x_i)$.*
3. *$\Sigma(I)$ enthält für alle $i = 1, \ldots, n$ eine reine Potenz $x_i^{\mu_i}$.*
4. *Jede Gröbnerbasis $G = GBasis(B)$ enthält für alle $i = 1, \ldots, n$ Elemente g_i, deren Leitterm $lt(g_i) = x_i^{\nu_i}$ eine reine x_i-Potenz ist.*
5. *$R/I(B)$ ist ein endlichdimensionaler k-Vektorraum, d.h. es gibt nur endlich viele Standardterme.*

Ein Ideal I mit diesen Eigenschaften nennen wir nulldimensional.

Beweis : Wir zeigen zuerst die Äquivalenz von 1. und 2.:

Ist $V_K(B)$ endlich, so gibt es insbesondere unter den $\mathbf{a} \in V_K(B)$ nur endlich viele verschiedene Werte für die Koordinate x_i, also ein Polynom $\tilde{p}_i(x_i) \in I(V(B)) = rad(I)$. Nach dem Hilbertschen Nullstellensatz liegt aber eine geeignete Potenz $p_i(x_i)$ dann bereits in $I = I(B)$.

Gibt es umgekehrt solche univariaten Polynome, dann impliziert dies, daß es für jede der Koordinaten einer Lösung nur endlich viele Möglichkeiten gibt, also die Lösungsmenge selbst endlich sein muß.

Nun zeigen wir die Äquivalenz der verbleibenden Aussagen.

2. $\Rightarrow$ 3. : $lt(p_i) \in \Sigma(I)$.
3. $\Rightarrow$ 4. : $x_i^{\mu_i} \in \Sigma(I) \Rightarrow \exists\, x_i^{\nu_i} \in Gen(\Sigma(I))$.
4. $\Rightarrow$ 5. : evident.
5. $\Rightarrow$ 2. : $p_i(x_i)$ ist eine lineare Abhängigkeitsrelation zwischen den (unendlich vielen) x_i-Potenzen. □

Bemerkung: In diesem Fall bezeichnet man $dim_k\, R/I(B)$ als den *Grad* $deg\, R/I$ des Gleichungssystems B. Dieser ist als Zahl der Standardterme mit einfachen kombinatorischen Argumenten aus einer Gröbnerbasis zu gewinnen. Der Grad stimmt mit der Anzahl der Nullstellen überein, wenn man jeder von ihnen eine geeignete Vielfachheit zuordnet. Der Grad ist eine Invariante von $I(B)$, hängt also nicht von der verwendeten Termordnung ab. In obigem Beispiel ist B_2 bereits eine Gröbnerbasis bzgl. der gradweise lexikographischen Termordnung, woraus man unmittelbar $Grad = 8$ ableitet.

Der Beweis des Satzes liefert zugleich eine Möglichkeit, wie man aus einer Gröbnerbasis G univariate Polynome $p_i(x_i)$ konstruieren kann: Ist $N = deg\, R/I$ die Zahl der Standardterme, so sind die $N + 1$ Polynome $TNF(x_i^k, G)$, $k = 0, \ldots, N$ modulo I linear abhängig. Eine solche Abhängigkeitsrelation kann man mit Mitteln der linearen Algebra berechnen:

`UPoly(`x_i`:Variable,G:GBasis):Polynom`

Input: `Gröbnerbasis` G `eines nulldimensionalen Ideals, Variable` x_i
Output: `Polynom` $p(x_i) \in I$

`N:=`$|T(X) \setminus \Sigma(G)|$`; (* Anzahl der Standardterme *)`

`Bilde` $F(\mathbf{a}, x_i) := \sum_{k=0}^{N} a_k \, NF(x_i^k, G) = \sum_{m \notin \Sigma(G)} l_m(\mathbf{a}) \, m$

`mit neuen Variablen` $a_0, \ldots, a_N$ `und homogenen Linearformen` $l_m(\mathbf{a})$

`Finde nichttriviale Lösung` A_0 `des homogenen Gleichungssystems`

$\{l_m(\mathbf{a}) = 0, \;\; m \notin \Sigma(G)\}$

`return` $F(A_0, x_i)$

Das hierbei entstehende homogene Gleichungssystem hat $N+1$ Variablen und N Gleichungen, besitzt also immer nichttriviale Lösungen.

Aufgabe: 1.) Finden Sie alle Lösungen von

$$V(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z)$$

und geben Sie eine Interpretation der Lösungsmenge als Schnitt geometrischer Figuren im Raum.
2.) Untersuchen Sie die Menge

$$V(x^2y - z^3, 2xy - 4z - 1, z - y^2, x^3 - 4yz)$$

3.) Untersuchen Sie das Gleichungssystem

$$\{3x^2 + 2yz - 2x\lambda, 2xz - 2y\lambda, 2xy - 2z - 2z\lambda, x^2 + y^2 + z^2 - 1\},$$

das wir im Abschnitt 2 im Ergebnis der Suche nach einem konditionierten Extremum über die Methode der Lagrange-Faktoren erhalten hatten.

5 Gröbnerbasen und Eliminationstheorie

Im Gegensatz zu den einfachen Eigenschaften von Gröbnerbasen, die wir im letzten Abschnitt kennengelernt haben und die für beliebige Termordnungen galten, wollen wir in diesem Abschnitt Eigenschaften von Gröbnerbasen kennenlernen, die nur für lexikographische bzw. allgemeiner Eliminationstermordnungen gelten.

5.1 Eliminationsideale und der Eliminationssatz

Variablenelimination ist eine der grundlegenden Techniken zur Lösung nichtlinearer Gleichungssysteme. Um etwa die Lösungen eines Gleichungssystems $I = I(B)$ in $x > y > z$ zu finden, gehen wir in zwei Schritten vor:

(a) (Eliminationsschritt) Finde eine Gleichung $g(z) \in I$, die nur die Variable z enthält, d.h. eliminiere x und y aus dem System.

(b) (Extensionsschritt) Erweitere die Lösungen der Gleichung $g(z) = 0$ zu Lösungstupeln von I.

Wir hatten bereits gesehen, daß dabei vollkommen neue Polynome ins Spiel kommen können und wollen nun untersuchen, wie sich diese Frage mit Gröbnerbasen bearbeiten läßt.

Sei dazu $R = k[x_1, \ldots, x_n]$ ein Polynomring und $I = I(B)$ ein Ideal. Wir wollen eine allgemeinere Frage studieren und die Variablen $x_1, \ldots, x_r$ eliminieren, d.h. untersuchen, welche der Polynome aus I im Ring $R_r := k[x_{r+1}, \ldots, x_n]$ liegen. Sei dazu noch $T_r = T(x_{r+1}, \ldots, x_n)$ das Termmonoid von R_r.

DEFINITION: Das Ideal $I_r := I \cap R_r$ bezeichnet man als das *r-te Eliminationsideal* von I.

Gröbnerbasen erlauben es, auf einfachem Wege solche Eliminationsideale zu bestimmen:

Satz 26 *(Eliminationssatz) Sei G eine Gröbnerbasis des Ideals I bzgl. der lexikographischen Termordnung. Dann ist*

$$G_r = G \cap R_r = \{g \in G \,|\, lt(g) \in T_r\}$$

eine Gröbnerbasis des r-ten Eliminationsideals von I.

BEWEIS : Auf Grund der Auswahl der Termordnung ist offensichtlich für $0 \neq f \in R$

$$(*) \qquad lt(f) \in R_r \;\Leftrightarrow\; T(f) \subset T_r,$$

d.h. $G \cap R_r = \{g \in G \,|\, lt(g) \in T_r\}$ und somit $\Sigma(G) \cap T_r = \Sigma_{T_r}(G_r)$

Ist $0 \neq f \in I_r$, so gilt $lt(f) \in \Sigma(I) \cap T_r = \Sigma_{T_r}(G_r)$. Folglich ist $\Sigma_{T_r}(G_r) = \Sigma_{T_r}(I_r)$, also G_r eine Gröbnerbasis von I_r im Ring R_r. $\square$

Bemerkung: Im Beweis haben wir für festes r nur von der Eigenschaft $(*)$ Gebrauch gemacht. Demzufolge kann man jede Termordnung $>$ auf $T(X)$ mit der Eigenschaft

$$m \in T(X) \setminus T_r(X),\; n \in T_r(X) \;\Rightarrow m > n$$

mit demselben Erfolg zur Berechnung von I_r verwenden. Jede Termordnung mit dieser Eigenschaft heißt *Eliminationsordnung* für R_r.

Für das System

$$B = \{x^2 + y + z - 3,\, x + y^2 + z - 3,\, x + y + z^2 - 3\}$$

hatten wir bzgl. der lexikographischen Termordnung mit $x > y > z$ die Gröbnerbasis

$$G = \{x + y + z^2 - 3, y^2 - y - z^2 + z, 2yz^2 - 4y + z^4 - 5z^2 + 6, z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6\}$$

gefunden. Entsprechend erhalten wir die Eliminationsideale

$$I \cap \mathbf{C}[y, z] = I(y^2 - y - z^2 + z, 2yz^2 - 4y + z^4 - 5z^2 + 6, z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6)$$

$$I \cap \mathbf{C}[z] = I(z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6)$$

Das Polynom $g(z) = z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6$ ist also nicht irgendein durch Elimination von x und y entstandenes univariates Polynom, sondern das Erzeugende von $I \cap \mathbf{C}[z]$, d.h. jedes andere durch Elimination entstehende Polynom $h(z) \in I$ ist ein Vielfaches von $g(z)$.

AUFGABE: (1) Gegeben sei das von $B = \{x^2 + 2y^2 - 3,\, x^2 + xy + y^2 - 3\}$ erzeugte Ideal I. Bestimmen Sie die beiden Eliminationsideale $I \cap k[x]$ und $I \cap k[y]$ sowie $V(I)$.

(2) Lösen Sie das Gleichungssystem

$$\begin{aligned} x^2 + y^2 + z^2 &= 4 \\ x^2 + 2y^2 &= 5 \\ xz &= 1 \end{aligned}$$

Zum Abschluß dieses Punkts wollen wir untersuchen, für welche Werte (a, b, c) das Gleichungssystem

$$\begin{aligned} x^2 + y^2 &= a \\ x^3 + y^3 &= b \\ x^4 + y^4 &= c \end{aligned}$$

Lösungen besitzt. Dazu müssen die drei rechten Seiten in einem wohlbestimmten Verhältnis zueinander stehen, das wir ermitteln können, wenn wir im Polynomring $k[x, y, a, b, c]$ das Eliminationsideal

$$I(x^2 + y^2 - a,\, x^3 + y^3 - b,\, x^4 + y^4 - c) \cap k[a, b, c]$$

bestimmen. Die entsprechende Gröbnerbasis besteht aus 19 Polynomen, darunter eins, das die Variablen x, y nicht enthält:

$$a^6 - 4\,a^3\,b^2 - 3\,a^2\,c^2 + 12\,a\,b^2\,c - 4\,b^4 - 2\,c^3.$$

Auf dieselbe Weise können wir untersuchen, für welche Koeffizienten $f(x) = x^2 + ax + b$ Mehrfachnullstellen hat. Dies ist genau dann der Fall, wenn $f(x)$ und $f'(x)$ gemeinsame Nullstellen besitzen, d.h. das System $B := \{f(x), f'(x)\}$ gemeinsame Lösungen besitzt. Dazu berechnen wir für $I = I(B)$ in $k[x, a, b]$ das Eliminationsideal $I \cap k[a, b]$, das vom Polynom $a^2 - 4b$ erzeugt wird. Dieses Polynom nennt man die *Diskriminante* von f. Man beachte den Zusammenhang zur allgemeinen Lösungsformel für quadratische Gleichungen.

AUFGABE: Bestimmen Sie die Diskriminante des allgemeinen Polynoms dritten Grades $f(x) = x^3 + ax^2 + bx + c$ sowie des reduzierten Polynoms dritten Grades $g(x) = x^3 + px + q$ und vergleichen Sie Ihr Ergebnis mit der Cardanoschen Formel für die allgemeine Lösung einer Gleichung dritten Grades.

5.2 Der Projektionssatz

Betrachten wir die Projektion affiner Räume

$$\pi_r : \mathbf{A}^n \longrightarrow \mathbf{A}^{n-r} : \quad via \quad (a_1, \ldots, a_n) \mapsto (a_{r+1}, \ldots, a_n).$$

Diese hängt eng zusammen mit der Einbettung $\pi_r^* : R_r \subset R$. Ist insbesondere $I \subset R$ ein Ideal und $V = V(I) \subset \mathbf{A}^n$ dessen Nullstellenmenge, so können wir deren *Projektion* $\pi_r(V) \subset \mathbf{A}^{n-r}$ betrachten.

Diese Projektion muß nicht unbedingt wieder eine algebraische Menge sein. Betrachten wir etwa $V = V(I)$ mit $I = I(xy - 1, xz - 1)$ und dessen Projektion auf die yz-Ebene, so erhalten wir $\pi_2(V) = V(y - z) \setminus \{(0, 0)\}$. In der Tat, es ist $V = \{(a, 1/a, 1/a) \mid a \neq 0\}$. Andererseits liefert das zugehörige Eliminationsideal $I_2 = I(y - z)$ die kleinste algebraische Menge, die $\pi_2(V)$ umfaßt.

Dies gilt allgemein:

Satz 27 *(Projektionssatz) Sei π_r die oben beschriebene Projektion, $I \subset R$ ein Ideal und $V = V(I) \subset \mathbf{A}^n$ dessen Nullstellenmenge. Dann ist die Nullstellenmenge des r-ten Eliminationsideals $V(I_r) \subset \mathbf{A}^{n-r}$ genau der Zarisski-Abschluß $\overline{\pi_r(V)}$ der Projektion $\pi_r(V)$.*

BEWEIS : Wegen $\overline{\pi_r(V)} = V(I(\pi_r(V)))$ genügt es, $I(\pi_r(V)) = rad(I_r)$ in R_r zu zeigen. Das folgt aber sofort aus

$$\pi_r(V) = \{(a_{r+1}, \ldots, a_n) \in \mathbf{A}^{n-r} \mid \exists\ (a_1, \ldots, a_n) \in V\}$$

und der Tatsache, daß $f \in R_r$ nur von den Koordinaten $x_{r+1}, \ldots, x_n$ abhängt. $\square$

5.3 Lösung des regulären Implizitierungsproblems

Sei $\phi : \mathbf{A}^d \longrightarrow \mathbf{A}^n$ eine reguläre Parametrisierung der d-dimensionalen Varietät $V = im\,\phi$, d.h. gegeben durch die polynomialen Funktionen $x_i = \phi_i(t_1, \ldots, t_d)$, $i = 1, \ldots, n$. Wir hatten festgestellt, daß ϕ einen Ringhomomorphismus $\phi^* : k[x_1, \ldots, x_n] \longrightarrow k[t_1, \ldots, t_d]$ induziert, so daß $I(V) = Ker\,\phi^*$ gilt. ϕ^* wird dabei durch die Substitutionen $x_i \mapsto \phi_i(t_1, \ldots, t_d)$, $i = 1, \ldots, n$ induziert. Es stellt sich heraus, daß man das Verschwindungsideal $I(V)$ ebenfalls als Eliminationsideal interpretieren kann.

Satz 28 *(Polynomiale Implizitierung) Sei $I = I(x_i - \phi_i(\mathbf{t}),\, i = 1, \ldots, n)$ ein Ideal im Polynomring $k[\mathbf{x}, \mathbf{t}]$. Mit obigen Bezeichnungen kann man das Verschwindungsideal $I(V)$ der polynomial parametrisierten Varietät V als Eliminationsideal $I(V) = I \cap k[\mathbf{x}]$ berechnen.*

Beweis : Betrachten wir die Menge $B := \{x_i - \phi_i(\mathbf{t}),\, i = 1, \ldots, n\} \subset k[\mathbf{x}, \mathbf{t}]$. Bzgl. einer Eliminationsordnung $\mathbf{x} > \mathbf{t}$ ist sie offensichtlich eine Gröbnerbasis. Da $F(x_1, \ldots, x_n) \in Ker\, \phi^*$ genau dann gilt, wenn $F(\phi_1(\mathbf{t}), \ldots, \phi_n(\mathbf{t})) = NF(F, B) = 0$, folgt die Behauptung. $\square$

Eine Basis von $I(V)$ findet man nach dem Eliminationssatz damit über eine Gröbnerbasisberechnung für I, aber bzgl. einer Eliminationsordnung $\mathbf{t} > \mathbf{x}$. Der im Satz betrachtete Polynomring $k[\mathbf{x}, \mathbf{t}]$ gehört zu einem affinen Raum $\mathbf{A}^{d+n}$, in dem das Ideal I die Varietät

$$\Gamma_\phi = \{(t_1, \ldots, t_d, x_1, \ldots, x_n) \,|\, x_i = \phi_i(\mathbf{t}),\, i = 1, \ldots, n\}$$

beschreibt. Dies ist genau der *Graph* der Funktion ϕ.

Beispiel: Betrachten wir die Tangentialfläche T an die getwistete Kubik, die durch die Abbildung $(t, u) \mapsto (x = t+u, y = t^2+2ut, z = t^3+3ut^2)$ gegeben ist. $I(T)$ können wir damit berechnen, indem wir im Ideal $I = I(x - (t + u), y - (t^2 + 2u\,t), z - (t^3 + 3u\,t^2))$ die Parameter t und u eliminieren. Berechnen wir dazu die Gröbnerbasis bzgl. der entsprechenden lexikographischen Termordnung

```
 Compute GBasis of
1 -->   - t - u + x
2 -->   - t^2 - 2*t*u + y
3 -->   - t^3 - 3*t^2*u + z

   New base elements :

   Investigate (1.2)
4. ---> u^2 - x^2 + y
   Investigate (1.3)
5. ---> 2*u*x^2 - 2*u*y - 2*x^3 + 3*x*y - z
   Investigate (4.5)
6. ---> u*x*y - u*z - x^2*y - x*z + 2*y^2
   Investigate (5.6)
7. ---> 2*u*x*z - 2*u*y^2 + 2*x^2*z - x*y^2 - y*z
   Investigate (6.7)
8. ---> 2*u*y^3 - 2*u*z^2 - 4*x^2*y*z + x*y^3 - 2*x*z^2 + 5*y^2*z
   Investigate (5.7)
9. ---> 4*x^3*z - 3*x^2*y^2 - 6*x*y*z + 4*y^3 + z^2
   Investigate (4.7)
   Investigate (4.6)
   Investigate (6.8)
   Investigate (5.9)
   Investigate (4.8)

{u**2 - x**2 + y,
t + u - x,
4*x**3*z - 3*x**2*y**2 - 6*x*y*z + 4*y**3 + z**2,
2*u*x*z - 2*u*y**2 + 2*x**2*z - x*y**2 - y*z,
u*x*y - u*z - x**2*y - x*z + 2*y**2,
2*u*x**2 - 2*u*y - 2*x**3 + 3*x*y - z,
2*u*y**3 - 2*u*z**2 - 4*x**2*y*z + x*y**3 - 2*x*z**2 + 5*y**2*z}$
```

Da nur das dritte Polynom in der Gröbnerbasis die zu eliminierenden Variablen nicht enthält, wird das Verschwindungsideal $I(T)$ (wie für eine Fläche im $\mathbf{A}^3$ zu erwarten) von einem einzigen Polynom

$$4\,x^3\,z - 3\,x^2\,y^2 - 6\,x\,y\,z + 4\,y^3 + z^2$$

erzeugt.

Wir hatten Beispiele von Parametrisierungen kennengelernt, wo $T = im\,\phi$ nicht abgeschlossen in der Zariski-Topologie war. Wir können in unserem Fall die anderen Gleichungen der Gröbnerbasis verwenden, um eine Aussage zu treffen, welche Punkte auf $V(h)$ mit $h := 4\,x^3\,z - 3\,x^2\,y^2 - 6\,x\,y\,z + 4\,y^3 + z^2)$ wirklich zu T gehören, indem wir entsprechende Parameter (t, u) finden. Für $(x_0, y_0, z_0) \notin V(x{*}z - y^2, x{*}y - z, x^2 - y, y^3 - z^2)$ können wir eine der linearen Gleichungen nach u auflösen. Ergeben sich aus zwei unterschiedlichen Gleichungen unterschiedliche Formeln $u_1(X) = f_1(X)/g_1(X)$ und $u_2(X) = f_2(X)/g_2(X)$ (mit $X = (x, y, z)$ und $g_1(X_0)g_2(X_0) \neq 0$), so gilt $u\,g_1 - f_1, u\,g_2 - f_2 \in I$, also $f_1 g_2 - f_2 g_1 \in I \cap k[X] = I(T)$. Demzufolge ist $u_1(X_0) = u_2(X_0)$, d.h. wir erhalten keine sich widersprechenden Lösungen. Ansonsten ist $u^2 = 0$, also $u = 0$. In jedem Fall bekommen wir aus der ersten Gleichung den zugehörigen Parameter für t heraus.

Betrachten wir als zweites Beispiel die Kurve $C = \{(t^2, t^3, t^4) \mid t \in \mathbf{C}\}$. Zur Bestimmung ihres Verschwindungsideals berechnen wir `GBasis`($\{x - t^2, y - t^3, z - t^4\}$):

```
 Compute GBasis of

1 -->   - t^2 + x
2 -->   - t^3 + y
3 -->   - t^4 + z

 New base elements :

Investigate (1.2)  Pair list has length 1
4. ---> t*x - y
Investigate (1.4)  Pair list has length 1
5. ---> t*y - x^2
Investigate (4.5)  Pair list has length 2
6. ---> x^3 - y^2
Investigate (1.5)  Pair list has length 2
Investigate (4.6)  Pair list has length 1
Investigate (1.3)  Pair list has length 0
7. ---> x^2 - z
Investigate (6.7)  Pair list has length 1
8. ---> x*z - y^2
Investigate (7.8)  Pair list has length 2
9. ---> x*y^2 - z^2
Investigate (4.8)  Pair list has length 4
Investigate (4.7)  Pair list has length 3
10. ---> t*z - x*y
Investigate (5.10)  Pair list has length 5
Investigate (8.9)  Pair list has length 2
11. ---> y^4 - z^3

{y**4 - z**3,
t*z - x*y,
x*y**2 - z**2,
x*z - y**2,
```

```
x**2 - z,
t*y - z,
t*x - y,
t**2 - x}
```

Das Eliminationsideal hat damit die Basis

$$\{y^4 - x^3,\ xy^2 - z^2,\ xz - y^2,\ x^2 - z\}$$

AUFGABE: Bestimmen Sie die Verschwindungsideale der folgenden Kurven und Flächen vgl. [6]

(1) $E_1 := \{(t^4, t^6, t^7) \mid t \in \mathbf{C}\}$
(2) $E_2 := \{(s^4, s^3t, st^3, t^4) \mid s, t \in \mathbf{C}\}$
(3) $E_3 := \{(s^5, s^4t + t^5, s^2t^3, st^4) \mid s, t \in \mathbf{C}\}$

Die Flächen E_2 und E_3 sind *Kegel* mit der Spitze im Ursprung, d.h. mit jedem Punkt $P := (w_0, x_0, y_0, z_0) \in E_i$ gehört die gesamte Gerade $\lambda\, P$ zu E_i. Der Schnitt dieser Fläche mit der Hyperebene $(w = 0)$ ist dann eine Kurve C_i und wir haben eine eineindeutige Korrespondenz zwischen den Mantellinien des Kegels E_i und den Punkten auf C_i, wenn wir letztere um "unendlich ferne" Punkte ergänzen, die Mantellinien durch Punkte $P \in E_i$ mit $w_0 = 0$ entsprechen. Wir sprechen in diesem Zusammenhang auch vom *projektiven Raum* und sagen, daß E_2 und E_3 Kurven im projektiven Raum $\mathbf{P}^3$ beschreiben. Es stellt sich heraus, daß ähnlich wie zwischen Idealen und affinen Varietäten eine enge Bezeihung zwischen projektiven Varietäten und *homogenen* Idealen besteht. Diese wichtige geometrische Konstruktion müssen wir allerdings außerhalb unserer Betrachtungen lassen.

5.4 Berechnung des Idealdurchschnitts

Betrachten wir die beiden Ideale

$$I_1 = I(x^3 - x^2\, y, x\, y^2 - y^3), \quad I_2 = I(x^3 - x\, y^2, x^2\, y - y^3).$$

Man überzeugt sich leicht, daß beide Idealbasen bzgl. der lex. Termordnung bereits Gröbnerbasen sind.

AUFGABE: Zeigen Sie, daß die gegebenen Basen sogar Gröbnerbasen bzgl. jeder nur denkbaren Termordnung, d.h. *universelle Gröbnerbasen* sind.

Offensichtlich ist $f = x^3 - x^2y - xy^2 + y^3 \in I_1 \cap I_2$, da sich f jeweils als Summe der beiden Basiselemente ergibt. Wir erkennen hieran zunächst noch einmal, daß Idealdurchschnitt und Idealprodukt zwar dieselbe Nullstellenmenge $V(I_1 \cdot I_2) = V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$ beschreiben, aber im Allgemeinen $I_1 \cdot I_2 \subsetneq I_1 \cap I_2$ gilt. In der Tat, jedes Polynom im Idealprodukt hat wenigstens den Grad 4.

Die vorliegende geometrische Situation ist recht kompliziert. Wegen

$$I_1 = I(x - y) \cdot I(x^2, y^2) \quad I_2 = I(x^2 - y^2) \cdot I(x, y)$$

erkennen wir, daß die zugehörigen Nullstellengebilde die Gerade $V_1 = V(x - y)$ bzw. das Geradenpaar $V_2 = V(x + y) \cup V(x - y)$ sind, diese jedoch jeweils noch den Ursprung als eingebetteten Punkt höherer Multiplizität enthalten. Dem Idealdurchschnitt entspricht die Vereinigung der beiden Nullstellenmengen, also V_2, mit Vielfachheit 1, dem Idealprodukt eine Gerade mit Vielfachheit 1, die andere mit Vielfachheit 2, den eingebettetn Punkt jeweils nicht gerechnet.

Der Eliminationssatz gestattet es, eine Basis für den Durchschnitt zweier Ideale zu berechnen. Grundlage des Verfahrens ist der folgende

Satz 29 *Seien I_1, I_2 zwei Ideale im Polynomring $R = k[\mathbf{x}]$ und t eine neue Variable. Dann gilt*

$$I_1 \cap I_2 = (I_1 \cdot t + I_2 \cdot (1 - t)) \cap R.$$

Beweis : $f(x) \in I_1 \cap I_2 \;\Rightarrow\; f = f \cdot t + f \cdot (1-t) \in (I_1 \cdot t + I_2 \cdot (1-t)) \cap R$.

Zum Beweis der anderen Inklusion sei $B_1 := \{f_1(x), \ldots, f_r(x)\}$ eine Basis von I_1 und $B_2 := \{g_1(x), \ldots, g_s(x)\}$ eine Basis von I_2. $f(x) \in I_1 \cdot t + I_2 \cdot (1-t)$ kann man dann darstellen als

$$f(x) = \sum_i p_i(x,t)\, f_i(x)\, t + \sum_j q_j(x,t)\, g_j(x)\, (1-t).$$

Setzen wir $t = 0$, so erhalten wir $f(x) = \sum_j q_j(x,0)\, g_j(x) \in I_2$. Setzen wir dagegen $t = 1$, so erhalten wir $f(x) = \sum_i p_i(x,1)\, f_i(x) \in I_1$, also insgesamt $f \in I_1 \cap I_2$. $\square$

In unserem Beispiel berechnen wir also zunächst die Idealsumme $J := I_1 \cdot t + I_2 \cdot (1-t)$. Aus den Basen der beiden Ideale erhalten wir eine Basis für J:

$$B := \{t\,(x^3 - x^2 y), t\,(xy^2 - y^3), (1-t)\,(x^3 - xy^2), (1-t)\,(x^2 y - y^3)\}$$

und interreduziert

$$B' = \{t\,y^2\,(x-y), x^3 - x^2\,y - x\,y^2 + y^3, y\,(t\,x^2 - t\,y^2 - x^2 + y^2)\}.$$

Um eine Basis des gesuchten Eliminationsideals zu finden, berechnen wir die entsprechende Gröbnerbasis

```
Compute GBasis of

1 -->  t*x*y^2 - t*y^3
2 -->  x^3 - x^2*y - x*y^2 + y^3
3 -->  t*x^2*y - t*y^3 - x^2*y + y^3

 New base elements :

Investigate (1.3)  Pair list has length 1
4. ---> x^2*y^2 - y^4
Investigate (2.4)  Pair list has length 2
Investigate (3.4)  Pair list has length 1
Investigate (2.3)  Pair list has length 0

{x**2*y**2 - y**4,
t*x*y**2 - t*y**3,
x**3 - x**2*y - x*y**2 + y**3,
t*x**2*y - t*y**3 - x**2*y + y**3}$
```

Dies liefert den Idealdurchschnitt

$$I(x^2y^2 - y^4,\, x^3 - x^2y - xy^2 + y^3) = I(x^2 - y^2) \cdot I(y^2, x - y),$$

dessen Nullstellengebilde die erwartete Gestalt hat.

Von geometrisch einfacherer Gestalt sollte der Durchschnitt zweier Kurven ohne gemeinsame Komponente sein. Betrachten wir die beiden Kurven

$$C_1 := \{(t, t^2, t^3) \mid t \in \mathbf{C}\} \qquad C_2 := \{(t^2, t^3, t^4) \mid t \in \mathbf{C}\},$$

die beide auf der rationalen Quadrik $V(y^2 - xz)$ liegen und deren Verschwindungsideale wir bereits kennen:

$$I_1 = I(z - x^3, y - x^2) \qquad I_2 = I(z - x^2, y^2 - xz).$$

Für den Idealdurchschnitt erhalten wir

$$\begin{aligned} I_1 \cap I_2 = I(&x\,z - y^2,\, y^7 - y^4\,z^2 - y^3\,z^3 + z^5, \\ &x\,y^5 - y^4\,z - y^3\,z^2 + z^4,\, x^2\,y^3 - y^4 - y^3\,z + z^3, \\ &x^4 - x^2\,y - x\,y^2 + y\,z,\, x^3\,y - x\,y^2 - y^3 + z^2) \\ = I(&x\,z - y^2,\, x^4 - x^2\,y - x\,y^2 + y\,z,\, x^3\,y - x\,y^2 - y^3 + z^2) \end{aligned}$$

für das Idealprodukt dagegen

$$\begin{aligned} I_1 \cdot I_2 = I(&x^3\,y - x^2\,z - x\,y\,z + z^2,\, x^2\,y\,z - x\,y^3 - x\,z^2 + y^2\,z, \\ &x^3\,z - x^2\,y^2 - x\,y\,z + y^3,\, x^4 - x^2\,y - x^2\,z + y\,z) \end{aligned}$$

Aufgabe: Führen Sie die entsprechenden Rechnungen aus.
Auch in diesem Fall sind also Idealdurchschnitt und -produkt verschieden.

Aufgabe: Berechnen Sie den Idealdurchschnitt

$$I(wz - xy, w^2y - x^3) \cap I(wy^2 - x^2z, xz^2 - y^3)$$

Aufgabe: Obigen Satz kann man folgendermaßen auf die Berechnung des Durchschnitt mehrerer Ideale erweitern:

Seien $I_1, \ldots, I_k$ Ideale im Polynomring $R = k[\mathbf{x}]$ und $y_1, \ldots, y_k$ neue Variablen. Dann gilt

$$I_1 \cap \ldots \cap I_k = (I_1\,y_1 + \ldots I_k\,y_k + I(y_1 + \ldots + y_k - 1)) \cap R.$$

Beweisen Sie diese Verallgemeinerung.

5.5 Ein Radikalenthaltenseinstest

Betrachten wir als nächstes die Frage, ob ein Polynom $f \in R$ auf einer gegebenen Varietät $V = V(I)$ verschwindet. Wir hatten dies bereits auf die Frage $f \in rad(I)$, den *Radikalenthaltenseinstest*, zurückgeführt. Leider kennen wir im allgemeinen die Basis von $rad(I)$ nicht. Nach Hilberts Nullstellensatz könnten wir statt dessen $f^k \in I$ für $k > 0$ testen, bis wir eine positive Antwort gefunden haben oder aber k groß genug ist, um sicher eine negative Antwort ableiten zu können. Ein effizienteres Verfahren zur Beantwortung des Radikalenthaltenseinstests geht auf den sogenannten Rabinowitsch-Trick zurück.

Satz 30 *Sei $R = k[\mathbf{x}]$, $f \in R$, $I \subset R$ ein Ideal und t eine neue Variable. Dann gilt*

$$f \in rad(I) \quad \Leftrightarrow \quad I \cdot R[t] + I(1 - t \cdot f) = I(1),$$

wobei das Ideal im Ring $R[t]$ betrachtet wird.

Beweis : Sei $B = \{f_1(x), \ldots, f_r(x)\}$ eine Basis des Ideals I. Gilt $f^k \in I$, also

$$f^k = p_1(x)f_1(x) + \ldots + p_r(x)f_r(x)$$

in R, so folgt

$$1 = t^k \cdot (r_1(x)f_1(x) + \ldots + r_k(x)f_k(x)) + (1 - (t\,f)^k)) \in I\,R[t] + I(1 - t \cdot f).$$

Ist umgekehrt

$$1 = p_1(x,t)f_1(x) + \ldots + p_r(x,t)f_r(x) + p(x,t) \cdot (1 - t \cdot f) \in I\,R[t] + I(1 - t \cdot f),$$

so erhalten wir nach der Substitution $t \mapsto 1/f$ eine rationale Funktion mit einem Hauptnenner f^k. Multiplizieren wir mit diesem durch, so bleibt ein polynomialer Ausdruck

$$f^k = \tilde{p}_1(x) f_1(x) + \ldots + \tilde{p}_r(x) f_r(x) \in I.$$

Damit haben wir den Satz bewiesen. $\square$

Beispiel: Da $V(I_1 \cap I_2) = V(I_1 \cdot I_2)$ gilt, sollte im Beispiel, das wir im letzten Abschnitt durchgerechnet hatten,

$$f := x\,z - y^2 \in rad(I_1 \cdot I_2)$$

gelten. Prüfen wir das entsprechend dem bewiesenen Satz:

```
 Compute GBasis of

1 -->  x*z*t - y^2*t - 1
2 -->  x^3*y - x^2*z - x*y*z + z^2
3 -->  x^2*y*z - x*y^3 - x*z^2 + y^2*z
4 -->  x^3*z - x^2*y^2 - x*y*z + y^3
5 -->  x^4 - x^2*y - x^2*z + y*z

 New base elements :

Investigate (2.4)  Pair list has length 5
6. ---> x^2*y^3 - x^2*z^2 + x*y^2*z - x*y*z^2 - y^4 + z^3
Investigate (2.3)  Pair list has length 6
7. ---> x^2*z^2 - 2**x*y^2*z + y^4
Investigate (3.7)  Pair list has length 8
8. ---> x*y^3*z - x*z^3 - y^5 + y^2*z^2
Investigate (4.7)  Pair list has length 9
Investigate (4.5)  Pair list has length 8
9. ---> x*y^2*z - x*z^2 - y^4 + y^2*z
Investigate (8.9)  Pair list has length 8
10. ---> x*y*z^2 - x*z^3 - y^3*z + y^2*z^2
Investigate (9.10)  Pair list has length 10
11. ---> x*z^4 - x*z^3 - y^2*z^3 + y^2*z^2
Investigate (3.10)  Pair list has length 12
Investigate (3.9)  Pair list has length 11
12. ---> x*z^3 - x*z^2 - y^2*z^2 + y^2*z
Investigate (11.12)  Pair list has length 11
Investigate (10.12)  Pair list has length 10
Investigate (7.12)  Pair list has length 9
Investigate (2.5)  Pair list has length 8
13. ---> x*y*z - x*z^2 - y^3 + y^2*z
Investigate (10.13)  Pair list has length 8
Investigate (9.13)  Pair list has length 7
Investigate (3.13)  Pair list has length 6
Investigate (1.13)  Pair list has length 5
14. ---> y - z
Investigate (13.14)  Pair list has length 5
Investigate (2.14)  Pair list has length 4
15. ---> x^2*z - 2*x*z^2 - z^4 + 3*z^3 - z^2
Investigate (7.15)  Pair list has length 5
16. ---> z^5 - 2*z^4 + z^3
```

```
Investigate (3.15)  Pair list has length 6
Investigate (4.15)  Pair list has length 5
Investigate (1.15)  Pair list has length 4
17. ---> z^4*t - 2*z^3*t + z^2*t -x + z
Investigate (6.14)  Pair list has length 6
Investigate (1.12)  Pair list has length 5
18. ---> z^2 - z
Investigate (14.18)  Pair list has length 5
Investigate (12.18)  Pair list has length 4
Investigate (7.18)  Pair list has length 3
Investigate (1.18)  Pair list has length 2
19. ---> z - 1
Investigate (18.19)  Pair list has length 5
Investigate (14.19)  Pair list has length 4
Investigate (15.19)  Pair list has length 3
20. ---> x^2 - 2*x + 1
Investigate (15.20)  Pair list has length 5
Investigate (14.20)  Pair list has length 4
Investigate (1.19)  Pair list has length 3
21. ---> x*t - t - 1
Investigate (1.21)  Pair list has length 5
Investigate (14.21)  Pair list has length 4
Investigate (20.21)  Pair list has length 3
22. ---> x - 1
Investigate (19.22)  Pair list has length 6
Investigate (14.22)  Pair list has length 5
Investigate (20.22)  Pair list has length 4
Investigate (21.22)  Pair list has length 3
23. ---> 1
```

Eine direkte Anwendung des Idealenthaltenseinstests zeigt, daß $f \notin I_1 \cdot I_2$, aber $f^2 \in I_1 \cdot I_2$ gilt.

5.6 Idealquotienten und relative Nullstellenmengen

Im Zusammenhang mit dem rationalen Implizitierungsproblem haben wir den Fall zu berücksichtigen, daß Punkte zu vermeiden sind, in denen eines der Nennerpolynome verschwindet. Studieren wir diese Situation zunächst einzeln.

Seien $B, C \subset R$ endliche Teilmengen unseres Polynomrings. Wir bezeichnen

$$V(B,C) := \{a \in \mathbf{A}^n \mid \forall\ f \in B\ :\ f(a) = 0 \quad \forall\ g \in C\ :\ g(a) \neq 0\}$$

als *relative Nullstellenmenge*. Offensichtlich gilt

$$V(B,C) = V(B) \setminus V(c),$$

wobei $c := \prod (g \in C)$ das Produkt der Nebenbedingungen $g \in C$ ist. Eine solche relative Nullstellenmenge ist normalerweise nicht mehr abgeschlossen in der Zariski-Topologie. Wir können aber ähnlich wie im Projektionssatz nach dem affinen Abschluß einer solchen Menge fragen. Offensichtlich kann dieser größer als $I(B)$ sein, weil $c \neq 0$ ganze Komponenten von $V(B)$ ausschließen kann.

Genauer gilt folgende Aussage:

$$f \text{ verschwindet auf } V(B,C) \ \Leftrightarrow\ f \cdot c \text{ verschwindet auf } V(B).$$

Bezeichnet $I(B,C)$ ein noch in geeigneter Weise zu definierendes *relatives Ideal*, so können wir eine analoge idealtheoretische Aussage wie folgt formulieren:

$$f \in I(B,C) \;\Leftrightarrow\; f \cdot c \in I(B).$$

Erinnern wir uns weiterhin daran, daß $I(B)$ die Nullstellen von B mit ihren Vielfachheiten widerspiegelt, so ist noch zu berücksichtigen, daß zwar $f\,c$ auf $V(B)$ verschwindet, aber vielleicht nicht mit der nötigen Vielfachheit, sondern dies erst für $f\,c^k$ bei einem geeigneten $k > 0$ erreicht wird.

Dies führt auf die folgenden beiden Begriffe

DEFINITION: Ist $I \subset R$ ein Ideal und $c \in R$ ein Polynom, so bezeichnet man

$$I : c \;:=\; \{f \in R \mid f\,c \in I\}$$

als den *Idealquotienten* von I nach c und

$$I : c^\infty \;:=\; \{f \in R \mid \exists\, k\ f\,c^k \in I\}$$

als den *stabilen Idealquotienten* von I nach c.

Es zeigt sich, daß man Basen der entsprechenden Ideale ebenfalls mit Eliminationstechniken berechnen kann.

Satz 31 *Ist $R = k[\mathbf{x}]$, $I \subset R$ ein Ideal, $c(x) \in R$ und t eine neue Variable, so gilt*

$$I : c = \tfrac{1}{c}(I \cap I(c))$$

und

$$I : c^\infty = (I \cdot R[t] + I(1 - t \cdot c)) \cap R.$$

BEWEIS : Die erste Beziehung ist offensichtlich. Zum Beweis der zweiten wenden wir wieder den Rabinowitsch-Trick an.

Sei dazu $B = \{f_1(x), \ldots, f_r(x)\}$ eine Basis des Ideals I. Gilt $f(x) \in I : c^\infty$, also $f\,c^k \in I$ für ein geeignetes $k \gg 0$, so folgt

$$f\,c^k = p_1(x) f_1(x) + \ldots + p_r(x) f_r(x)$$

in R und damit

$$f = t^k \cdot (r_1(x) f_1(x) + \ldots + r_k(x) f_k(x)) + f \cdot (1 - c^k\,t^k) \in I\,R[t] + I(1 - t\,c).$$

Ist umgekehrt

$$f = p_1(x,t) f_1(x) + \ldots + p_r(x,t) f_r(x) + p(x,t) \cdot (1 - t\,c) \in I\,R[t] + I(1 - t\,c),$$

so erhalten wir nach der Substitution $t \mapsto 1/c$ wiederum eine rationale Funktion mit einem Hauptnenner c^k. Multiplizieren wir mit diesem durch, so bleibt ein polynomialer Ausdruck

$$f\,c^k = \tilde{p}_1(x) f_1(x) + \ldots + \tilde{p}_r(x) f_r(x) \in I.$$

Damit haben wir den Satz bewiesen. $\square$

5.7 Zur Geometrie von Nullstellenmengen

Untersuchen wir nun die Struktur von Nullstellengebilden und den damit verbundenen Idealen genauer. Wir hatten gesehen, daß sich manche affine Varietäten als Vereinigung anderer affiner Varietäten darstellen lassen.

DEFINITION: Eine affine Varietät V heißt *irreduzibel*, wenn sie sich nicht als Vereinigung zweier echt kleinerer Varietäten darstellen läßt, d.h. wenn

$$V = V_1 \cup V_2 \;\Rightarrow\; V = V_1 \text{ oder } V = V_2$$

gilt.

Ist V eine solche irreduzible Varietät und verschwindet das Produkt $f\,g$ auf ganz V, so muß bereits einer der Faktoren auf V verschwinden. In der Tat, wegen

$$(V \cap V(f)) \cup (V \cap V(g)) = V \cap (V(f) \cup V(g)) = V \cap V(fg) = V$$

wäre das eine Zerlegung in kleinere Varietäten. Das Verschwindungsideal $I := I(V)$ hat also eine besondere Eigenschaft

$$f, g \in R,\ f\,g \in I \ \Rightarrow\ f \in I \text{ oder } g \in I.$$

DEFINITION: Ideale I mit dieser Eigenschaft nennt man *Primideale*.

AUFGABE: Zeigen Sie, daß $P \subset R$ genau dann ein Primideal ist, wenn der Faktorring R/P nullteilerfrei, also ein Integritätsbereich ist.

Satz 32 *Jedes Radikalideal läßt sich als Durchschnitt endlich vieler Primideale darstellen.*

BEWEIS : Wir zeigen zunächst, daß jedes Radikalideal I, das kein Primideal ist, sich als Durchschnitt zweier echt größerer Radikalideale darstellen läßt. Ist nämlich I kein Primideal, so gibt es $f, g \in R \setminus I$ mit $fg \in I$. Dann gilt aber

$$I = rad(I, f) \cap rad(I, g).$$

Die eine Inklusion ist offensichtlich. Die andere folgt aus

$$rad(I, f) \cap rad(I, g) \subseteq rad((I, f) \cdot (I, g)) \subset rad(I, fg) = I,$$

vgl. die entsprechende Übungsaufgabe aus Abschnitt 3.3. zum Rechnen mit Radikalidealen.

Jedes nicht prime Radikalideal ist also Durchschnitt zweier größerer Radikalideale. Da nach dem Hilbertschen Basissatz Idealketten endlich sind, kann ein solcher Zerlegungsprozeß nur endlich oft durchgeführt werden, jeder Zweig endet also nach endlich vielen Schritten in einem Primideal. □

Korollar 2 *Jede affine Varietät ist die Vereinigung von endlich vielen irreduziblen Varietäten.*

Kleinste affine Varietäten sind Punkte. Ihnen entsprechen die größten Verschwindungsideale.

$$P = (a_1, \ldots, a_n) \in \mathbf{A}^n \quad \Rightarrow \quad I(P) = I(x_1 - a_1, \ldots, x_n - a_n)$$

Ein solches Ideal ist in keinem nichttrivialen Ideal enthalten und heißt deshalb *maximales Ideal*.

AUFGABE: Zeigen Sie, daß $P \subset R$ genau dann ein maximales Ideal ist, wenn der Faktorring R/P ein Körper ist. In unserem Fall ist

$$R/I(P) \cong k \qquad \text{via} \qquad f \in R/I \mapsto f(P) \in k.$$

5.8 Lösung des rationalen Implizitierungsproblems

Betrachten wir zum Abschluß das rationale Parametrisierungsproblem: Gegeben ist eine Varietät

$$V = \{(\phi_1(a), \ldots, \phi_n(a)) \mid a \in \mathbf{C}^d \setminus W\},$$

wobei $\phi_i(T) \in k(T)$ rationale Funktionen in $T = (t_1, \ldots t_d)$ sind und W die Varietät, auf der eine dieser rationalen Funktionen nicht definiert ist. Gesucht ist das Verschwindungsideal $I(V)$ dieser Varietät.

Wir können zuerst einmal annehmen, daß die rationalen Funktionen $\phi_i(T) = f_i(T)/g(T)$ einen gemeinsamen Nenner haben und $gcd(f_1, \ldots, f_n, g) = 1$ gilt. Eine solche Parametrisierung kann man dann analog dem regulären Fall als Abbildung

$$\phi\ :\ \mathbf{A}^d \setminus W \ \longrightarrow\ \mathbf{A}^n$$

mit $W = V(g)$ auffassen, wobei $V = im\,\phi$ gilt.

Die Dualisierung ergibt eine Abbildung

$$\phi^* \;:\; k[X] \;\longrightarrow\; k(T) \qquad \text{via} \qquad x_i \mapsto \frac{f_i(T)}{g(T)},$$

wobei $X = (x_1, \ldots, x_n)$ bedeutet. Im Gegensatz zu regulären Parametrisierungen besteht das Bild $im\,\phi^*$ nicht mehr aus Polynomen, weil die Variablen x_i durch rationale Funktionen ersetzt wurden. Wir werden diese Abbildung deshalb mit Hilfe einer Zusatzvariablen y in zwei Etappen zerlegen, die polynomiale Substitution $x_i \mapsto f_i \cdot y$ und die rationale Substitution $y \mapsto 1/g$.

Dabei verfahren wir ähnlich wie im Fall regulärer Parametrisierungen und betrachten geeignete Zwischenringe:

$$\begin{array}{ccccc} \phi^* : & k[X] & \longrightarrow & k[T,X,y] & \\ & & & \psi_1 \downarrow & \searrow \psi_3 \\ & & & k[T,y] & \xrightarrow{\psi_2} \quad k(T) \end{array}$$

wobei die Abbildung ψ_1 durch die Substitution $x_i \mapsto f_i \cdot y$, die Abbildung ψ_2 durch die Substitution $y \mapsto 1/g$ und ψ_3 durch die Substitution $x_i \mapsto f_i/g,\, y \mapsto 1/g$ induziert wird. Setzt man die Abbildungen zusammen, so erhält man offensichtlich gerade unsere Substitution ϕ^*.

Berechnen wir nun

$$Ker\,\phi^* = Ker(\psi_2 \circ \psi_1) \cap k[X] = \psi_1^{-1}(Ker\,\psi_2) \cap k[X].$$

Dazu wollen wir zuerst $Ker\,\psi_2$ berechnen. Sei $p(T,y) = \sum_{i=0}^n p_i(T) y^i \in Ker\,\psi_2$. Dann gilt $\sum_{i=0}^n \frac{p_i}{g^i} = 0$ und damit auch

$$g^n \cdot p(T,y) = \sum_{i=0}^n g^n \cdot p_i(y^i - \frac{1}{g^i}) = \sum_{i=0}^n g^{n-i} \cdot p_i((g\,y)^i - 1) \in I(g\,y - 1),$$

also $p(T,y) \in I(g\,y - 1) : g^\infty$. Nach unserem Algorithmus erhalten wir diesen stabilen Idealquotienten als Eliminationsideal

$$I(g\,y - 1) : g^\infty = I(g(T)\,y - 1,\, g(T)\,z - 1) \cap k[T,y]$$

mit einer neuen Variablen z.

AUFGABE: Zeigen Sie, daß $I(g\,y - 1) : g^\infty = I(g\,y - 1)$ gilt.

Umgekehrt ist natürlich jedes Element aus diesem Ideal bereits in $Ker\,\psi_2$, so daß wir insgesamt schließen, daß $Ker\,\psi_2 = I(g\,y - 1)$ gilt.

$\psi_1^{-1}(Ker\,\psi_2)$ ergibt sich damit genau wie im Fall regulärer Parametrisierung als

$$\psi_1^{-1}(Ker\,\psi_2) = I(x_1 - f_1\,y,\, \ldots,\, x_n - f_n\,y,\, g\,y - 1),$$

wobei man wieder verwenden kann, daß die angegebene Basis nach dem Hauptsyzygienkriterium bereits eine Gröbnerbasis bzgl. einer Eliminationsordnung für $x_1, \ldots, x_n \gg y \gg t_1, \ldots, t_d$ ist.

Wir haben damit folgenden Satz bewiesen:

Satz 33 *(Implizitierung rational parametrisierter Varietäten) Sei*

$$V = \{(\frac{f_1(a)}{g(a)}, \ldots, \frac{f_n(a))}{g(a)} \mid a \in \mathbf{C}^d \setminus V(g)\}$$

eine rational parametrisierte Varietät. Dann gilt

$$I(V) = I(x_1 - f_1(T)\,y,\, \ldots,\, x_n - f_n(T)\,y,\, g(T)\,y - 1) \cap k[X],$$

wobei $T = (t_1, \ldots t_d)$ und y neue Variablen sind, d.h. das Verschwindungsideal kann man als Eliminationsideal berechnen.

Aufgabe: Zeigen Sie, daß

$$I(x_1 - f_1\,y,\,\ldots,\,x_n - f_n\,y,\,g\,y - 1) = I(g\,x_1 - f_1,\,\ldots,\,g\,x_n - f_n,\,g\,y - 1)$$

gilt.

Letzteres Ideal entstand bei der Berechnung des stabilen Idealquotienten von $I_2 := I(g\,x_1 - f_1, \ldots, g\,x_n - f_n)$ nach g. Diese Verbindung ist nicht zufällig. Bei der Substitution ϕ^* entstehen nicht beliebige rationale Funktionen, sondern nur solche, deren Nenner eine Potenz von g ist. Die Menge $\{g^i,\, i \in \mathbf{N}\}$ aller Potenzen von g ist aber eine *multiplikative Menge*, d.h. eine solche Menge $s \subset R$, daß $1 \in S$ und

$$s_1, s_2 \in S \quad \Longrightarrow \quad s_1 \cdot s_2 \in S$$

gilt. Die Menge

$$R_S := \{\frac{f}{s} \,|\, f \in R\ s \in S\}$$

ist, wie man leicht nachprüft, abgeschlossen unter Addition und Multiplikation rationaler Funktionen, also ein Ring zwischen R und dessen Quotientenkörper. Im Fall $S := \{g^i,\, i \in \mathbf{N}\}$ schreiben wir auch kurz R_g. Für $R = k[T]$ besteht dieser Ring aus genau den auf $\mathbf{A}^d \setminus V(g)$ regulären Funktionen.

Die Substitution ϕ^* kann man damit als

$$k[X] \longrightarrow R' := k[T,X] \longrightarrow R'_g := k[T,X]_g \stackrel{x_i \mapsto f_i/g}{\longrightarrow} k[T]_g$$

beschreiben, wobei die nicht markierten Abbildungen die natürlichen Ringeinbettungen sind und $I_2 \subset R'$ in R'_g offensichtlich das Ideal

$$I'_2 = I_2 \cdot R'_g = I(x_1 - \frac{f_1}{g}, \ldots, x_n - \frac{f_n}{g})$$

erzeugt. Also gilt $Ker\,\phi^* = I'_2 \cap k[X]$.

Aufgabe: Zeigen Sie, daß für ein Ideal $I \subset R'$ und $I' = I \cdot R'_g$ stets $I' \cap R' = I : g^\infty$ gilt.

Der Polynomring $k[T,X] = (k[T])[X]$, betrachtet als Polynomring in X mit polynomialen Koeffizienten in T, ist ein Unterring von $k(T)[X]$. Auf der Ebene dieser größeren Ringe ist ϕ^* ebenfalls wohldefiniert und bildet das Polynom $f(x_1, \ldots, x_n)$ auf dessen Wert im Punkt $P(T) := (\phi_1(T), \ldots, \phi_n(T)) \in \mathbf{A}^n_{k(T)}$ ab. $\mathbf{A}^n_{k(T)}$ ist dabei der affine n-dimensionale Raum, dessen Koordinaten aus dem Körper $k(T)$ gewählt sind. Den Punkt $P(T)$ nennt man deshalb auch den *allgemeinen Punkt* der parametrisiert gegebenen Varietät V. Das Verschwindungsideal $I_{k(T)}(P) \in k(T)[X]$ eines solchen Punktes wird, wie wir im letzten Abschnitt gesehen haben, von den Polynomen $(x_1 - \phi_1(T), \ldots, x_n - \phi_n(T))$ erzeugt.

Literatur

[1] D. Cox, J. Little, D. O'Shea: Ideals, Varieties and Algorithms An Introduction to algebraic geometry and commutative algebra Undergraduate Text, Springer, 1992.

[2] Atiyah, MacDonald: Introduction to commutative algebra. Addison Wesley, 1968.

[3] T. Becker, V. Weispfenning: Groebner bases. Springer, 1993.

[4] D. Eisenbud: Commutative algebra with a view toward algebraic geometry. Springer, 1995.

[5] B. Mishra: Algorithmic Algebra. Springer 1993.

[6] B. Renschuch: Elementare und praktische Idealtheorie. Verlag der Wissenschaften, Berlin 1976.