Konstruktive Nichtlineare Algebra
Sommersemester 2000
Notizen zur Vorlesung

H.-G. Gräbe, Institut für Informatik,
`http://www.informatik.uni-leipzig.de/~graebe`

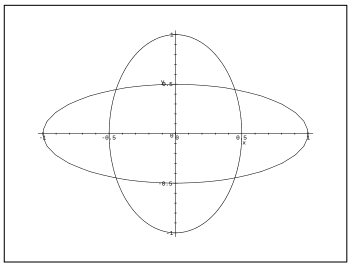
27. Juni 2000

1 Einführung

1.1 Besonderheiten bei nichtlinearen Gleichungssystemen

Bsp: Pseudolineares Gl.-S.

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



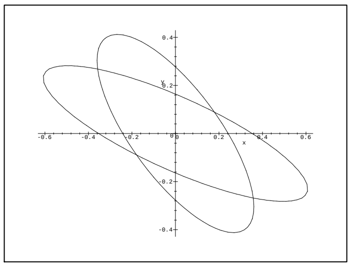
Lösungsmenge

$$L = \{(\pm\frac{\sqrt{5}}{5}, \pm\frac{\sqrt{5}}{5})\}$$

Gleichungssystem nach Koordinatentransformation

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

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



Lösungsmenge :

$(x,y) =$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$	$*\frac{\sqrt{5}}{5}$
$(x',y') =$	$(2,1)$	$(-4,3)$	$(4,-3)$	$(-2,-1)$	$*\frac{\sqrt{5}}{25}$

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

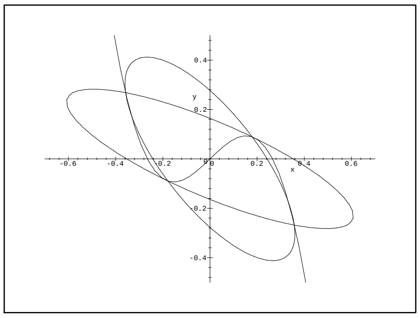
Lösungsmenge hat paarweise verschiedene x-Werte. Das sind die Nullstellen des Polynoms

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

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

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

Eine allgemeine Theorie müsste also die Polynome



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

umwandeln in

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

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

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

und

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

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 1.1:

Versuchen Sie dasselbe Programm mit

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

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.

1.3 Ideale und Faktorringe

Sei $R = k[x_1, \ldots, x_n]$ der Ring der Polynome in $x_1, \ldots, x_n$ über einem Körper k.

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

(1) $0 \in I$,
(2) $f, g \in I \;\Rightarrow\; f + g \in I$ und
(3) $f \in I,\ h \in R \;\Rightarrow\; h \cdot f \in I$

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* $I(1)$. Ein Ring R ist genau dann ein Körper, wenn er keine *echten*, d.h. von diesen trivialen verschiedene, Ideale enthält.

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 $I_1 = I(B_1)$ mit $B_1 = \{x_1, x_2, x_3\}$, das alle Polynome in $k[x_1, x_2, x_3]$ ohne Absolutglied enthält.

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

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 1.2:

Zeigen Sie
(1) $I(x + x\,y, y + x\,y, x^2, y^2) = I(x, y)$
(2) $I(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = I(x^2 - 4, y^2 - 1)$
(3) $I = I(x_1^2 - x_2, x_2^2 - x_3, x_1 + x_3, x_1^3 - 1) = I(1)$

Ähnlich wie für den Ring der ganzen Zahlen definieren wir für ein Ideal $I \subset R$

$$f \equiv g\ (mod\ I) \;:\Longleftrightarrow f - g \in I.$$

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

Man überzeugt sich leicht davon, dass diese Relation eine Äquivalenzrelation ist, womit wir entsprechende Äquivalenzklassen bilden können, die wir auch als *Restklassen* (mod I) bezeichnen.

Diese Äquivalenzrelation ist in Wirklichkeit sogar eine Kongruenzrelation, da sie Summen und Produkte respektiert. Mit

$$\begin{aligned} f_1 &\equiv g_1\ (mod\ I) \\ f_2 &\equiv g_2\ (mod\ I) \end{aligned}$$

gilt nämlich auch

$$\begin{aligned} f_1 \pm f_2 &\equiv g_1 \pm g_2\ (mod\ I) \\ f_1 \cdot f_2 &\equiv g_1 \cdot g_2\ (mod\ I). \end{aligned}$$

Damit können wir die Addition bzw. Multiplikation von Restklassen modulo I repräsentantenweise definieren. Die Menge der Restklassen bildet bzgl. dieser Operationen einen Ring, den *Restklassen-* oder *Faktorring* $S = R/I$ des Polynomrings R nach dem Ideal I.

DEFINITION: Ein Ideal $M \subset R$ bezeichnet man als *maximales Ideal*, wenn es maximal bzgl. der Inklusionsrelation unter allen echten Idealen von R ist.

Ein Ideal $P \subset R$ bezeichnet man als *Primdeal*, wenn

$$\forall\ a, b \in R\ (a \cdot b \in P \ \Rightarrow\ a \in P \text{ oder } b \in P)$$

gilt.

AUFGABE 1.3:

Zeigen Sie:

(a) M ist genau dann ein maximales Ideal, wenn R/M ein Körper ist.

(b) $a \in R$ ist genau dann invertierbar, wenn es in keinem maximalen Ideal von R enthalten ist.

(c) Das Ideal $P \subset R$ ist genau dann ein Primideal, wenn R/P ein Integritätsbereich ist.

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

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

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

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

Dann gilt $V(B) = V(I(B))$

$I(V) := \{f \in S\ :\ f(\mathbf{a}) = 0\ \forall \mathbf{a} \in V\}$ 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 gilt $C = V(y - f(x))$. Ist dagegen $f(x) = \frac{p(x)}{q(x)}$ eine rationale Funktion mit teilerfremden $p(x), q(x)$, so gilt $C = V(q(x) \cdot y - p(x))$. 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

$$V = \left\{ \left(\frac{1-r^2}{1+r^2}, \frac{2r}{1+r^2} \right) \;:\; r \in \overline{k}\,, 1 + r^2 \neq 0 \right\}$$

Diese ergibt sich aus folgender Überlegung: Wir betrachten die Schar der Geraden 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

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

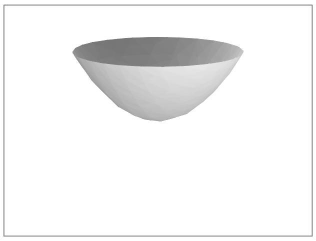
Dass sich dieses durch Elimination entstandene Polynom zweiten Grades in zwei Linearfaktoren zerlegen lässt, entspricht der Tatsache, dass wir einen seiner Faktoren, der P entspricht, vorab kannten. Der zweite Faktor beschreibt die x-Koordinate des zweiten Schnittpunkts, die Geradengleichung daraus die 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 2.1:

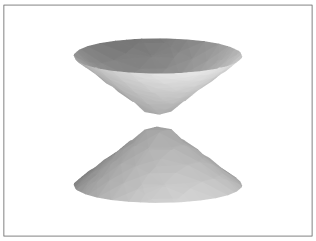
> Betrachten Sie auf analoge Weise die Kurve $V = V(y^2 - x^2 - x^3)$ und versuchen Sie, eine (rationale) Parametrisierung zu finden. Eine solche Kurve nennt man eine *elliptische Kurve.*
>
> Hinweis: Betrachten Sie Geraden durch $(0,0)$. Das erlaubt sogar eine reguläre Parametrisierung, d.h. eine solche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

Affine Varietäten im Raum

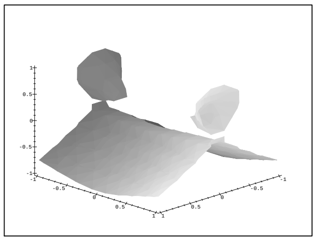
Sind diese wiederum von der Gestalt $V = V(F(x,y,z))$, so handelt es sich um Flächen im Raum wie etwa die folgenden.



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



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



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

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

Beispiel:

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

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.

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 $V = V(B)$, $W = V(C)$ und $V_\alpha = V(B_\alpha)$, so gilt $V \cup W = V(\{fg \;:\; f \in B, g \in C\})$ und $\cap_\alpha V_\alpha = V(\cup_\alpha B_\alpha)$.

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:

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

AUFGABE 2.2:

(a) Zeigen Sie, dass (2) auch für endliche Vereinigungen affiner Varietäten gilt.
(b) Zeigen Sie an einem Beispiel, dass die unendliche Vereinigung affiner Varietäten nicht unbedingt eine affine Varietät sein muss.
(c) Zeigen Sie, dass $V \setminus W$ nicht unbedingt eine affine Varietät sein muss.
(d) Zeigen Sie, 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 affine Varietät ist.

2.4 Parametrisierung affiner Varietäten

Im linearen Fall ist eine solche immer möglich:

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

Die Parametrisierung erfasst alle Punkte der Varietät genau einmal.

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

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

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. Wir können die Parametrisierung verstehen als Abbildung

$$\phi : \mathbf{A}^1 \setminus \{i, -i\} \longrightarrow \mathbf{A}^2,$$

die durch die beiden rationalen Funktionen gegeben wird, durch die sich die x- bzw. y-Koordinate berechnet.

Sei nun n beliebig und $V \subset \mathbf{A}^n$ 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 die Menge

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

die Varietät V so weit wie möglich ausschöpft, d.h. $V = \overline{V'}$ gilt.

Dabei können wir oBdA eine Normierung auf den gemeinsamen Nenner vornehmen:

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

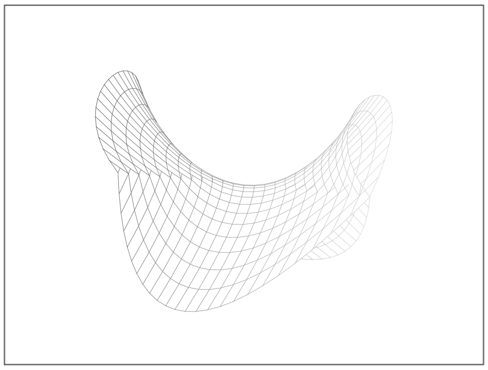
DEFINITION: Eine Parameterdarstellung heißt *polynomial* oder *regulär*, wenn $q(\mathbf{t}) = 1$ gewählt werden kann, d.h. die $r_i(\mathbf{t})$ polynomiale Funktionen sind.

Wie oben können wir eine solche Parametrisierung stets als Abbildung

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

betrachten, die einem Parametertupel $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbf{A}^d$ den Punkt $\mathbf{c} = (r_1(a), \ldots, r_n(a)) \in \mathbf{A}^n$ zuordnet. Dabei ist $W = V(q)$ die Ausnahmemenge, auf der eine der rationalen Koordinatenfunktionen nicht definiert ist. Im Falle einer regulären Parametrisierung ist diese Menge leer.

Vorteile einer Parameterdarstellung: Man kann die Punkte auf V besser generieren. Betrachten wir als Beispiel die "Schweinsohrfläche" $V = V(x^2 - y^2 z^2 + z^3)$.



Setzen wir $y = c$ als Parameter, so erhalten wir eine Schar elliptischer Kurve $x^2 = c\,z^2 - z^3$, die in Aufgabe 4 zu untersuchen war. Die entsprechende Parametrisierung

$$(x, z) = (t\,(c - t^2),\, (c - t^2))$$

kann man zu einer der ganzen Fläche fortsetzen:

$$V = \{t(u^2 - t^2), u, (u^2 - t^2)) \;:\; (u, t) \in C^2\}$$

Eine implizite Darstellung ist vorteilhaft für Tests, ob gegebene Punkte auf einer Varietät liegen. Damit entstehen folgende weiteren Fragen:

(1) Umrechnung einer impliziten in eine Parameterdarstellung.

(2) Implizite Darstellung einer in parametrisierter Form gegebenen Varietät.

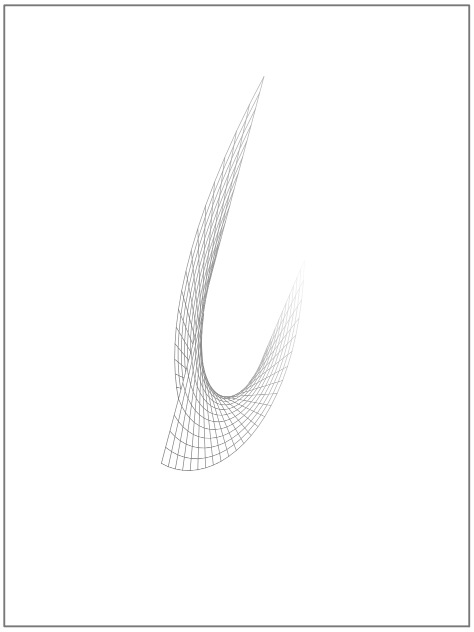
Bei der zweiten Fragestellung entsteht wieder auf natürliche Weise ein Eliminationsproblem. Betrachten wir etwa die Kurve

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

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:

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

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

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

Aufgabe 2.3:

> Betrachten Sie die Kurve $C = \{(\frac{t}{1+t}, 1 - \frac{1}{t^2}) \; : \; t \in \mathbf{C} \setminus \{-1, 0\}\}$.
>
> (a) Finden Sie die Gleichung der affinen Varietät $V = \overline{C}$.
>
> (b) Zeigen Sie, dass $C = V \setminus \{(1,1)\}$ gilt.

Wir sehen an diesem Beispiel noch einmal, dass die Parametrisierung nicht alle Punkte der Varietät erfassen muss, d.h. die Menge der durch die Parametrisierung erzeugten Punkte ist nicht unbedingt abgeschlossen. Das kann selbst für reguläre Parametrisierungen auftreten:

Aufgabe 2.4:

> Gegeben sei die Fläche $F = \{(u\,v, u\,v^2, u^2) \; : \; u, v \in \mathbf{C}\}$. Finden Sie die Gleichung der affinen Varietät $V = \overline{F}$ und bestimmen Sie $V \setminus F$.

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 $0 \leq t \leq 1$, 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, ihre konvexe Hülle bezeichnet man als *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 2.5:

> Zeigen Sie, dass die Bézier-Kurve immer vollständig innerhalb ihres Kontrollpolygons verläuft.
>
> Hinweis: Zeigen Sie, dass ein Punkt P mit den Koordinaten $P = a_1 P_1 + \ldots + a_4 P_4$ in der konvexen Hülle der Punkte $P_1, \ldots, P_4$ liegt.

AUFGABE 2.6:

> 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.
>
> (a) Lassen Sie sich von einem CAS ein Bild einer Strophoide erzeugen ($t = -5 \ \ldots \ 5$).
>
> (b) 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.
>
> (c) Finden Sie eine rationale Parametrisierung für die Strophoide.

3 Verschwindungsideal und Koordinatenring

3.1 Beispiele

Bisher hatten wir Nullstellenmengen zu vorgegebenen Idealen bestimmt. Wir wollen nun $I(V)$, das Ideal der auf einer vorgegebenen Menge verschwindenden Polynome, näher untersuchen.

In einzelnen Fällen lässt sich eine Basis für dieses Ideal leicht angeben. Ist z.B. $V = \{(0, 0, 0)\}$ der Ursprung des $\mathbf{A}^3$, so gilt offensichtlich $I(V) = I(x_1, x_2, x_3)$.

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 $B_2 = \{y - x^2, z - x^3\}$ erzeugt wird.

Sei $J = I(B_2)$. Wegen $B_2 \subset I(C_2)$ haben wir nur $I(C_2) \subset J$ zu zeigen. Ist $f(x, y, z) \in I(C_2)$ ein auf C_2 verschwindendes Polynom, so gilt $f(t, t^2, t^3) = 0$ für alle t, d.h. f wird nach dieser Substitution (und Vereinfachung) das Nullpolynom in $k[t]$. Andererseits gilt $y \equiv x^2, z \equiv x^3$ $(mod\ J$ und somit

$$f(x, y, z) \equiv f(x, x^2, x^3) =: g(x) \ (mod\ J),$$

da f eine polynomiale Funktion ist. Wegen $f \in I(C_2)$ 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 3.1:

> 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 3.2:

> Bestimmen Sie das Verschwindungsideal der Kurve $C_4 = \{(a^3, a^4, a^5) \; : \; a \in \mathbf{C}\}$.

Der Faktorring $k[V] := R/I(V)$ bgzl. des Verschwindungsideals $I(V)$ einer affinen Varietät V hat eine direkte geometrische Interpretation: Dieser Ring ist der Ring der polynomialen Funktionen auf V. In der Tat, sind $f, g \in R$ zwei Polynome, die als Funktionen auf V zusammenfallen, so gilt $f - g \in I(V)$ und umgekehrt. Man bezeichnet $k[V]$ deshalb auch als den *Koordinatenring* von V.

3.2 Das Verschwindungsideal regulär parametrisierter Varietäten

Sei nun V eine regulär parametrisierte Varietät und

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

mit $\phi = (\phi_1, \phi_2, \ldots, \phi_n)$ und polynomialen Funktionen $\phi_i \in k[t_1, \ldots, t_d]$, $i = 1, \ldots, n$ die zugehörige Parametrisierung. Im Fall der Kurve C_2 aus dem vorigen Abschnitt gilt

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

und $C_2 = im(\phi)$.

$f(x, y, z)$ verschwindet genau dann auf C_2, wenn das durch die entsprechenden Substitutionen aus f erzeugte Polynom identisch, d.h. als Element des Polynomrings $k[t]$, verschwindet. Dies können wir auch so formulieren: Die Ersetzung $x \to t, y \to t^2, z \to t^3$ induziert einen Ringhomomorphismus zwischen den Koordinatenringen

$$\phi^* : \; k[\mathbf{A}^3] = k[x, y, z] \longrightarrow k[\mathbf{A}^1] = k[t] \qquad \text{via} \qquad f \mapsto f \circ \phi,$$

wobei

$$f \in I(V) \iff \phi^*(f) = f \circ \phi = 0$$

gilt.

Auch im allgemeinen Fall induziert ϕ eine solche duale Abbildung zwischen den Koordinatenringen

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

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 $f \in ker(\phi^*)$ gilt.

Hierbei steht $ker(\psi) = \{u \in R \,:\, \psi(u) = 0\}$ für den *Kern* des Ringhomomorphismus $\psi : R \longrightarrow R'$.

Aufgabe 3.3:

> 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 regulär parametrisierten 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 Parametrisierungsabbildung, so gilt $I(V) = ker(\phi^*)$ und $k[V] = R/I(V) = im(\phi^*)$.*

3.3 Der Korrespondenzsatz, Teil 1

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 (über dem algebraischen Abschluss $\overline{k}$ des Grundkörpers k !) 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 3.4:

> Zeigen Sie, dass $rad(I)$ wiederum ein Ideal ist.

Es stellt sich heraus, dass dies bereits alle Funktionen sind, die auf einer gegebenen Varietät V verschwinden. Betrachten wir dafür zunächst $V = \emptyset$. Im Fall $n = 1$ 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 $I \subset k[x_1, \ldots, x_n]$ ein Ideal, so gilt*

$$V_{\overline{k}}(I) = \emptyset \quad \Longleftrightarrow \quad I = I(1).$$

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

Satz 6 *Ist $I \subset R = k[x_1, \ldots, x_n]$ ein Ideal und $V = V_{\overline{k}}(I)$, 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 $B = \{f_1, \ldots, f_m\}$ eine Idealbasis von I. Sei weiter t eine neue Variable, $S = R[t]$ und $J \subset S$ das von $f_\alpha \in B,\ \alpha = 1, \ldots, m$, 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*.

Wir haben damit den folgenden Satz bewiesen:

Satz 7 *(Korrespondenzsatz, Teil 1) Sei*

- *$\mathcal{V}$ die Menge der Teilmengen des $\mathbf{A}^n$,*
- *$\mathcal{I}$ die Menge der Ideale $I \subset R$,*
- *$V : \mathcal{I} \longrightarrow \mathcal{V}$ die Abbildung, die einem Ideal J die zugehörige Nullstellenmenge $V(J)$ zuordnet und*
- *$I : \mathcal{V} \longrightarrow \mathcal{I}$ die Abbildung, die einer Teilmenge $W \subset \mathbf{A}^n$ das Ideal $I(W)$ 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. $\square$

3.4 Affine Varietäten und 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 zugelassen 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:

$I_1 + I_2 = I(x_1 + x_2, x_2x_3, x_2x_4, x_3^2 - x_4x_5, x_4^2 - x_5^2)$

$J_1 = I(x_1 + x_2, x_1x_2),\ J_2 = I(x_1 - x_2, x_1x_2),\ \ J_1 + J_2 = I(x_1, x_2)$ (nach Transformation).

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:

$I_1 \cdot I_2 = I((x_1 + x_2)^2, (x_1 + x_2)x_2x_4, \ldots, (x_3^2 - x_4x_5)(x_4^2 - x_5^2))$ (insgesamt $3 \cdot 3 = 9$ Produkte)

$J_1 \cdot J_2 = I(x_1^2 - x_2^2, x_2^3, x_1x_2^2)$ (nach Transformation).

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.

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: Betrachten wir den Polynomring $k[x]$ in einer Variablen. Das ist ein Hauptidealring. Für $I = I(f), J = I(g)$ gilt

$$I + J = I(\gcd(f, g)) \qquad I \cdot J = I(f \cdot g) \qquad I \cap J = I(\mathrm{lcm}(f, g)).$$

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 als das Produkt.

AUFGABE 3.5:

> Zeigen Sie, dass Summe oder Produkt von Radikalidealen nicht unbedingt wieder Radikalideale sein müssen.
>
> 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) Mit den Bezeichnungen aus dem Korrespondenzsatz, 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 3.6:

> Seien $a, b, c \subset R$ Ideale. Beweisen Sie die folgenden Relationen
>
> $$\begin{array}{rrcl} 1. & (a+b)c & = & ac+bc \\ 2. & (a\cap b)+c & \subseteq & (a+c)\cap(b+c) \\ 3. & (a\cap b)\cdot c & \subseteq & (a\cdot c)\cap(b\cdot c) \\ 4. & a\cdot b+c & \supseteq & (a+c)\cdot(b+c) \\ 5. & a\cap(b+c) & \supseteq & (a\cap b)+(a\cap c) \\ 6. & a\cap(b\cdot c) & \supseteq & (a\cap b)\cdot(a\cap c) \end{array}$$
>
> 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*
>
> $$7. \quad c \subseteq a \Rightarrow a \cap (b+c) = (a \cap b) + c.$$
>
> Beweisen Sie diese Aussage.

3.5 Zur Geometrie von Nullstellenmengen

Der Darstellung affiner Varietäten als Vereinigung anderer solcher Varietäten entsprechen Durchschnitte der zugehörigen Verschwindungsideale. Der (noch zu beweisende) **Hilbertsche Basissatz** sagt aus, dass jedes Ideal in einem Polynomring eine endliche Basis besitzt. Diese Aussage lässt sich in eine geometrische Aussage über die Zerlegung affiner Varietäten in unzerlegbare Teile übersetzen.

AUFGABE 3.7:

Zeigen Sie, dass für einen Ring R die folgenden beiden Aussagen äquivalent sind:

(a) Jedes Ideal $I \subset R$ hat eine endliche Basis.

(b) Es gibt in R keine unendliche echt aufsteigende Kette $I_1 \subset I_2 \subset \ldots$ von Idealen.

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 $I := I(V)$ ist also ein Primideal.

Satz 12 *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

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

Jedes nicht prime Radikalideal ist also Durchschnitt zweier größerer Radikalideale. Nach dem Hilbertschen Basissatz kann ein solcher Zerlegungsprozess nur endlich oft durchgeführt werden, jeder Zweig endet also nach endlich vielen Schritten in einem Primideal. $\square$

Korollar 1 *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, ist also ein maximales Ideal.

4 Gröbnerbasen

4.1 Potenzproduktideale 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 $\mathbf{x}^\alpha = x_1^{a_1} \dots x_n^{a_n}$

Definition: Ein Ideal $I \subset R$ heißt *Potenzproduktideal*, wenn mit $f = \sum c_\alpha \mathbf{x}^\alpha \in I$ auch alle PP $\mathbf{x}^\alpha, c_\alpha \neq 0$ zu I gehören.

Offensichtlich besitzt jedes Ideal mit dieser Eigenschaft eine Basis aus PP. Umgekehrt ist auch ein von PP erzeugtes Ideal ein Potenzproduktideal in diesem Sinne: 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. Potenzproduktideale sind also genau die Ideale, für die man eine Basis und damit auch eine Minimalbasis aus PP angeben kann.

Die Menge $T := T(X) = T(x_1, \dots, x_n)$ aller PP in $(x_1, \dots, x_n)$ bildet bzgl. der Multiplikation ein Monoid. Die Menge aller in einem Potenzproduktideal 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 $\Sigma_0 = \{\mathbf{x}^{a_1}, \dots, \mathbf{x}^{a_m}\}$ 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 $\Sigma = \langle \mathbf{x}^{a_1}, \dots, \mathbf{x}^{a_m} \rangle$.

Satz 13 *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 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 Potenzproduktidealen $I \in \mathcal{MI}(R)$ und den Monoididealen $\Sigma \in \mathcal{O}(T)$, gegeben durch die Zuordnungen

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

Satz 14 *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 Potenzproduktideale in R und der Menge $\mathcal{O}(T)$ der Monoidideale in T sind zueinander invers, wobei für Potenzproduktideale $I_1, I_2 \subset R$*

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 Potenzproduktidealen auf das Rechnen mit Monoididealen zurückgeführt werden, wobei die Rechnungen für Monoidideale oft rein kombinatorischen Charakter haben.

Aufgabe 4.1:

Beweisen Sie diesen Satz und leiten Sie daraus her, dass für Potenzproduktideale $a, b, c \subset R$

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

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

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

Man kann auf diese Weise insbesondere für Potenzproduktideale 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 4.2:

> Finden Sie eine allgemeine Formel für die Erzeugenden des Durchschnitts zweier Potenzproduktideale.

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

Satz 15 *(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 $C := \bigcup_{l \le m} C_l \subset I$ 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

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

abgeleitet, diese als Ersetzungsregeln aufgefasst und damit

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

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 16 *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. □

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 4.3:

Die folgende Aufgabe gibt eine Charakterisierung von allgemeinen 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: $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$

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

AUFGABE 4.4:

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 Potenzproduktideal 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 $f \equiv f'$ $(mod\ I(B))$ und $f' = 0$ oder $lt(f') \notin \Sigma(B)$.

```
while (f ≠ 0) and (M := {b ∈ B : lt(b) | lt(f)} ≠ ∅) do         choose b ∈ M
        f := f − (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

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

Ähnlich wie im Erweiterten Euklidschen Algorithmus kann man den Normalform-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,...,m do v_i := 0 while (f ≠ 0) and (M := {b ∈ B : lt(b) | lt(f)} ≠ ∅) do
        choose b_i ∈ M
        f := f − (lm(f)/lm(b_i)) b_i
        v_i := v_i + 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

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

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 17 *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 4.5:

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 18 *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 Potenzproduktideale 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 Potenzproduktideal $Lt(I) \subset R$ 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 19 *(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 20 *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 2 *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 bgzl. $\Sigma(G) = \Sigma(I)$ 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:

$$s_{14} = z^2 f_1 - u f_4 = (uxz^2 - y^2z^2) - (uxz^2 - uy^3) = uy^3 - y^2z^2$$

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

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

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 21 *(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 $N(G) := T(X) \setminus \Sigma(G)$ sind linear unabhängig (mod I).*
8. *Die Standardterme $N(G)$ bilden eine Vektorraumbasis des Faktorrings R/I, d.h. jedes Element $f \in R$ besitzt eine eindeutige Darstellung*
$$f \equiv \sum_{m \in N(G)} c_m m\ (mod\ I)$$
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

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

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 $N(G)$.

□

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 22 *(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;`
$P := \{(f_i, f_j) \mid 1 \leq i < j \leq m\}$; `While` $P \neq \emptyset$ `do` `Choose` $p \in P$; $P := P \setminus \{p\}$;
  $f := NF(S(p), G)$
  `if` $f \neq 0$ `then`
    $P := P \cup \{(g, f) \mid g \in G\}$;
    $G := G \cup \{f\}$; `return G;`

Satz 23 *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 24 *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 Beispiele für Gröbnerbasisberechnungen in den wichtigsten CAS

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.

Wir wollen jeweils das Polynomsystem

$$F = [x^2 - 2\,x\,z + 5, x\,y^2 + y\,z^3, 3\,y^2 - 8\,z^3]$$

untersuchen, Gröbnerbasen bzgl. verschiedener Termordnungen (deglex und pure lex) bestimmen und die Normalform von

$$p = 320\,x\,y^2 + 9\,x\,y^4 - 96\,z^2\,y^4\,x + 1600\,y^3 - 18\,y^5\,x\,z - 592\,x\,z\,y^3 + 45\,y^5 + 240\,z\,y^4$$

und

$$q = x^3y^3z^3$$

bestimmen.

Maple V.5

Maples Gröbnerpaket `Groebner` wurde mit der Version V.5 gründlich überarbeitet und erweitert. Die Syntax des neuen Pakets stimmt an einigen Stellen nicht mehr mit der des alten Pakets `grobner` überein. Das Paket ist explizit zu laden.

Gröbnerbasis von F bzgl. der degrevlex-Ordnung:

```
with(Groebner);
F := [x^2 - 2*x*z + 5, x*y^2 + y*z^3, 3*y^2 - 8*z^3];
TO := tdeg(x,y,z);
G := gbasis(F,TO);
```

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

und dann die Normalformen von p und q bzgl. G

```
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;
q:=x^3*y^3*z^3;
reduce(p,G,TO);
reduce(q,G,TO);
```

$$0$$

$$1469184\, y^3 z^2 - 362565\, z y^3 + 950640\, z^2 y^2 - 1879680\, y^3 + 9909760\, z y^2 - 1215300\, y^2$$

Gröbnerbasis von F bzgl. einer lexikographischen Ordnung:

```
TO := plex(x,y,z);
G1 := gbasis(F,TO);
```

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

Die Leitterme sind schlecht zu sehen:

$$z^9, y z^3, y^2, x z^3, x^2$$

Die erste Gleichung kann zur Berechnung der z-Komponente der Nullstellen verwendet werden: $z = 0$ oder $1600 + 240\, z^3 - 96\, z^5 + 9\, z^6 = 0$.

Für jeden der beiden Zweige erhalten wir mit

```
inter_reduce([z,op(G1)],TO);
```

$$[z, y^2, x^2 + 5]$$

und

```
gbasis([1600+240*z^3-96*z^5+9*z^6,op(G1)],TO);
```

$$[1600 + 240\, z^3 - 96\, z^5 + 9\, z^6,\ 32\, z^4 + 80\, y - 40\, z^2 - 3\, z^5,\ 640\, x + 9\, z^5 - 96\, z^4 + 120\, z^2]$$

je eine Basis mit Leittermen z, y^2, x^2 bzw. z^6, y, x.

```
gsolve(F,{x,y,z});
```

berechnet diese Gröbnerbasen ebenfalls, indem es einen Algorithmus anwendet, der den Buchberger-Algorithmus mit Faktorisierung verbindet.

Für q erhalten wir bzgl. dieser anderen Termordnung auch eine andere Normalform:

```
reduce(p,G1,TO);
```

$$-46992\, z^8 + 120855\, z^6 + 7200\, z^5 + 76800\, z^4 + 11520\, z^7 + 801200\, z^3$$

Mathematica 4.0

Die Möglichkeiten zur Berechnung von Gröbnerbasen sind seit der Version 3.0 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 und

`GroebnerBasis[PolyList, xVars, yVars]` berechnet aus der Idealbasis `PolyList` die Gröbnerbasis bzgl. einer Ordnung, die `yVars` eliminiert.

Andere Termordnungen kann man über die Option `MonomialOrder` einstellen.

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. Allein die Normalform erhält man mit `PolynomialReduce[Poly,PolyList, xVars]//Last`

Führen wir dieselben Berechnungen wie oben durch:

```
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]
```

Dabei wird standardmäßig die Gröbnerbasis bzgl. der lexikographischen Ordnung bestimmt

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

```
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
q = x^3*y^3*z^3
PolynomialReduce[p,G,vars]//Last
PolynomialReduce[q,G,vars]//Last
```

$$0$$

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

Das Ergebnis der Normalformberechnung unterscheidet sich von dem Maple-Ergebnis um den skalaren Faktor $\frac{243}{64}$.

Eine Gröbnerbasis und Normalformen unter `deglex` bekommt man mit den Aufrufen

```
H = GroebnerBasis[F,vars,MonomialOrder->DegreeLexicographic]
PolynomialReduce[p,H,vars,MonomialOrder->DegreeLexicographic]//Last
PolynomialReduce[q,H,vars,MonomialOrder->DegreeLexicographic]//Last
```

MuPAD

MuPADs Groebner-Paket greift intern auf den Datentyp `poly` zu, hat aber eine Schnittstelle, die diese Umwandlung gegebenenfalls automatisch vornimmt (dafür wird, dem objektorientierten Ansatz von MuPAD folgend, der Typ der Eingabeparameter ausgewertet).

```
export(groebner);
F := [x^2 - 2*x*z + 5, x*y^2 + y*z^3, 3*y^2 - 8*z^3];
G := gbasis(F,DegreeOrder);
```

oder, wenn man explizit auf die Ordnung der Variablen Einfluss nehmen will:

```
vars := [x,y,z];
F1 := map(F,poly,vars);
G1 := gbasis(F1,DegreeOrder);
G  := map(G1,expr);
```

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

Ähnlich kann man die Normalformen berechnen

```
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;
q:=x^3*y^3*z^3;
normalf(p,G,DegreeOrder);
normalf(q,G,DegreeOrder);
```

$$0$$

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

und in lexikographischer Ordnung

```
G := gbasis(F,LexOrder);
```

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

```
normalf(p,G,LexOrder);
normalf(q,G,LexOrder);
```

$$0$$

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

Reduce 3.7

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 von mir 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.

Im Paket `groebner` berechnen die Funktionen `groebner(PolyList,VarList)` eine (lex.) Gröbnerbasis und `preduce(Poly,GBasis)` die totale Normalform eines gegebenen Polynoms. Für unser Beispiel können die Testrechnungen wie folgt ausgeführt werden:

```
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);
```

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

```
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;
q:=x^3*y^3*z^3;
preduce(p,G);
preduce(q,G);
```

$$0$$
$$\frac{-3007488\,z^8 + 737280\,z^7 + 7734720\,z^6 + 460800\,z^5 + 4915200\,z^4 + 51276800\,z^3}{243}$$

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:

```
torder gradlex;
G := groebner(F,vars);
```

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

```
preduce(p,G);
preduce(q,G);
```

$$0$$
$$\frac{23506944\,y^3\,z^2 - 5801040\,y^3\,z - 30074880\,y^3 + 15210240\,y^2\,z^2 + 158556160\,y^2\,z - 19444800\,y^2}{243}$$

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

`setring(vars,WeightList,tag)` definiert einen 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)` weist einer Liste `PolyList` von Polynomen eine Variable `Name` zu, unter der bereits berechnete Ergebnisse gespeichert werden. Diese Zuweisung löscht zugleich früher (unter einer anderen Termordnung) berechnete Zwischenergebnisse.

`gbasis(Name);` berechnet eine Gröbnerbasis über dem vereinbarten Grundring.

`Poly mod GBasis;` berechnet eine totale Normalform.

Typische Vereinbarungen sind

```
load(cali);
setring(vars,degreeorder vars,revlex);
setideal(F,F);
G:=gbasis F;
```

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

```
p mod G;
q mod G;
```

$$0$$

$$\frac{23506944\,y^3\,z^2-5801040\,y^3\,z-30074880\,y^3+15210240\,y^2\,z^2+158556160\,y^2\,z-19444800\,y^2}{243}$$

Die Zerlegung von F durch eine Mischung von Gröbneralgorithmus und Faktorisierung kann man mit `cali` berechnen über

```
setring(vars,{},lex);
groebfactor F;
```

$$\{\{640\,x+9\,z^5-96\,z^4+120\,z^2,\ 80\,y-3\,z^5+32\,z^4-40\,z^2,\ 9\,z^6-96\,z^5+240\,z^3+1600\},$$

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

Mit

```
setcalitrace 30;
```

oder einer anderen Zahl kann man sich schließlich Zwischenergebnisse anzeigen lassen und soden Fortgang der Rechnungen (insbesondere den Stand der S-Polynom-Berechnung) beobachten.

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;
```

bzw. zwei Ideale auf Gleichheit prüfen

EqualIdeal(A,B: Basis): Boolean

Input: Idealbasen $A, B \subset R$

Output: true $\Leftrightarrow$ $I(A) = I(B)$

```
return SubIdeal(A,B) and SubIdeal(B,A);
```

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 25 *Gegeben sei ein polynomiales Gleichungssystem $B \subset R = k[x_1, \ldots, x_n]$ 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 (bzgl. der Lex. Termordnung mit $x > y$)

$$\begin{aligned}
f_4 &= NF(S(f_1, f_2), f_{1\ldots3}) = x\,y^2 - 2\,x - y^3 + 3 \\
f_5 &= NF(S(f_1, f_4), f_{1\ldots4}) = 2\,x\,y - 3\,x + 2\,y^4 - 4\,y^2 - 3\,y + 4 \\
f_6 &= NF(S(f_4, f_5), f_{1\ldots5}) = x - 4\,y^5 - 6\,y^4 + 4\,y^3 + 18\,y^2 + y \\
f_7 &= NF(S(f_1, f_6), f_{1\ldots6}) = 2\,y^6 - 6\,y^4 - 6\,y^3 + 12\,y^2 + 1 \\
f_8 &= NF(S(f_1, f_3), f_{1\ldots7}) = y^4 - 2\,y^2 \\
f_9 &= NF(S(f_4, f_8), f_{1\ldots8}) = 2\,y^3 - 3\,y^2 \\
f_{10} &= NF(S(f_8, f_9), f_{1\ldots9}) = y^2 \\
f_{11} &= NF(S(f_4, f_{10}), f_{1\ldots10}) = 2y + 3 \\
f_{12} &= NF(S(f_{10}, f_{11}), f_{1\ldots11}) = 1
\end{aligned}$$

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

Aufgabe 4.6:

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.

Ähnlich kann man auch prüfen, 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. Im Allgemeinen ist es schwierig, die Basis von $rad(I)$ zu berechnen. Wir verwenden statt dessen die Äquivalenz

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

die wir im Zusammenhang mit Hilberts Nullstellensatz über den Rabinowitsch-Trick bewiesen hatten. t ist hierbei eine neue Variable.

Beispiel: Sei I das von der Basis

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

erzeugte Ideal und $f = x\,z - y^2$.

Es gilt $f \in rad(I)$ genau dann, wenn das Ideal $I + (1 - f\,t)$ trivial ist. Dazu berechnen wir die Gröbnerbasis von

$$\{-t\,x\,z + t\,y^2 + 1,\ -x^2\,z^2 + x\,y^2\,z + x\,z^2 - y^2\,z,\ -x\,y\,z + x\,z^2 + y^3 - y^2\,z,\\ x^3\,y - x^2\,z - x\,y\,z + z^2,\ x^4 - x^2\,y - x^2\,z + y\,z,\ -x^3\,z + x^2\,y^2 + x\,z^2 - y^2\,z\}$$

Diese ist in der Tat trivial. Alternativ hätten wir in diesem Fall $f^2 \in I$ mit dem Normalformalgorithmus zeigen können.

4.10 Polynomsysteme mit endlich vielen Nullstellen

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 26 *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 4.7:

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

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

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 in [1][?] zur Suche nach einem konditionierten Extremum über die Methode der Lagrange-Faktoren aufgestellt wird.

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

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

eine Gröbnerbasis des r-ten Eliminationsideals von I.

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

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

d.h. $G \cap R_r = \{g \in G \mid lt(g) \in T_r\}$ 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 5.1:

(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 5.2:

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 28 *(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 Implizite Darstellung regulär parametrisierter Varietäten

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 $x_i = \phi_i(t_1, \ldots, t_d)$, $i = 1, \ldots, n$. Dann gilt $I(V) = Ker\,\phi^*$, wobei ϕ^* durch die Substitutionen $x_i \mapsto \phi_i(t_1, \ldots, t_d)$, $i = 1, \ldots, n$ induziert wird. Es stellt sich heraus, dass man das Verschwindungsideal $I(V)$ ebenfalls als Eliminationsideal interpretieren kann.

Satz 29 *(Implizite Darstellung regulär parametrisierter Varietäten)*
Sei I das Ideal $I(x_i - \phi_i(\mathbf{t}),\ i = 1, \ldots, n)$ im Polynomring $k[\mathbf{x}, \mathbf{t}]$. Dann kann man das Verschwindungsideal $I(V)$ 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

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

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. Als Gröbnerbasis bzgl. der entsprechenden lexikographischen Termordnung erhalten wir

$$\begin{aligned}
&\{u^2 - x^2 + y,\\
&t + u - x,\\
&4\,x^3\,z - 3\,x^2\,y^2 - 6\,x\,y\,z + 4\,y^3 + z^2,\\
&2\,u\,x\,z - 2\,u\,y^2 + 2\,x^2\,z - x\,y^2 - y\,z,\\
&u\,x\,y - u\,z - x^2\,y - x\,z + 2\,y^2,\\
&2\,u\,x^2 - 2\,u\,y - 2\,x^3 + 3\,x\,y - z,\\
&2\,u\,y^3 - 2\,u\,z^2 - 4\,x^2\,y\,z + x\,y^3 - 2\,x\,z^2 + 5\,y^2\,z\}
\end{aligned}$$

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

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

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 $V(h)$ wirklich zu T gehören, indem wir entsprechende Parameter (t, u) finden. Für $X_0 = (x_0, y_0, z_0) \notin V(x\,z - y^2, x\,y - z, x^2 - y, y^3 - z^2)$

können wir eine der linearen Gleichungen nach u auflösen. Sind $u\,g_1 - f_1, u\,g_2 - f_2 \in I$ zwei unterschiedliche solche Formeln, so gilt $g_2(u\,g_1 - f_1) - g_1(u\,g_2 - f_2) = f_2 g_1 - f_1 g_2 \in I \cap k[X] = I(T)$. Folglich ergibt sich aus zwei unterschiedlichen Gleichungen $u_1(X) = f_1(X)/g_1(X)$ und $u_2(X) = f_2(X)/g_2(X)$ für $X = X_0$ derselbe Wert für u, 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 Die Gröbnerbasis `GBasis`$(\{x - t^2, y - t^3, z - t^4\})$ bzgl. einer Ordnung, die t eliminiert:

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

Das Eliminationsideal hat damit die Basis

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

Aufgabe 5.3:

> 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) $E_2 := \{(s^4, s^3 t, s t^3, t^4) \mid s, t \in \mathbf{C}\}$
> (3) $E_3 := \{(s^5, s^4 t + t^5, s^2 t^3, s t^4) \mid s, t \in \mathbf{C}\}$

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 λP zu E_i. Der Schnitt dieser Fläche mit der Hyperebene $(w = 1)$ 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 5.4:

> Zeigen Sie, dass die gegebenen Basen sogar Gröbnerbasen bzgl. jeder nur denkbaren Termordnung, d.h. *universelle Gröbnerbasen* sind.

Offensichtlich ist $f = x^3 - x^2 y - x y^2 + y^3 \in I_1 \cap I_2$, 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.

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

Satz 30 *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 Gröbnerbasis von B'

$$\{x^2\,y^2 - y^4,\; t\,x\,y^2 - t\,y^3,\; x^3 - x^2\,y - x\,y^2 + y^3,\; t\,x^2\,y - t\,y^3 - x^2\,y + y^3\}$$

Dies liefert den Idealdurchschnitt

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

AUFGABE 5.5:

Berechnen Sie den Idealdurchschnitt

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

AUFGABE 5.6:

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 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. $\square$

5.6 Implizite Darstellung rational parametrisierter Varietäten

Gegeben ist eine Varietät

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

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 zunächst 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 $V = im\,\phi$ und $I(V) = Ker\,\phi^*$ gilt. ϕ^* ist hierbei die 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 wie im Fall regulärer Parametrisierungen in Etappen zerlegen, jedoch noch eine Zusatzvariable y einfügen und mit der polynomialen Substitution $\psi_1 :\; x_i \mapsto f_i \cdot y$ und der rationalen Substitution $\psi_2 :\; y \mapsto 1/g$ arbeiten.

$$k[X] \xrightarrow{\psi_1} k[T, y] \xrightarrow{\psi_2} k(T)$$

Sei $B = \{x_1 - f_1(T)\, y,\; x_2 - f_2(T)\, y,\; \ldots\;,\; x_n - f_n(T)\, y\}$. Dies ist nach dem Hauptsyzygienkriterium eine Gröbnerbasis in $k[X, T, y]$ bzgl. einer Termordnung mit $X \gg y, T$ und für $F(x_1, \ldots, x_n) \in k[X]$ gilt

$$\tilde{F} := \psi_1(F) = F(f_1 y, \ldots, f_n y) = \mathrm{NF}(F(x_1, \ldots, x_n), B).$$

Da $\phi^*(F) = \psi_2(\tilde{F})$ und $\tilde{F} \in k[T, y]$, gilt weiter

$$F \in Ker\,\phi^* \quad \Leftrightarrow \quad \tilde{F} \in Ker\,\psi_2.$$

Berechnen wir deshalb zuerst $Ker\,\psi_2$. 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

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

Wegen

$$(g\,y)^n = ((g\,y - 1) + 1)^n \equiv 1 \ mod\ I(g\,y - 1)$$

gilt schließlich auch

$$p(T, y) \equiv (g\,y)^n p(T, y) \equiv 0 \ mod\ I(g\,y - 1)$$

und somit $Ker\,\psi_2 = I(g\,y - 1)$.

Also gilt

$$F \in Ker\,\phi^* \quad \Leftrightarrow \quad \mathrm{NF}(\mathrm{NF}(F, B), (g\,y - 1)) = 0.$$

Wir haben damit folgenden Satz bewiesen:

Satz 32 *(Implizite Darstellung 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 5.7:

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

$$R_S := \left\{ \frac{f}{s} \mid f \in R,\ s \in S \right\}$$

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.

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.