Gröbnerbasen und Anwendungen
Sommersemester 2017
Notizen zur Vorlesung

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

3. Juli 2017

1 Einführung

1.1 Lineare Gleichungssysteme

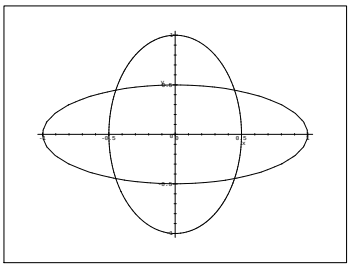
Kurze Wiederholung zum Lösen linearer Gleichungssysteme, gegeben in Matrixschreibweise als $A \cdot \mathbf{x} = \mathbf{b}$ mit $(m \times n)$-Matrix A mit Einträgen aus einem Körper k.

- Vektorraum $Z(A) \subset k^n$ der Zeilen der Matrix A.
- Entscheidend für die Dimension des Lösungsraums ist nicht m, sondern der Rang $r = \mathrm{rk}(A) = \dim_k(Z(A))$.
- Das homogene Gleichungssystem ($\mathbf{b} = 0$) hat stets wenigstens die triviale Lösung. Der Lösungsraum L ist ein Untervektorraum von k^n der Dimension $\dim_k(L) = n - r$.
- Ein inhomogenes Gleichungssystem ist genau dann lösbar, wenn der Rang der Koeffizientenmatrix mit dem Rang der erweiterne Koeffizientenmatrix übereinstimmt.
- Die allgemeine Lösung eines inhomogenen Gleichungssystems setzt sich zusammen aus einer speziellen Lösung des inhomogenen Systems und der allgemeinen Lösung des homogenen Systems. In diesem Sinne *parametrisiert* die allgemeine Lösung des homogenen Systems die allgemeine Lösung des inhomogenen Systems.
- Mit dem Gaussverfahren auf den Zeilen von A kann man A in eine Matrix A' transformieren, aus der die allgemeine Lösung (des homogenen Systems) unmittelbar ermittelt werden kann.
- Dabei werden nur arithmetische Operationen in k ausgeführt. Das Ergebnis ist also über k definiert.
- Es gilt $A' = F \cdot A$ für eine invertierbare Matrix F. Es gilt also auch $A = F^{-1} \cdot A'$.
- Ist $m = n = r$, also $\det(A) \neq 0$, so hat das Gleichungssystem $A \cdot \mathbf{x} = \mathbf{b}$ stets eine eindeutig bestimmte Lösung $\mathbf{x} = A^{-1}\mathbf{b}$

1.2 Nichtlineare Gleichungssysteme. Ein Beispiel

Beispiel 1: Ein pseudolineares Gleichungssystem

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

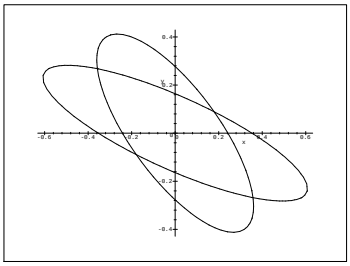


Lösungsmenge

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

Gleichungssystem nach Koordinatentransformation

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



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

Klassisches Eliminationsverfahren der linearen Algebra hilft nicht mehr weiter.

$$37\cdot(1) - 13\cdot(2) \;:\; 525\,x^2 + 450\,x\,y = 24$$

Nun sind alle „höchsten Terme“ paarweise verschieden. Hier kann man zur Not nach y auflösen

$$y = -\frac{175\,x^2 - 8}{150\,x},$$

in eine der Ausgangsgleichungen einsetzen

$$\frac{203125\,x^4 - 10000\,x^2 + 832}{22500\,x^2} = 1$$

und dann nach x auflösen. Ist eine (biquadratische) Gleichung 4. Grades in x

$$\left\{\left\{x = \frac{2}{25}\sqrt{5}\right\}, \left\{x = -\frac{2}{25}\sqrt{5}\right\}, \left\{x = \frac{4}{25}\sqrt{5}\right\}, \left\{x = -\frac{4}{25}\sqrt{5}\right\}\right\}$$

Lösungsmenge ist aber auch so bekannt:

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

Schlussfolgerungen:

- Im Zuge der Elimination treten auf natürliche Weise nichtlineare Gleichungen in einer Variablen auf.

- Der Grad einer solchen Gleichung kann höher sein als der Grad der Ausgangsgleichungen.
- Mit dem Lösen solcher nichtlinearer Gleichungen wird der Bereich der Polynome verlassen. Damit erhöht sich die Komplexität der Rechnungen.

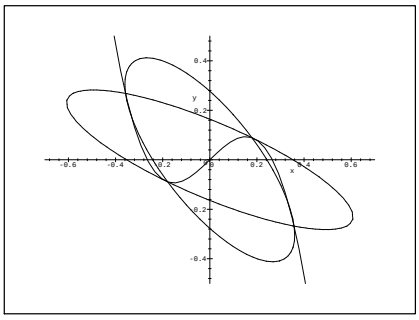
Es ergibt sich die Frage, ob es auch für nichtlineare Gleichungssysteme Eliminationsverfahren gibt, die so lange wie nur möglich mit Polynomen rechnet. In unserem Beispiel müsste das folgende Ergebnis herauskommen:
Lösungsmenge hat paarweise verschiedene x-Werte. Das sind die Nullstellen des Polynoms

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

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



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

umwandeln in

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

Beide Gleichungssysteme sind sogar äquivalent:

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

mit

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

und

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

Allerdings gilt nicht wie im linearen Fall $M_2 = M_1^{-1}$, sondern nur

$$M_1 M_2\,\mathbf{g} = \mathbf{g} \text{ und } M_2 M_1\,\mathbf{f} = \mathbf{f}.$$

1.3 Folgerungen

Wir benötigen

- polynomiale statt skalare Linearkombinationen,
- Ringe statt Vektorräume und
- Ideale statt Unterräume.

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

2 Grundlagen

2.1 Ringe, Ideale und Faktorringe

Definition Ring $(R, +, *)$.

Alle Ringe in diesem Kurs sind kommutativ mit 1.

$u \in R$ heißt *Einheit*, wenn es $u' \in R$ mit $u\,u' = u'\,u = 1$ gibt. Die Menge aller Einheiten bildet eine multiplikative Gruppe R^*.

Ein Ring heißt *Körper*, wenn alle $a \in R, a \neq 0$ Einheiten sind.

Beispiele für Körper: $\mathbb{R}, \mathbb{Q}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$\mathbb{Z}$ ist kein Körper, es gilt $\mathbb{Z}^* = \{+1, -1\}$.

Eine operationstreue Abbildung $\phi : R \longrightarrow R'$ zwischen zwei Ringen R und R' bezeichnet man als *Ringhomomorphismus*.

Definition 1 *Eine Teilmenge $I \subset R$ eines Rings 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 $B = \{f_1, f_2, \ldots, f_m\} \subset R$ muss also auch jede R-lineare Kombination von Elementen aus B zu I gehören.

Definition 2 *Wir bezeichnen die Menge*

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

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.

Sei $\phi : R \to R'$ ein Ringhomomorphismus.

Ist $I' \subset R'$ ein Ideal in R', so ist das Urbild $I = \phi^{-1}(I')$ ein Ideal in R. Dieses Ideal bezeichnet man auch als den *Rückschnitt* von I nach R (vgl. spezielle Situation, wenn ϕ eine Ringeinbettung ist).

Ist $I \subset R$ ein Ideal in R, so ist $\phi(I)$ nicht unbedingt ein Ideal in R' (Beispiel: Ideale unter der Einbettung $\mathbb{Z} \to \mathbb{Q}$). Allerdings kann man $I' = I(\phi(I))$, das von $\phi(I)$ erzeugte Ideal, betrachten. Dies ist das kleinste Ideal, welches $\phi(I)$ enthält, und wird als *Erweiterungsideal* bezeichnet.

Definition 3 *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.

$$B_2 = \left\{x_1 + x_3,\ x_1^2 + x_2,\ x_1x_2,\ x_1^3 + x_1\right\}$$

und

$$B_3 = \left\{x_1 + x_3,\ x_1^2 + x_2,\ x_1x_2,\ x_1(x_1^2x_3 + x_1^2 + x_3 + 1),\ x_1x_3(x_1^2 + 1)\right\}$$

erzeugen alle dasselbe Ideal, denn z. B. gilt

$$(x_1^2 + x_2)\, x_1 - x_1x_2 = x_1^3.$$

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

$$f \equiv g \pmod{I} \ :\Leftrightarrow\ f - g \in I.$$

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

Man überzeugt sich leicht davon, dass diese Relation eine Äquivalenzrelation ist, womit wir entsprechende Äquivalenzklassen bilden können, die wir auch als *Restklassen* $\pmod{I}$ bezeichnen.

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

$$\begin{aligned} f_1 &\equiv g_1 \pmod{I} \\ f_2 &\equiv g_2 \pmod{I} \end{aligned}$$

gilt nämlich auch

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

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. Die natürliche Abbildung $\pi : R \longrightarrow S$, die jedem Polynom die zugehörige Restklasse zuordnet, ist dann ein Ringhomomorphismus. Sie erzeugt eine eineindeutige Abbildung

$$\pi^{-1} : Ideale(S) \longrightarrow Ideale(R)$$

zwischen den Idealen von S und denen von R, die $I = \pi^{-1}(0)$ umfassen.

2.2 Polynomringe

Als *Term* bezeichnet man ein Potenzprodukt

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$$

Die Menge aller Terme

$$T = T(\mathbf{x}) = T(x_1, \ldots, x_n) = \{\mathbf{x}^\alpha \ : \ \alpha \in \mathbb{N}^n\}$$

ist eine Halbgruppe mit $1 = \mathbf{x}^0$ bzgl. der üblichen Multiplikation, das *Term-Monoid*.

$|\alpha| = \alpha_1 + \ldots + \alpha_n$ bezeichnet man als den *Totalgrad* des Terms $\mathbf{x}^\alpha$ (bzgl. der Standardgraduierung).

Sei k ein Körper. Als *Polynom* in $x_1, \ldots, x_n$ über k bezeichnet man jede endliche k-lineare (mit $c_\alpha \in k$) Kombination von Termen $f = \sum c_\alpha \mathbf{x}^\alpha$. Einen einzelnen Summanden $c_\alpha \mathbf{x}^\alpha$ bezeichnen wir auch als *Monom*. Beachten Sie, dass in der Literatur die Bezeichnung Term und Monom unterschiedlich verwendet wird.

Beispiel: $2\,x^3y^2z + \frac{3}{2}\,y^3z^3 - 3\,x\,y\,z + y^2 \in \mathbb{Q}[x, y, z]$.

Die Polynome in $x_1, \ldots, x_n$ über k bilden einen Ring, den Polynomring $R = k[x_1, \ldots, x_n]$.

Die Darstellung $f = \sum c_\alpha \mathbf{x}^\alpha$ für $f \in R$ kann in den meisten CAS aus allgemeineren Darstellungen polynomialer Ausdrücke durch `expand` gewonnen werden. Diese Darstellung ist eindeutig, d.h. eine kanonische Form für Polynome $f \in R$, wenn für die Koeffizienten, also die Elemente aus k, eine solche kanonische Form existiert und die Reihenfolge der Summanden festgelegt ist.

Jedes Ideal in einem Polynomring hat eine endliche Basis.

Satz 1 *Für einen Ring R sind die folgenden beiden Bedingungen äquivalent:*

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

(b) Jede aufsteigende Kette $I_1 \subset I_2 \subset \ldots$ ist endlich, d.h. $\exists N \forall n > N : I_N = I_n$.

Beweis: $(a) \Rightarrow (b)$: Betrachte $I = \cup_{k=1}^{\infty} I_k$. Das ist wieder ein Ideal und nach (a) endlich erzeugt. Ist $B = \{f_1, \ldots, f_s\}$ ein Erzeugendensystem für I, $f_i \in I_{k_i}$ und $k = \max(k_i)$, so ist $B \subset I_k$ und damit $I_k = I_{k+1} = \cdots = I$.

$(b) \Rightarrow (a)$: Wähle nacheinander $f_1, f_2, \cdots \in I$, so dass $f_i \notin I_{i-1} = I(f_1, \ldots, f_{i-1})$. Die I_k bilden eine aufsteigende Kette, die nach b endlich ist. Das Verfahren bricht also mit einem endlichen Erzeugendensystem für I ab. $\square$

Definition 4 *Ringe mit dieser Eigenschaft heißen* Noethersche Ringe.

Der Polynomring $R = k[x_1, \ldots, x_n]$ über einem Körper k ist stets ein Noetherscher Ring. Ideale in R haben also stets endliche Erzeugendensysteme. Dies ergibt sich aus dem folgenden Satz:

Satz 2 (Hilberts Basissatz) *Ist R ein Noetherscher Ring, so auch $R[x]$.*

Beweis: Wir zeigen, dass ein Ideal $I \subset R[x]$ ein endliches Erzeugendensystem hat und betrachten dazu

$$C_n = \left\{ r \in R \ : \ \exists f = rx^n + \sum_{i=0}^{n-1} a_i x^i \in I \right\}.$$

Das ist eine aufsteigende Kette von Idealen in R und deshalb existiert ein N, so dass $C_N = C_n$ für alle $n > N$ gilt.

Nimm Erzeugende $a_{ij} \in R$ für die Ideale C_i, $i = 1, \ldots, N$ und die zugehörigen Polynome

$$f_{ij} = a_{ij}x^i + < \text{kleinere Terme} > .$$

Diese erzeugen ein Ideal I'. Wir zeigen $I = I'$.

Beweis für $f \in I$ mit Induktion nach dem Grad.

Induktionsanfang: $\deg(f) = 0 \Rightarrow f \in C_0$.

Induktionsschritt:
$\deg(f) = i \leq N \Rightarrow r = lc(f) \in C_i$. Dann kann man R als R-lineare Kombination $r = \sum_j r_j a_{ij}$ darstellen. $f' = \sum_j r_j f_{ij} \in I'$ ist dann auch vom Grad i und hat r als Leitkoeffizienten. $f - f'$ ist also in I und vom Grad $< i$, liegt also nach Induktionsvoraussetzung in I'. Damit ist aber auch $f \in I'$.

Genauso geht es für $\deg(f) = i > N$. Dann ist $r = lc(f) \in C_i = C_N$ und $r = \sum_j r_j a_{Nj}$. $f' = \sum_j r_j x^{i-N} f_{ij} \in I'$ ist dann auch vom Grad i und hat r als Leitkoeffizienten. Argumentiere weiter wie im Fall $i \leq N$. $\square$

3 Affine Varietäten

3.1 Der affine Raum

K ein Erweiterungskörper von k. Als *affinen Raum* bezeichnen wir die Menge

$$\mathbb{A}^n_K = \{(a_1, \ldots, a_n), a_1, \ldots, a_n \in K\}$$

$f \in R = k[x_1, \ldots, x_n]$ kann als Funktion $f : k^n \to k$ auf dem Raum $\mathbb{A}^n_k$ aufgefasst werden. Es kann sein, dass f nicht das Nullpolynom ist, aber dennoch auf ganz k^n verschwindet.

Beispiel: $f = x(x-1) \in \mathbb{F}_2[x]$.

Satz 3 *Ist k ein unendlicher Körper und $f \in k[x_1, \ldots, x_n]$. Dann ist f das Nullpolynom genau dann, wenn f auf $\mathbb{A}^n_k$ als Funktion verschwindet.*

Beweis: Mit Induktion nach n. Für $n = 1$ gilt in $k[x]$ der Satz von der Division mit Rest, aus dem folgt, dass man für jede Nullstelle a des Polynoms $f(x)$ eine Zerlegung $f(x) = g(x)\cdot(x-a)$ hat mit $\deg(g) = \deg(f) - 1$. Jedes Polynom hat deshalb nur endlich viele Nullstellen und $\exists\, a \in k : f(a) \neq 0$.

Induktionsschritt: Wir betrachten f als Polynom in $k[x_1, \ldots, x_{n-1}][x_n]$:

$$f = \sum_{i=0}^{d} P_i(x_1, \ldots, x_{n-1}) \cdot x^i$$

Ist f nicht das Nullpolynom, so gibt es einen Koeffizienten P_i, der nicht das Nullpolynom ist und damit nach Induktionsvoraussetzung auch nicht die Nullfunktion auf $\mathbb{A}_k^{n-1}$. Dann existieren aber $a_1, \ldots, a_{n-1} \in k$ mit $P(a_1, \ldots, a_{n-1}) \neq 0$. Damit ist $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ ein univariates Polynom in x_n, das auch nicht das Nullpolynom ist. Wie im Fall $n = 1$ gezeigt bedeutet das die Existenz eines $a_n \in k$, für das $f(a_1, \ldots, a_{n-1}, a_n) \neq 0$ gilt. □

Anmerkung: Das gilt für endliche Körper nicht mehr. Beispiele dazu auch in den Übungsaufgaben.

3.2 Affine Varietäten

$S = k[x_1, \ldots, x_n]$ bezeichnet den Polynomring in $X = (x_1, \ldots, x_n)$ über einem Körper k. K ist der algebraische Abschluss von k. $\mathbb{A}^n := \{(a_1, \ldots, a_n) \,:\, a_i \in K\}$ ist der n-dimensionale *affine Raum* (über K).

Weiter sei $B = \{f_1, \ldots, f_s\} \subset S$ ein (endliches) System von Polynomen, $I = I(B)$ das von B erzeugte Ideal in S und

$$V = V(B) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n \,:\, \forall f \in B\ f(\mathbf{a}) = 0\}$$

deren gemeinsame Nullstellenmenge. Es gilt $V(B) = V(I(B))$.

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

Zu einer beliebigen Teilmenge $V \subset \mathbb{A}^n$ kann man umgekehrt die Menge

$$I(V) := \{f \in S \,:\, f(\mathbf{a}) = 0\ \forall\, \mathbf{a} \in V\}$$

der auf $V \subset \mathbb{A}^n$ verschwindenden polynomialen Funktionen betrachten.

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 $q(a_x) \neq 0$ oder $p(a_x) = q(a_x) = 0$. 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. für $F = x^2+y^2-1$. $V(F)$ ist ein Kreis 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

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

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

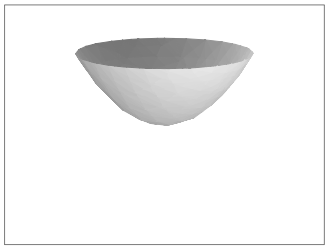
$$x^2 + r^2x^2 + 2\,r^2x + r^2 - 1 = (x+1)\left(x + r^2x - 1 + r^2\right)$$

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.

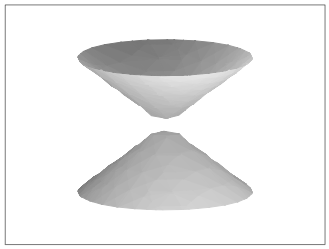
Affine Varietäten im Raum

Nullstellengebilde der Gestalt $V = V(F(x,y,z))$ sind Flächen im Raum wie etwa die folgenden. Die Bilder wurden mit der Funktion `plots[implicitplot3d]` und Maple 8 erzeugt. Mit Maple 2016 hat sich an der Qualität nichts geändert.

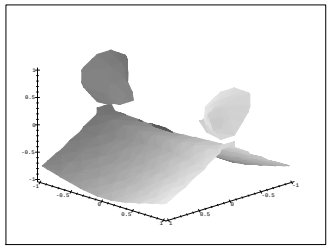
```
with(plots):
implicitplot3d(u1,x=-2..2, y=-2..2, z=-2..2);
```



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



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



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

Auch andere CAS liefern ähnliche Bilder. Besonders am letzten Beispiel wird deutlich, dass Gradientenverfahren, die zur impliziten Darstellungen von Flächen benutzt werden, in der Nähe von Singularitäten wie der Selbstdurchdringung der Fläche längs der y-Achse oder gar in der Nähe der komplizierteren Singularität im Ursprung ihre Schwierigkeiten haben.

Nullstellengebilde im Raum, die sie sich durch zwei Gleichungen beschreiben lassen, ergeben im Normalfall eine Raumkurve.

Beispiel:

$$V = V\left(\{y - x^2, z - x^3\}\right) = \left\{\left(t, t^2, t^3\right) \ : \ t \in K\right\}$$

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 $\mathbb{A}^n$ 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

$$V\left(\{x\,y + y^2 - y, x^2 - x - y^2 + y\}\right),$$

die sich aus den beiden Teilvarietäten $V(\{x + y - 1\})$ und $V(\{x, y\})$ zusammensetzt, d. h. aus einem Punkt und einer Geraden besteht. (Es gilt $x^2 - x - y^2 + y = (x - y)\,(x + y - 1)$ und $x\,y + y^2 - y = y\,(x + y - 1)$).

Ähnlich, aber noch trivialer zu sehen ist das bei $V(x\,z, y\,z) = V(z) \cup V(x, y)$.

3.3 Erste Eigenschaften affiner Varietäten

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

Satz 4 *Eine affine Varietät $V \subset \mathbb{A}^1$ besteht aus dem ganzen $\mathbb{A}^1$ oder endlich vielen Punkten.*

Damit bekommen wir ein notwendiges Kriterium

Satz 5 *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 $\mathbb{A}^1$ beschreiben. □

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

Satz 6

(1) $\emptyset$ und $\mathbb{A}^n$ sind affine Varietäten

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

(3) Ist $V_\alpha \subset \mathbb{A}^n$ 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 $\cap_\alpha V_\alpha = V(\cup_\alpha B_\alpha)$. $\square$

Die affinen Teilvarietäten des $\mathbb{A}^n$ 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 $V \subset \mathbb{A}^n$: Dies ist die kleinste affine Varietät, die V umfasst. Äquivalent:

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

3.4 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 $C = V(x^2 + y^2 - 1)$

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

Hier kann man ebenfalls aus vorgegebenen Koordinaten $P = (x, y) \in C$ den Parameterwert t über die Formeln $t = \frac{y}{1+x}$ für $x \neq -1$ eindeutig rekonstruieren, jedoch erfasst C' den Punkt $(-1, 0)$ auf der Kreislinie nicht. Wir können die Parametrisierung verstehen als Abbildung

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

die durch die beiden rationalen Funktionen gegeben wird, durch die sich die x- bzw. y-Koordinate berechnet. Dann ist $C' = im\ \phi$ und $C = C' \cup \{(-1, 0)\}$. Die Abbildung ϕ ist injektiv.

Sei nun n beliebig und $V \subset \mathbb{A}^n$ eine affine Varietät.

Definition 5 *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*

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

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 6 *Eine Parameterdarstellung mit $q = 1$ heißt* polynomial *oder* regulär. *In dem Fall sind die $r_i(\boldsymbol{t})$ polynomiale Funktionen.*

Wie oben können wir eine solche Parametrisierung stets als Abbildung

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

betrachten, die einem Parametertupel $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{A}^d$ den Punkt

$$\mathbf{c} = \phi(\mathbf{a}) = (r_1(\mathbf{a}), \ldots, \mathbf{r_n}(\mathbf{a})) \in \mathbb{A}^{\mathbf{n}}$$

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 und damit grafische Darstellungen erzeugen.

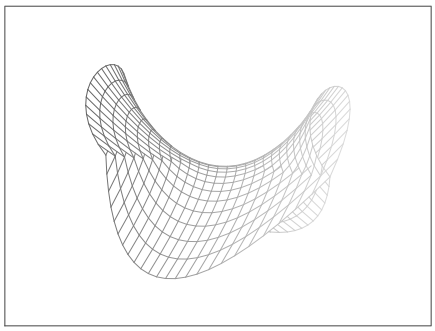
Betrachten wir als Beispiel die „Schweinsohrfläche“ $V = V(x^2 - y^2z^2 + z^3)$.

Setzen wir $y^2 = c$ als Parameter, so erhalten wir eine Schar elliptischer Kurve $x^2 = c\,z^2 - z^3$, zu denen in einer Aufgabe eine Parametrisierung zu finden ist. Diese Parametrisierung

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

kann man zu einer der ganzen Fläche fortsetzen:

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



Hier ist die Parameterrekonstruktion aus $(x, y, z) \in V$ etwas komplizierter: Allgemein ist $u = y$ und $t = x/z$ für $z \neq 0$. Für $z = 0$ ist auch $x = 0$ und aus $z = u^2 - t^2 = 0$ ergeben sich zwei Lösungen $t = \pm u = \pm y$ für t. Das ist aber auch klar, denn die Fläche schneidet sich selbst längs der y-Achse.

Ist $I = I(x - t(u^2 - t^2), y - u, z - (u^2 - t^2))$, so gilt $x \equiv t(u^2 - t^2) \pmod I$, $y \equiv u \pmod I$ und $z \equiv (u^2 - t^2) \pmod I$. Daraus folgt $x^2 - y^2z^2 + z^3 \equiv 0 \pmod I$, also $x^2 - y^2z^2 + z^3 \in I$.

Die Frage, ob ϕ eine injektive Abbildung ist, ist also selbst für den Fall einer regulären Parametrisierung eine komplizierte Frage. Normalerweise kann man Injektivität, wie in diesem Beispiel, nur jenseits einer Ausnahmemenge erreichen, die wie hier selbst wieder eine algebraische Varietät kleinerer Dimension ist. Das werden wir im Closure Theorem beweisen.

Eine *implizite Darstellung* dagegen ist vorteilhaft für Tests, ob gegebene Punkte auf einer Varietät liegen.

Damit entstehen folgende weiteren Fragen:

(1) Umrechnung einer impliziten in eine Parameterdarstellung.

(2) Inverses Problem: Finde Formeln, nach denen aus den Koordinaten eines Punkts auf der Varietät dessen Parameterkoordinaten berechnet werden können.

(3) Finde eine implizite Darstellung einer in parametrisierter Form gegebenen Varietät V. Bestimme also eine Basis von $I(V)$.

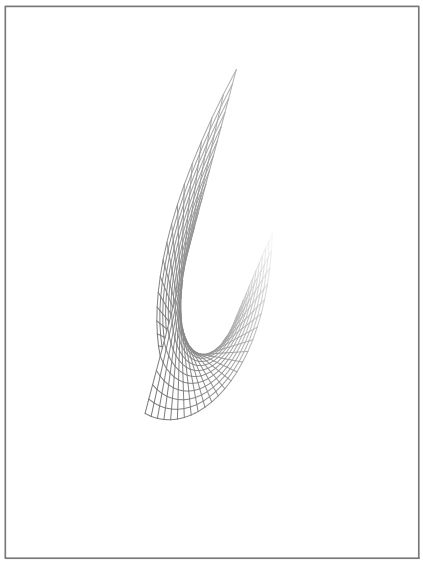
Die zweite und dritte Fragestellung führen auf Eliminationsprobleme. Betrachten wir etwa die Kurve

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

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 $C = V(x^2-2\,x+y)$ sowie die inverse Formel $t = 1-x$ führt. Auch hier ist wieder $x^2-2\,x+y \in I(x-(1-t), y-(1-t^2))$.

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

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



$$F = \left\{\left(t+u, t^2+2\,u\,t, t^3+3\,u\,t^2\right) \,:\, t, u \in K\right\}$$

oder explizit

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

Als inverse Formel ergibt sich unter Verwendung der Lösungsformel für quadratische Gleichungen

$$u = x-t, t = x \pm \sqrt{x^2-y}$$

und insgesamt

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

In diesem Fall stimmen also F und $\overline{F}$ überein. Im Allgemeinen muss die Parametrisierung nicht alle Punkte der Varietät erfassen, d. h. die Menge der durch die Parametrisierung erzeugten Punkte ist nicht unbedingt abgeschlossen. Das kann selbst für reguläre Parametrisierungen auftreten:

Beispiel: Gegeben sei die Fläche $F = \left\{(u\,v, u\,v^2, u^2) \,:\, u, v \in \mathbb{C}\right\}$.

Die Gleichung der Fläche lautet $V = V(x^4 - y^2z^2)$: Es ist $F \subset V$ und für Punkte auf V mit $x, y \neq 0$ kann man mit $u = \frac{x^2}{y}$ und $v = \frac{y}{x}$ auf die Parameter zurückschließen. Damit schöpft F die Varietät V „fast“ aus. Es bleiben die Geraden $x = y = 0$ (z-Achse) und $x = z = 0$ (y-Achse), die beide zu V gehören, zu untersuchen. $x = y = 0$ liegt in F ($v = 0$, u beliebig), von $x = z = 0$ gehört nur der Ursprung zu F.

3.5 Verschwindungsideal regulär parametrisierter Kurven. Beispiele

Wir wollen das Verschwindungsideal $I_2 = I(V)$ der getwisteten Kubik $C_2 = \{(a, a^2, a^3) \,:\, a \in \mathbb{C}\}$ bestimmen. 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 $y \equiv x^2, z \equiv x^3 \pmod J$ und somit

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

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 $f \equiv 0 \pmod J$, d. h. $f \in J$.

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

Weitere Elemente des Verschwindungsideals sind etwa $x^5 - z^2$ oder $y^5 - z^3$. Diese Polynome liegen allerdings bereits in $I(B_3)$, sind also für eine Minimalbasis überflüssig.

Setzen wir wieder $J := I(B_3)$, so können wir mit den Beziehungen $z \equiv x\,y,\ y^2 \equiv x^3 \pmod J$ nur bis zu einer Darstellung $f(x,y,z) \equiv g_1(x) + g_2(x)\cdot y \pmod J$ 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

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

für alle $a \in \mathbb{C}$, 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.

4 Termordnungen

Wir betrachten Ordnungen auf dem Monoid $T(\mathbf{x}) = T(x_1,\ldots,x_n)$. Eine solche Ordnung kann alternativ über die Variante $<$ oder $\leq$ definiert werden, wobei

$$t_1 \leq t_2 \Leftrightarrow t_1 < t_2 \text{ oder } t_1 = t_2$$

gilt, und die folgenden Axiome einer partiellen Ordnung

$$\forall t \in T : t \leq t \qquad \text{(Reflexivität)} \tag{1}$$
$$\forall t_1,t_2 \in T : t_1 \leq t_2 \wedge t_2 \leq t_1 \Rightarrow t_1 = t_2 \qquad \text{(Antisymmetrie)} \tag{2}$$
$$\forall t_1,t_2,t_3 \in T : t_1 \leq t_2 \wedge t_2 \leq t_3 \Rightarrow t_1 \leq t_3 \qquad \text{(Transitivität)} \tag{3}$$

sowie die Vergleichbarkeitsbedingung für je zwei Elemente

$$\forall t_1,t_2 \in T : t_1 \leq t_2 \vee t_2 \leq t_1 \qquad \text{(totale Ordnung)} \tag{4}$$

erfüllt sein müssen.

Als *distributive Darstellung* eines Polynoms $f \in R$ bzgl. einer solchen Ordnung bezeichnet man eine Darstellung $f = \sum_a c_a\,\mathbf{x}^a$, in welcher die Summanden paarweise verschiedene Terme enthalten, diese in fallender Reihenfolge angeordnet sind und die einzelnen Koeffizienten in

ihre kanonische Form gebracht wurden. In dieser Darstellung ist die Addition von Polynomen besonders effizient ausführbar. Gilt darüber hinaus

$$\forall t_1, t_2, t \in T : t_1 \le t_2 \Rightarrow t \cdot t_1 \le t \cdot t_2 \qquad \text{(Monotonie)} \tag{5}$$

so kann man auch die Multiplikation effektiv ausführen, da dann beim gliedweisen Multiplizieren einer geordneten Summe mit einem Monom die Summanden geordnet bleiben. Ordnungen mit dieser Zusatzeigenschaft bezeichnet man als *Termordnungen*. Oft werden als Termordnungen nur wohlfundierte Ordnungen dieser Art bezeichnet.

Wichtige Ordnungen auf $T(\mathbf{x})$, die in praktischen Anwendungen eine Rolle spielen:

- *Lexikographische Ordnung* (lex)

$$x_1^{a_1} x_2^{a_2} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{lex}} x_1^{b_1} x_2^{b_2} \cdot \ldots \cdot {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} a_1 > b_1 & \text{oder} \\ a_1 = b_1 & \text{und } x_2^{a_2} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{lex}} x_2^{b_2} \cdot \ldots \cdot {x_n}^{b_n} \end{cases}$$

- *Revers lexikographische Ordnung* (revlex)

$$x_1^{a_1} \cdot \ldots \cdot {x_{n-1}}^{a_{n-1}} {x_n}^{a_n} >_{\text{revlex}} x_1^{b_1} \cdot \ldots \cdot {x_{n-1}}^{b_{n-1}} {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} a_n < b_n & \text{oder} \\ a_n = b_n & \text{und } x_1^{a_1} \cdot \ldots \cdot {x_{n-1}}^{a_{n-1}} >_{\text{revlex}} x_1^{b_1} \cdot \ldots \cdot {x_{n-1}}^{b_{n-1}} \end{cases}$$

- *Gradordnung* (bzgl. der Standardgraduierung)

$$x_1^{a_1} \cdot \ldots \cdot {x_n}^{a_n} >_{\deg xxx} x_1^{b_1} \cdot \ldots \cdot {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} \deg(\mathbf{a}) > \deg(\mathbf{b}) & \text{oder} \\ \deg(\mathbf{a}) = \deg(\mathbf{b}) & \text{und } x_1^{a_1} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{xxx}} x_1^{b_1} \cdot \ldots \cdot {x_n}^{b_n} \end{cases}$$

- *Gewichtete Gradordnung* bzgl. $w(x_i) = w_i$

$$x_1^{a_1} \cdot \ldots \cdot {x_n}^{a_n} >_{w,xxx} x_1^{b_1} \cdot \ldots \cdot {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} w(\mathbf{a}) > w(\mathbf{b}) & \text{oder} \\ w(\mathbf{a}) = w(\mathbf{b}) & \text{und } x_1^{a_1} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{xxx}} x_1^{b_1} \cdot \ldots \cdot {x_n}^{b_n} \end{cases}$$

  wobei $w(\mathbf{a}) = w_1 a_1 + \cdots + w_n a_n$ ist.

Hier ist *xxx* eine andere Termordnung, nach welcher Terme gleichen Grades geordnet werden. Wichtige Gradordnungen sind insbesondere die *gradweise lexikographische* (deg-lex) und die *gradweise revers lexikographische* (deg-revlex) Termordnung.

Beispiel: Anordnung der Terme vom Grad ≤ 2 für $n = 3$.

Als *wohlfundierte Ordnung*, *Wohlordnung* oder *noethersche Ordnung* bezeichnet man eine totale Ordnung $(T, <)$, in der eine der beiden äquivalenten Bedingungen gilt:

(a) Jede Teilmenge $M \subset T$ hat ein kleinstes Element.

(b) Jede (echt) absteigende Kette $t_1 > t_2 > \ldots$ in T ist endlich.

Während die lexikographische und jede Gradordnung Wohlordnungen sind, gilt dies für die (rein) revers-lexikographische Ordnung nicht: $x_1 > x_1^2 > x_1^3 > \ldots$ ist für diese Termordnung eine unendliche absteigende Kette von Termen.

Satz 7 *Eine Termordnung $(T, >)$ ist genau dann eine Wohlordnung, wenn gilt*

(c) $m \geq 1$ für alle $m \in T$.

Beweis: Wir zeigen die Gültigkeit der Implikationen $(a)\Rightarrow(b)\Rightarrow(c)\Rightarrow(a)$:
$(a)\Rightarrow(b)$: Nimm $M = \{t_1, t_2, \ldots\}$.
$(b)\Rightarrow(c)$: Gäbe es ein $m < 1$, so gilt wegen der Monotonie $m > m^2 > m^3 > \ldots$.
$(c)\Rightarrow(a)$: Sei $M \subset T$ eine Teilmenge ohne minimales Element. Dann können wir eine unendliche Folge von Elementen $m_1 > m_2 > \ldots$ aus M auswählen. Nach dem Dickson-Lemma (Beweis später) existieren $i < j$ mit $m_i \,|\, m_j$, also $m_j = m_i \cdot t$ mit $t \in T$. Wegen $m_j = m_i \cdot t < m_i$ und der Monotonie folgt $t < 1$. $\square$

Charakterisierungssatz für Termordnungen:

Mit $\tilde{T} = \{\mathbf{x}^\alpha : \alpha \in \mathbb{Z}^n\}$ bezeichnen wir die Gruppe der *verallgemeinerten Terme*, deren Exponenten beliebig ganzzahlig sein können.
(1) Jede Termordnung auf T kann man eindeutig auf $\tilde{T}$ ausdehnen:
Für $\alpha, \alpha', \beta, \beta' \in \mathbb{N}^n$ setzen wir

$$\mathbf{x}^{\alpha-\alpha'} < \mathbf{x}^{\beta-\beta'} \Leftrightarrow \mathbf{x}^{\alpha+\beta'} < \mathbf{x}^{\alpha'+\beta}$$

Die Repräsentantenunabhängigkeit dieser Definition folgt aus der Kürzungsregel

$$\mathbf{x}^\alpha \cdot \mathbf{x}^\gamma < \mathbf{x}^\beta \cdot \mathbf{x}^\gamma \Rightarrow \mathbf{x}^\alpha < \mathbf{x}^\beta,$$

die sich für lineare Ordnungen wiederum aus der Monotonie ergibt.
(2) Dann gilt

$$\mathbf{x}^\alpha < \mathbf{x}^\beta \Leftrightarrow 1 < \mathbf{x}^{\beta-\alpha},$$

so dass die Termordnung durch ihren *Positivkegel* $C_+ = \left\{\mathbf{x}^\alpha \in \tilde{T} \;:\; \mathbf{x}^\alpha \geq 1\right\}$ bestimmt wird.
(3) Da die Ordnung eine lineare Ordnung ist, ist der Positivkegel ein Halbraum, der durch ein lineares Funktional $w \in (\mathbb{Z}^n)^* \cong \mathbb{R}^n$ beschrieben werden kann, so dass für $\alpha \in \mathbb{Z}^n$ gilt

$$w(\alpha) > 0 \Rightarrow \mathbf{x}^\alpha > 1$$

und folglich auch (wegen $w(-\alpha) = -w(\alpha)$)

$$w(\alpha) < 0 \Rightarrow \mathbf{x}^\alpha < 1$$

Wir setzen kurz auch $w(\mathbf{x}^\alpha) = w(\alpha)$.

Satz 8 *Zu jeder Termordnung $(T, <)$ gibt es einen Gewichtsvektor $w \in (\mathbb{Z}^n)^* \cong \mathbb{R}^n$, so dass*

$$\boldsymbol{x}^\alpha < \boldsymbol{x}^\beta \Rightarrow w(\alpha) \leq w(\beta)$$

gilt. Ist $(T, <)$ eine noethersche Termordnung, so gilt $w \in \mathbb{R}^n_{\geq 0}$.

Die Aussage über noethersche Termordnungen ergibt sich daraus, dass alle $x^a, a \in \mathbb{N}^n$, zum Positivkegel gehören.

(4) Einzig über Terme $\mathbf{x}^\alpha$ mit $w(\alpha) = 0$ kann allein aus diesem *Gewichtsvektor* w keine Aussage getroffen werden. Diese liegen jedoch in einem linearen Unterraum von $\mathbb{Z}^n$ und wir können für diese Gitterpunkte dieselbe Argumentation mit einem weiteren Gewichtsvektor wiederholen.

(5) Jeder solche Gewichtsvektor ist durch den Zeilenvektor $(w(x_i), i = 1, \ldots, n)$, die *Gewichte der Variablen*, eindeutig bestimmt. Beschränkt man sich auf rationale Gewichte, so kann man alle Gewichte sogar als ganzzahlig annehmen, da sich die durch $w(\alpha) = 0$ beschriebene Gitterebene durch Skalieren nicht ändert. Durch Skalierung auf die Länge 1 kann man die Gewichtsvektoren mit Punkten auf der Sphäre S^{n-1} identifizieren und hat damit auch eine genaue Fassung des Begriffs „nahe beieinander liegender“ Termordnungen.

(6)

Satz 9 (Charakterisierungssatz für Termordnungen)

Jede Termordnung lässt sich durch eine Folge von Gewichtsvektoren $w_1, w_2, \ldots, w_k \in \mathbb{R}^n$ beschreiben, wobei für $\boldsymbol{x}^\alpha, \boldsymbol{x}^\beta \in T$ gilt

$$\boldsymbol{x}^\alpha > \boldsymbol{x}^\beta \Leftrightarrow \exists\, j < k \left(\forall\, i \leq j \;(w_i(\alpha) = w_i(\beta)) \wedge (w_{j+1}(\alpha) > w_{j+1}(\beta))\right)$$

Hierbei ist w_1 bis auf einen positiven skalaren Faktor eindeutig bestimmt, während w_j auch um Vielfache von $w_i,\ i < j$, abgeändert werden kann.

(7) Jede Termordnung lässt sich damit als *Matrix-Termordnung* darstellen, indem die Gewichte der Variablen bzgl. der w_i als Zeilen einer Matrix notiert werden.

Eine Termordnung ist offensichtlich genau dann eine Wohlordnung, wenn der erste Eintrag verschieden Null in jeder Spalte der Gewichtsmatrix positiv ist.

Die Matrizen für die oben beschriebenen noetherschen Termordnungen sind

$$>_{\text{lex}}: \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & 1 \end{pmatrix} \quad >_{\text{deglex}}: \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ & & \ldots & & \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \quad >_{\text{degrevlex}}: \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & -1 & 0 \\ & & \ldots & & \\ 0 & -1 & \ldots & 0 & 0 \end{pmatrix}$$

Beispiele mit CoCoA: Standardordnung ist `degrevlex`, andere Ordnungen können durch Kürzel vereinbart werden. Interne Darstellung erfolgt offensichtlich als Matrixordnung.

```
Use R ::= QQ[x,y,z];
OrdMat(R);
Mat[
  [1, 1, 1],
```

```
  [0, 0, -1],
  [0, -1, 0]
]

Use S::=QQ[x,y,z],Lex;
OrdMat(S);
Mat[
  [1, 0, 0],
  [0, 1, 0],
  [0, 0, 1]
]
```

(8) Ist $B \subset \tilde{T} \setminus \{1\}$ eine endliche Menge verallgemeinerter Terme, so können wir nach der Menge der Gewichtsvektoren

$$W_B = \{w \in \mathbb{R}^n \ : \ \forall \mathbf{x}^\alpha \in B \ w(\alpha) > 0\}$$

fragen, unter denen alle $\mathbf{x}^\alpha \in B$ positiv sind. Wegen $w(\alpha) = w_1 \cdot \alpha_1 + \cdots + w_n \cdot \alpha_n$ ist das der Durchschnitt der (offenen) Halbräume

$$\bigcap_{\mathbf{x}^\alpha \in B} \{w \in \mathbb{R}^n \ : \ w(\alpha) > 0\}\,.$$

Dieser Durchschnitt ist entweder leer oder eine offene Menge (hier kommt die Endlichkeit von B ins Spiel) und damit n-dimensional. Bezeichnet $\Sigma = \Sigma(B)$ den von den Elementen $\mathbf{x}^b \in B$ in $\tilde{T}$ aufgespannten Kegel, so gilt letzteres genau dann, wenn $\mathbf{x}^\alpha \in \Sigma \Rightarrow \mathbf{x}^{-\alpha} \notin \Sigma$ erfüllt ist.

Die entsprechenden Gewichtsvektoren bilden wegen $w_1, w_2 \in W_B \Rightarrow w_1 + w_2 \in W_B$ einen Kegel im $\mathbb{R}^n = (\mathbb{Z}^n)^*$, welcher dual zum Kegel ist, der von den Exponenten der $\mathbf{x}^\alpha \in \Sigma$ aufgespannt wird. W_B ist nicht leer genau dann, wenn Σ einen Kegel mit Spitze aufspannt.

Ist $W_B \neq \emptyset$, so enthält W_B als offene Menge Punkte mit rationalen und sogar ganzzahligen Koordinaten, da mit jedem Gewichtsvektor $w \in W_B$ auch alle positiven skalaren Vielfachen von w zu W_B gehören.

Satz 10 *Ist $B \subset \tilde{T}$ eine* endliche *Menge von Termen, $\Sigma = \Sigma(B)$ der von B in $\tilde{T}$ erzeugte Kegel und $\boldsymbol{x}^\alpha \in \Sigma \Rightarrow \boldsymbol{x}^{-\alpha} \notin \Sigma$, so gibt es einen ganzzahligen Gewichtsvektor $w \in W_B \cap \mathbb{Z}^n$, für den also $\boldsymbol{x}^\alpha \in \Sigma \setminus \{1\} \Rightarrow w(\alpha) > 0$ gilt. Für $B \supset \{x_1, \ldots, x_n\}$ gibt es sogar einen solchen Gewichtsvektor in $W_\Sigma \cap \mathbb{Z}^n_+$.*

Die letzte Behauptung ergibt sich unmittelbar daraus, dass dann $w_i = w(x_i) > 0$ gelten muss.

5 Gröbnerbasen

5.1 Potenzproduktideale, Monoidideale und das Dickson-Lemma

Eine wichtige Klasse von Beispielen, die sich einfach beschreiben lassen, aber trotzdem bereits recht komplizierte Ideale enthalten, sind die von Potenzprodukten erzeugten Ideale (PP-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.

Definition 7 *Ein Ideal $I \subset R$ heißt* Potenzproduktideal*, wenn mit $f = \sum c_\alpha \boldsymbol{x}^\alpha \in I$ auch alle Potenzprodukte $\boldsymbol{x}^\alpha, c_\alpha \neq 0$ zu I gehören.*

Für ein PP-Ideal I ist

$$\Sigma = \Sigma(I) = \{x^\alpha \in T \,:\, x^\alpha \in I\}$$

als Teilmenge von T ein *Monoidideal* (d. h. es gilt $\Sigma \cdot T = \Sigma$). Σ und jede Teilmenge Σ_0, die Σ als Monoidideal erzeugt, ist – nach Definition eines PP-Ideals – auch eine Idealbasis von I.
Beispiel: $I = I(x^4y^2, x^3y^4, x^2y^5)$. Grafische Darstellung im $\mathbb{N}^2$.

Definition 8 *Eine Teilmenge $\Sigma_0 = \{\boldsymbol{x}^{a_1}, \ldots, \boldsymbol{x}^{a_m}\}$ 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 $\Sigma = (\boldsymbol{x}^{a_1}, \ldots, \boldsymbol{x}^{a_m})$.

Satz 11 *Jedes Monoidideal $\Sigma \subset T$ hat eine eindeutig bestimmte Minimalbasis. Diese besteht genau aus den $\boldsymbol{x}^\alpha \in \Sigma$, die minimal in Σ bzgl. der Teilbarkeitsrelation sind, d. h. für die*

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

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

Satz 12 *(Dickson-Lemma) Jedes Monoidideal $\Sigma \subset T := T(x_1, \ldots, x_n)$ besitzt 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 $\Sigma \subset T$ zeigen. Mit $\mathbf{x} = (x_1, \ldots, x_{n-1})$ und $y = x_n$ kann jedes $M \in T$ (eindeutig) als $M = \mathbf{x}^\alpha y^m$ dargestellt werden.
Betrachten wir zunächst

$$\Sigma' := \{\mathbf{x}^\alpha \;:\; \exists\, m > 0\ \mathbf{x}^\alpha y^m \in \Sigma\}.$$

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 $\mathbf{x}^{\alpha_i} y^{m_i} \in \Sigma$ gilt.
Sei $m := max(m_i \,:\, i = 1, \ldots, k)$ und für $l \geq 0$

$$\Sigma_l := \{\mathbf{x}^\alpha \;:\; \mathbf{x}^\alpha y^l \in \Sigma\}.$$

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

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

sowie $\Sigma_l = \Sigma'$ 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

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

gilt.

Wir behaupten nun, dass die Vereinigung $C := \bigcup_{l \leq m} C_l \subset \Sigma$ eine endliche Basis von Σ ist. Nach der Basiseigenschaft ist dazu nur zu zeigen, dass jedes Monom $M \in \Sigma$ 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:

$\Sigma = (x^4y^2, x^3y^4, x^2y^5)$ Dann ist $\Sigma' = (x^2), m = 5$ und für die einzelnen „Scheiben“ erhalten wir $\Sigma_0 = \Sigma_1 = \{0\}, \Sigma_2 = \Sigma_3 = (x^4), \Sigma_4 = (x^3)$. Nach dem Beweisschema erhalten wir

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

wobei das Monom x^4y^3 in einer Minimalbasis überflüssig ist.

Folgerung 1 *Jede echt aufsteigende Kette $\Sigma_1 \subset \Sigma_2 \subset \ldots$ von Monoididealen ist endlich.*

Beweis: $\Sigma = \cup_i \Sigma_i$ ist dann ebenfalls eine Monoidideal und nach dem Dicksonlemma endlich erzeugt. Damit existiert aber ein m, für das $Sigma = \Sigma_m$ gilt. $\square$

5.2 Normalformen

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

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

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

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

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

$$4\,z = -4$$

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 zentraler Baustein, 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:

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

um daraus $f = \left(x^2 - x + 1\right)\, g + r$ zu erhalten.

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 $r = f \pmod g$ ist berechnet. Der Euklidsche Algorithmus wird nun mit g und r fortgesetzt, d. h. mit einer „einfacheren“ Ersetzungsregel $x \mapsto 1$. Im Gegensatz zum Gauß-Algorithmus gibt es (potentiell) unendlich viele x-Potenzen als linke Seiten unserer Ersetzungsregeln. Die Termination des Verfahrens beruht hier darauf, dass stets nur höhere durch niedrigere Potenzen ersetzt werden.

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

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

abgeleitet, diese als Ersetzungsregeln aufgefasst und damit

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

hergeleitet und so $f, g \in I$ geschlossen. Um 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 nachweisen, dass ein solches Ersetzungsverfahren aus noch zu präzisierenden Gründen terminiert.

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 $0 \neq f(\mathbf{x}) = \sum_{i=0}^{N} c_i \mathbf{x}^{\alpha_i} \in R$ ein Polynom, so dass in der fixierten Termordnung $\mathbf{x}^{\alpha_i} > \mathbf{x}^{\alpha_j}$ für $i < j$ gilt. Bezeichne weiter $T(f) := \{\mathbf{x}^{\alpha_i},\, i = 0, \ldots, N\}$ die Menge der in der Darstellung von f auftretenden Terme. Dann können wir die folgenden Begriffe definieren:

- den Leitterm $lt(f) := \mathbf{x}^{\alpha_0}$,
- den Leitkoeffizienten $lc(f) := c_0$,
- das Leitmonom $lm(f) := lc(f) \cdot lt(f)$,
- das Reduktum $red(f) := \sum_{i=1}^{N} c_i \mathbf{x}^{\alpha_i} = f - lm(f)$.

Beispiel: $f = 4\,x\,y^2z + 4\,z^2 - 5\,x^3 + 7\,x^2z^2$.

CoCoA ordnet die Terme eines Polynoms sofort entsprechend der aktuell gültigen Termordnung (d. h. bringt das Polynom in die *distributive Normalform*). Hier sind die Ergebnisse für f mit verschiedenen Termordnungen. Zunächst die Default-Ordnung DegRevLex:

```
4*x*y^2*z+4*z^2-5*x^3+7*x^2*z^2;
4*x*y^2*z + 7*x^2*z^2 - 5*x^3 + 4*z^2;
------------------------------
```

Nun die lexikografische und die gradweise lexikografische Termordnung.

```
Use R::=QQ[x,y,z],Lex;
4*x*y^2*z + 7*x^2*z^2 - 5*x^3 + 4*z^2
-5*x^3 +7*x^2*z^2 +4*x*y^2*z +4*z^2
------------------------------

Use R::=QQ[x,y,z],DegLex;
4*x*y^2*z + 7*x^2*z^2 - 5*x^3 + 4*z^2
7*x^2*z^2 +4*x*y^2*z -5*x^3 +4*z^2
------------------------------
```

Zusammenfassung in Tabellenform:

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

Aufgabe:

1. Untersuchen Sie, ob es eine Termordnung gibt, in der $lm(f) = 4z^2$ gilt.
2. Ordnen Sie die Summanden der folgenden Polynome bzgl. der drei wichtigsten Termordnungen:

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

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: $B_1 = \left\{f_1 = x^2 + xy + y^2,\ f_2 = xz + yz,\ f_3 = y^3 - z^3\right\}$ 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

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

```
Use R::=Q[x,y,z],Lex;
B1:=[x^2+x*y+y^2,x*z+y*z,y^3-z^3];
G:=x^2*y^2+x^2*z^2+y^2*z^2;
NR(G,B1);
y^2*z^2
------------------------------
```

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. Das von $\Sigma(B)$ erzeugte PP-Ideal bezeichnen wir mit $Lt(B)$.

Beispiel, dass es ganz wesentlich auf die Reihenfolge beim Berechnen der Normalform ankommt: $B_2 := \left\{ux - y^2, uy - z^2, uz - x^2\right\}$ und Reduktion des Monoms u^2xyz.

```
Use R::=QQ[u,x,y,z],Lex;
B2:=[u*x-y^2,u*y-z^2,u*z-x^2];
G:=u^2*x*y*z;
NR(G,[B2[1],B2[2]]);
y^2*z^3
------------------------------
NR(G,[B2[1],B2[3]]);
x^2*y^3
------------------------------
NR(G,[B2[2],B2[3]]);
x^3*z^2
------------------------------
```

Verschiedene Pfade liefern eine der Normalformen y^2z^3, z^3x^2 oder x^3z^2. Begriff des *Reduktionspfads*.

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

ist:

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

Input: Polynom $f \in R$, endliche Menge $B \subset R$.

Output: Polynom $f' \in R$ mit $f \equiv f' \pmod{I(B)}$ und $f' = 0$ oder $lt(f') \notin \Sigma(B)$.

```
while (f ≠ 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 noetherschen Termordnung endlich sein muss.

Ähnlich wie im Erweiterten Euklidschen Algorithmus kann man den Normalforn-Algorithmus so modifizieren, dass sogar eine Darstellung von $f' - f \in I(B)$ als polynomiale Kombination der Basiselemente zurückgegeben wird. In obigem Beispiel etwa erhalten wir bei der Berechnung von $g' := \mathtt{NF}(g, B)$ nacheinander

$$\begin{aligned}
g \mapsto g_1 &= g - y^2\, f_1 &&= x^2z^2 - xy^3 - y^4 + y^2z^2\\
\mapsto g_2 &= g_1 - z^2\, f_1 &&= -xy^3 - xyz^2 - y^4\\
\mapsto g_3 &= g_2 + x\, f_3 &&= -xyz^2 - xz^3 - y^4\\
\mapsto g_4 &= g_3 + y\,z\, f_2 &&= -xz^3 - y^4 + y^2z^2\\
\mapsto g_5 &= g_4 + z^2\, f_2 &&= -y^4 + y^2z^2 + yz^3\\
\mapsto g_6 &= g_5 + y\, f_3 &&= y^2z^2 = g'
\end{aligned}$$

also $g = (y^2 + z^2)f_1 + (-y\,z - z^2)f_2 + (-x + y)f_3 + g'$.

Allgemein lassen sich die Kofaktoren während der Reduktion auf dieselbe Weise in einem Vektor $(v_1, \ldots, v_m)$ aufsammeln:

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
```

$v_i := v_i + \frac{lm(f)}{lm(b_i)}$

`return` (f, v)

Diese Darstellung als polynomiale Kombination der Basisvektoren hat eine weitere wichtige Eigenschaft; sie kommt ohne „große“ intermediäre Terme aus:

Satz 13 *Sei $B = \{b_1, \ldots, b_m\} \subset R$ eine endliche Menge von Polynomen. Dann liefert der Algorithmus* **NFwithRelations** *für jedes Polynom $f \in R$ nach endlich vielen Schritten eine Darstellung*

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

mit $v_1, \ldots, v_m, r \in R$, in der $r = 0$ oder $lt(r) \notin \Sigma(B)$ und $lt(f) \geq lt(v_i)\, lt(b_i)$ für alle i gilt.

Beweis: Da `NFwithRelations` nur eine Modifikation von `NF` ist, muss nur die letzte Aussage $lt(f) \geq lt(v_i)\, lt(b_i)$ (1) bewiesen werden.
Sind f' und $f'' = f - \frac{lm(f')}{lm(b_i)} b_i$ zwei intermediäre Terme, so unterscheiden sich die Vektoren v für f' und f'' nur im Summand mit dem Term $m = \frac{lt(f')}{lt(b_i)}$, für den aber gilt $lt(f) \geq lt(f') = m \cdot lt(b_i)$. Aussage (1) gilt also für alle Terme von h_i und folglich auch für den Leitterm. □

Das CoCoA-Kommando `DivAlg` (für „division algorithm“) führt diese Rechnungen aus. Im folgenden Beispiel wird die Normalform von xyz bzgl. der interreduzierten Basis B_{3b} berechnet:

```
Use R::=QQ[u,x,y,z],Lex;
B2:=[u*x-y^2,u*y-z^2,u*z-x^2];
R:=DivAlg(u^2*x*y*z,B2);
R;
record[quotients := [u*y*z, y^2*z, 0], remainder := y^2*z^3]
------------------------------
```

Die Probe zeigt, dass das Ergebnis die Spezifikation der Aufgabenstellung erfüllt:

```
ScalarProduct(R.quotients,B2)+R.remainder;
u^2*x*y*z
------------------------------
```

Mit dem Algorithmus `NF` können wir schon eine Antwort auf die erste Hälfte des Idealenthaltenseins-Problems geben:

Satz 14 *Seien R, f und B wie in obigem Satz. Ist $NF(f, B) = 0$, so gilt $f \in I(B)$.*

Die Umkehrung dieses Satzes gilt nicht, d. h. es kann durchaus Elemente $f \in I$ geben, für die $\mathtt{NF}(f, B) \neq 0$ gilt. Mehr noch kann das Ergebnis vom gewählten Reduktionspfad abhängen. Der Satz kann dahingehend verschärft werden, dass $\mathtt{NF}(f, B) = 0$ für einen einzigen Reduktionspfad ausreicht, um auf $f \in I$ zu schließen. Jedoch auch von dieser Verschärfung gilt die Umkehrung nicht: Wir werden später auf systematische Weise Polynome $f \in I$ konstruieren, die als Summe von Standardtermen überhaupt nicht weiter reduziert werden können.

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. 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 $f \equiv f' \pmod{I(B)}$ 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. Die CoCoA-Kommandos `NR` und `DivAlg` berechnen bereits solche totalen Normalformen.

5.3 Interreduktion

Betrachten wir das folgende System von Polynomen

$$B_3 := \{f_1 = x^2 + y + z - 3,\ f_2 = x + y^2 + z - 3,\ f_3 = x + y + z^2 - 3\},$$

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

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

Hier die entsprechenden Rechnungen mit CoCoA (über `QQ[x,y,z],Lex`):

```
Use R::=QQ[x,y,z],Lex;
F1:=x^2 + y + z - 3;
F2:=x + y^2 + z - 3;
F3:=x + y + z^2 - 3;
B3:=[F1,F2,F3];
F4:=NR(F1,[F3]);
F4;
y^2 +2*y*z^2 -5*y +z^4 -6*z^2 +z +6
------------------------------
F5:=NR(F2,[F3]);
F5;
y^2 - y - z^2 + z
------------------------------
```

Im Allgemeinen können wir ähnlich vorgehen und erhalten ein Ergebnis, das der Triangulierung einer Matrix im Gaussverfahren entspricht: Solange in der Basis ein Element enthalten ist, das bzgl. der anderen reduziert werden kann, führen wir diese Reduktion aus und ersetzen das alte Basiselement durch das neue (oder lassen es weg, wenn die Reduktion 0 ergeben hat).

Eine Basis B mit der Eigenschaft

$$\forall\, f \in B \;:\; lt(f) \notin \Sigma(B - \{f\})$$

heißt *reduziert*. Der folgende Algorithmus `Interreduce` berechnet aus einer beliebigen Basis eine reduzierte Basis desselben Ideals.

Interreduce(B: Basis): Basis

Input: Basis $B = \{b_1, \ldots, b_m\} \subset R$

Output: Basis B' mit $I(B) = I(B')$ und $|B'| = |Gen(\Sigma(B'))|$

```
while exists f ∈ B, lt(f) ∈ Σ(B − {f}) do
  B = B − {f}
  f' = NF(f, B)
  if f' ≠ 0 then B = B ∪ {f'}
return B
```

Satz 15 *Der Algorithmus* **Interreduce** *terminiert, wenn* $(T, <)$ *eine noethersche Termordnung ist, und erfüllt die gegebene Spezifikation.*

Beweis: Sei $B' = B - \{f\}$. Wegen $f' = NF(f, B') \equiv f \pmod{B'}$ gilt offensichtlich $I(B' \cup \{f\}) = I(B' \cup \{f'\})$, so dass nur die Termination zu beweisen ist.

Nach Auswahl von f gilt $\Sigma(B) = \Sigma(B')$ und $f' = 0$ oder $lt(f') \notin \Sigma(B')$. Im zweiten Fall ist $\Sigma' = \Sigma(B' \cup \{f'\})$ eine echte Obermenge von $\Sigma = \Sigma(B)$.

Würde der Algorithmus nicht terminieren, so gäbe es also eine unendliche Kette $\Sigma_1 \subset \Sigma_2 \subset \ldots$ von echt ineinander enthaltenen Monoididealen. Dies widerspricht aber dem Dicksonlemma. □

Bemerkung: Die Eigenschaft, dass es sich um eine *noethersche* Termordnung handelt, wurde nur für die Termination von NF benötigt; die while-Schleife terminiert allein auf Grund des Dicksonlemmas.

In obigem Beispiel erhalten wir nacheinander

```
F4:=NR(F1,[F2,F3]);
F4;
y^4 +2*y^2*z -6*y^2 +y +z^2 -5*z +6
------------------------------
F5:=NR(F2,[F3,F4]);
F5;
y^2 - y - z^2 + z
------------------------------
F6:=NR(F4,[F3,F5]);
```

```
F6;
2*y*z^2 -4*y +z^4 -5*z^2 +6
------------------------------
```

also

$$B = \{f_1, f_2, f_3\} \mapsto \{f_2, f_3, f_4\} \mapsto \{f_3, f_4, f_5\} \mapsto \{f_3, f_5, f_6\}$$

mit den Monoididealen

$$\Sigma(x) \subset \Sigma(x, y^4) \subset \Sigma(x, y^2) \subset \Sigma(x, y^2, y\,z^2)$$

Das kann mit dem CoCoA-Kommando `Interreduced(B)` erreicht werden.

```
interreduced(B3);
[2*y*z^2 -4*y +z^4 -5*z^2 +6, -y^2 +y +z^2 -z, x +y +z^2 -3]
------------------------------
```

Die reduzierte Basis B heißt *vollständig interreduziert*, wenn alle Terme in den Basiselementen bis auf den Leitterm Standardterme sind.

$$\forall b \in B \quad T(red(b)) \cap \Sigma(B) = \emptyset.$$

Eine solche Basis kann aus einer interreduzierten gewonnen werden, indem das Reduktum jedes Basiselements durch dessen totale Normalform ersetzt wird.

Aufgabe: Überführen Sie die Idealbasis

$$B_5 := \{w + x + y + z, wx + xy + yz + zw, wxy + xyz + yzw + zwx, wxyz - 1\}$$

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

5.4 Gröbnerbasen und Hilberts Basissatz

Die systematische Vergrößerung von $\Sigma(B)$ im Zuge des Interreduktionsprozesses kann man verallgemeinern: Wir können beliebige Polynome $f \in I$ mit $lt(f) \notin \Sigma(B)$ mit demselben Erfolg zu B hinzunehmen, um die „Reduktionskraft“ von B zu verstärken.

Dafür müssen wir nicht einmal von einer Idealbasis ausgehen, sondern können diesen Prozess mit $B = \emptyset$ als Startmenge beginnen. In jedem Schritt ergänzen wir B um ein Element $0 \neq f \in I$ mit $lt(f) \notin \Sigma(B)$, so lange das möglich ist. Wir bekommen dabei eine Kette $\Sigma_0 \subset \Sigma_1 \subset \ldots$ von echt wachsenden Monoididealen, was nach dem Dicksonlemma nach endlich viele Schritten zu einer endlichen Menge G von Polynomen mit der Eigenschaft $\Sigma(G) = \Sigma(I)$ führt.

Es handelt sich dabei um besondere Teilmengen von I, denn selbst für eine Basis B des Ideals I gilt zwar $\Sigma(B) \subseteq \Sigma(I)$, es muss aber nicht unbedingt $\Sigma(B) = \Sigma(I)$ gelten.

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

Definition 9 *Eine Teilmenge $G \subset I$ des Ideals I mit $\Sigma(G) = \Sigma(I)$ heißt* Gröbnerbasis *von I.*

Da Σ als Monoidideal endlich erzeugt ist, hat das Ideal I auch Gröbnerbasen mit endlich vielen Elementen. Jede Teilmenge $G' \subset G$, deren Leitterme noch immer Σ erzeugen, ist ebenfalls eine Gröbnerbasis von I. Eine Gröbnerbasis G heißt *minimal*, wenn $\{lt(g) \mid g \in G\} = Gen(\Sigma)$ gilt.

Ist G darüber hinaus vollständig interreduziert, so heißt G *minimale reduzierte Gröbnerbasis*. Wir werden später sehen, dass eine solche Gröbnerbasis bei vorgegebenem Ideal I und vorgegebener Termordnung $(T, <)$ eindeutig bestimmt ist.

Obwohl unsere Argumentation nicht konstruktiv war, haben wir oben gezeigt, dass jedes Ideal eine Gröbnerbasis hat. Es bleibt noch der Begriff „Basis“ zu rechtfertigen, d. h. zu zeigen, dass G wirklich eine Basis des Ideals I ist.

Satz 16 *Jede endliche Gröbnerbasis $G = \{g_1, \ldots, g_r\} \subset I$ ist eine Basis des Ideals I.*

Beweis: Wegen $G \subset I$ bleibt 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 $q = 0$ und damit $f \in I(G)$. $\square$

Wir sagen deshalb auch ohne Bezug auf ein Ideal, dass G eine Gröbnerbasis ist, wenn G dies bzgl. des Ideals $I = I(G)$ ist.

Einer der zentralen Sätze der kommutativen Algebra ergibt sich nun als einfache Folgerung:

Folgerung 2 *(Hilberts Basissatz) Jedes Ideal $I \subset R$ besitzt eine endliche Basis.*

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 die Nützlichkeit des eingeführten Begriffs auch für andere konstruktive Fragestellungen zusammentragen.

5.5 Erste Eigenschaften von Gröbnerbasen

Gröbnerbasen erlauben eine eindeutige Antwort auf das Idealenthaltenseinsproblem:

Satz 17 *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 $f \equiv r \pmod I$, d. h. $r \in I$, ein Widerspruch. $\square$

Folgerung 3 *Für eine Gröbnerbasis G 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 $f \equiv TNF(f,G) \pmod{I(G)}$ auch $r := r_1 - r_2 \in I$. Da aber beide Normalformen Linearkombinationen aus Standardtermen sind, so auch r. Also muss $r = 0$ sein, da sonst $lt(r) \notin \Sigma(G) = \Sigma(I)$ wäre. $\square$

5.6 S-Polynome

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 $B_2 := \{f_1 = u\,x - y^2, f_2 = u\,y - z^2, f_3 = u\,z - x^2\}$ gesehen: $u^2\,x\,y\,z$ 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 $lt(f) = x^3z^2 \notin \Sigma(B_2)$.

```
Use R::=QQ[u,x,y,z],Lex;
F1:=u*x-y^2; F2:=u*y-z^2; F3:=u*z-x^2;
```

Kleinste Gegenbeispiele können auf folgende Weise konstruiert werden:

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

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 10 *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.*

Eine entsprechende Funktion kann man in CoCoA wie folgt vereinbaren:

```
Define SPoly(F,G)
  M:=LCM(LT(F),LT(G));
  Return (M/LM(F))*F-(M/LM(G))*G;
EndDefine;
```

Für die Elemente einer Idealbasis B definieren wir noch abkürzend

```
Define S(B,I,J)
  Return SPoly(B[I],B[J]);
EndDefine;
```

Ein solches S-Polynom, falls es nicht verschwindet, besitzt einen Leitterm, der echt kleiner als der erwartete Leitterm $m = lcm(lt(f), lt(g))$ 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_2 zur Basis die drei neu erzeugten Polynome hinzu, erhalten wir eine neue Basis

$$B_{2a} = \{f_1, f_2, f_3, f_4 := s_{12}, f_5 := s_{13}, f_6 := s_{23}\}$$

mit $\Sigma(B_{2a}) = \big(u\,x, u\,y, u\,z, x\,z^2, x^3, x^2y\big)$.
Bzgl. dieser neuen Basis ist offensichtlich

$$NF(S(f_i, f_j), B_{2a}) = 0$$

für $(i, j) \in \{(1, 2), (1, 3), (2, 3)\}$. Andererseits können zwischen den neuen und alten Elementen neue S-Polynome konstruiert werden:

$$s_{14} = z^2\,f_1 - u\,f_4 = (u\,x\,z^2 - y^2z^2) - (u\,x\,z^2 - u\,y^3) = u\,y^3 - y^2z^2$$

Im Gegensatz zu obigen Polynomen ist dieses Polynom nicht bereits in Normalform bzgl. B_{2a}. Es gilt

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

also $NF(s_{14}, B_{2a}) = 0$. 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

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

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

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

ein letztes solches Polynom. Die Normalformen aller weiteren S-Polynome verschwinden, 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 $I(B_3)$ hatten wir bereits eine neue Idealbasis

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

konstruiert. Hier liefert nur $NF(S(f_5, f_6), B_{3b})$ ein neues nichttriviales Polynom f_7:

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

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 18 *(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. es gilt $\Sigma(I) = \Sigma(G)$.*
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*

$$f = \sum_{g \in G} h_g g \quad \textit{mit} \quad \forall\, g\ (lt(f) \geq lt(h_g g)).$$

7. *Die Standardterme $N(G) := T(X) \setminus \Sigma(G)$ sind k-linear unabhängig $\pmod I$.*
8. *Die Standardterme $N(G)$ bilden eine k-Vektorraumbasis des Faktorrings R/I, d. h. jedes Element $f \in R$ besitzt eine eindeutige Darstellung*

$$f \equiv \sum_{m \in N(G)} c_m m \pmod I$$

mit $c_m \in k$.

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

5. ⇒ 6.: Sei $f = \sum h_g g \in I$, aber $lt(f) < m := \max(lt(h_g g) | h_g \neq 0)$. Im Folgenden bezeichnet $f_1, f_2, \ldots$ Kombinationen $\sum h'_g g \in I$ mit $\max(lt(h'_g g) | h'_g \neq 0) < m$. Zunächst ist

$$f = \sum\nolimits^{*} h_g g + f_1 = \sum\nolimits^{*} (lm(h_g) + red(h_g))\, g + f_1 = \sum\nolimits^{*} lm(h_g)\, g + f_2\,,$$

wobei sich die Summation $\sum^*$ nur über diejenigen $g \in G$ erstreckt, für die $lt(h_g g) = m$ gilt. Insbesondere ist $lt(g) \,|\, m$ für $g \in *$. Betrachten wir den Ausdruck unter dem Summenzeichen.

Für jeden einzelnen Summanden gilt nach Konstruktion $lt(h_g)\,lt(g) = m > lt(f)$, also ist $\sum^* lc(h_g)\,lc(g) = 0$. Sei o. B. d. A $g_1 \in *$. Dann gilt $lt(g_1) \,|\, m$ und

$$\sum^* lc(h_g)\,lc(g)\,\frac{m}{lm(g_1)}\,g_1 = 0\,.$$

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

$$\sum^* lm(h_g)\,g = \sum^* lc(h_g)\,lc(g)\,\frac{m}{lm(g)}\,g = \sum^* lc(h_g)\,lc(g)\,\frac{m}{m_g}\,S(g,g_1)\,,$$

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

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

1. $\Rightarrow$ 7.: Wäre

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

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 $N(G)$. $\square$

Der Charakterisierungssatz zeigt, dass die oben berechnete Menge $G = \{f_1, \ldots, f_8\}$ eine Gröbnerbasis von $I = I(B_2)$ 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 19 *(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

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

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

Betrachten wir noch einmal die Rechnungen zum Beispiel

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

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

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

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

5.7 Der Buchberger-Algorithmus

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

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

GBasis(B: Basis): Basis

Input: Endliche Menge $B = \{f_1, \ldots, f_m\} \subset R$.

Output: Gröbnerbasis G des Ideals $I = I(B)$.

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

Satz 20 *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 bzgl. der lexikografischen Termordnung mit $y > x$.

```
B0:=[17*x^2+22*x*y+13*y^2-1, 8*x^2+28*x*y+37*y^2-1];
```

Interreduktion liefert als Augangspunkt für den Gröbneralgorithmus

```
interreduced(B0);
```

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

Nichttrival reduzierende S-Polynome können mit CoCoA wie folgt berechnet werden:

```
NR(S(B0,1,2),B0);
Append(ref B0,It);
B0;
```

In unserem Beispiel erhalten wir nacheinander die folgenden neuen nicht trivialen Basiselemente

$$f_3 = NF(S(f_1, f_2), B_0) = 48\,y + 625\,x^3 - 44\,x$$
$$f_4 = NF(S(f_1, f_3), B_0 \cup \{f_3\}) = 15625\,x^4 - 2500\,x^2 + 64,$$

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 21 *Ist G eine Gröbnerbasis des Ideals I und $G' \subset G$ eine Teilmenge, so dass*

$$Gen(\Sigma(G)) = \big\{lt(g),\, g \in G'\big\}$$

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

$$G'' = \big\{lt(g) - TNF(lt(g), G'),\, g \in G'\big\} \subset I$$

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

5.8 Gröbnerbasen bzgl. verschiedener Termordnungen

Wir hatten oben bereits gesehen, dass man mit Gröbnerbasen das Idealenthaltenseinsproblem algorithmisch lösen kann. Der dabei zu treibende Aufwand hängt allerdings von der gewählten Termordnung ab.

Wollen wir etwa prüfen, ob $f = -4\,x^2y^2z^2 + y^6 + 3\,z^5$ im von $B = \{x\,z - y^2, x^3 - z^2\}$ 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 lexikografischen Termordnung mit $x > y > z$ erhalten wir etwa

```
Use R::=QQ[x,y,z],Lex;
F:=-4*x^2*y^2*z^2+y^6+3*z^5;
B:=Ideal(x*z-y^2,x^3-z^2);
GBasis(B);
[x*z -y^2, x^3 -z^2, -x^2*y^2 +z^3, -x*y^4 +z^4, -y^6 +z^5]
------------------------------
NF(F,B);
0
------------------------------
```

`NF(F,B)` berechnet dabei die Normalform von F bzgl. der Gröbnerbasis von B. Verwenden wir dagegen die gradweise revers-lexikografische Termordnung, so ist $B = \{-y^2 + x\,z, x^3 - z^2\}$ bereits selbst Gröbnerbasis.

In praktischen Anwendungen hat sich herausgestellt, dass Gröbnerbasen bzgl. der rein lexikografischen Termordnung besonders schwierig zu berechnen sind. Eine komplexitätstheoretische Aussage über die Laufzeit des Buchbergeralgorithmus für „zufällig“ gewählte Polynomsysteme fällt sehr pessimistisch aus: eine (scharfe) Gradschranke für entstehende Basiselemente ist doppelt exponentiell in der Anzahl der Variablen. Genauer: Ist D eine Gradschranke für die Ausgangspolynome in $R = k[x_1, \ldots, x_n]$, so ist $O\left(D^{2^n}\right)$ eine Gradschranke für die Elemente einer Gröbnerbasis bzgl. der degrevlex Termordnung. Für einen Körper k mit Einheitskostenarithmetik (etwa $k = \mathbb{Z}_p$) ist das auch eine Schranke für die Laufzeit des Buchberger-Algorithmus. Über $k = \mathbb{Q}$ kommt noch Koeffizientenwachstum hinzu, was etwa der Hinzunahme einer weiteren Variablen entspricht.

Betrachten wir als weiteres Beispiel das Polynomsystem

$$F = \left\{x^2 - 2\,x\,z + 5,\ x\,y^2 + y\,z^3,\ 3\,y^2 - 8\,z^3\right\}$$

```
Use R::=QQ[x,y,z],Lex;
F := [x^2 - 2*x*z + 5, x*y^2 + y*z^3, 3*y^2 - 8*z^3];
G := ReducedGBasis(Ideal(F));
G;
[z^9 +(-32/3)*z^8 +(80/3)*z^6 +(1600/9)*z^3,
 y*z^3 +(-3/80)*z^8 +(2/5)*z^7 +(-1/2)*z^5,
 y^2 +(-8/3)*z^3,
 x*z^3 +(9/640)*z^8 +(-3/20)*z^7 +(3/16)*z^5,
 x^2 -2*x*z +5]
-------------------------------
```

Wir können in diesem Fall das Gleichungssystem lösen, indem wir das Polynom

$$g_2 = z^9 - \frac{32}{3}z^8 + \frac{80}{3}z^6 + \frac{1600}{9}z^3 \in k[z]$$

faktorisieren, durch je einen der Faktoren ersetzen und noch einmal die Gröbnerbasis ausrechnen.

```
[ ReducedGBasis(Ideal(G)+Ideal(f)) | f In Factor(G[1]).factors];
```

$$\left[z^6 - \frac{32}{3}\,z^5 + \frac{80}{3}\,z^3 + \frac{1600}{9}, y - \frac{3}{80}\,z^5 + \frac{2}{5}\,z^4 - \frac{1}{2}\,z^2, x + \frac{9}{640}\,z^5 - \frac{3}{20}\,z^4 + \frac{3}{16}\,z^2\right],$$
$$\left[z, x^2 + 5, y^2\right],$$
$$[1]$$

Wir lesen daraus die 8 Lösungen dieses Gleichungssystems ab:

$$\left\{(x,y,z)\ :\ x = -\frac{9}{640}\,z^5 + \frac{3}{20}\,z^4 - \frac{3}{16}\,z^2,\ y = \frac{3}{80}\,z^5 - \frac{2}{5}\,z^4 + \frac{1}{2}\,z^2,\right.$$
$$\left. z \in \mathrm{RootOf}\left(z^6 - \frac{32}{3}\,z^5 + \frac{80}{3}\,z^3 + \frac{1600}{9}\right)\right\}$$
$$\cup \left\{\left(\sqrt{-5}, 0, 0\right),\ \left(-\sqrt{-5}, 0, 0\right)\right\}$$

Wir kommen darauf später zurück.

5.9 Der Gröbnerfächer

Frage: Wie viele und welche Gröbnerbasen sind möglich?
Beispiel: $I = \left\langle z^2 - x + y - 1, x^2 - y\,z + x, y^2 - x\,z + 2\right\rangle$.

```
Use R::=QQ[x,y,z],Lex;
B:=[z^2-x+y-1, x^2-y*z+x, y^2-x*z+2];
LT(Ideal(ReducedGBasis(Ideal(B))));
```

R/I ist ein endlichdimensionaler Vektorraum (hier der Dimension 8). Für eine Gröbnerbasis G muss also $N(G)$ genau 8 Elemente enthalten und das Komplement ein Monoidideal Σ sein. Dafür gibt es nur endlich viele Möglichkeiten. Für jede ist zu untersuchen, ob sie zu einer Gröbnerbasis gehört und dazu eine geeignete Termordnung zu finden.

Hier sind einige mögliche Werte für Σ und N für verschiedene Termordnungen.

$$
\begin{aligned}
x, y, z, Lex &: I\left(x, y, z^8\right) \\
y, z, x, Lex &: I\left(x^8, y, z\right) \\
z, x, y, Lex &: I\left(x, y^8, z\right) \\
x, y, z, DegLex &: I\left(z^2, x\,z, x^2, y^2\,z, x\,y^2, y^4\right) && N = [1, x, y, z, x\,y, y^2, x^2\,y, y^3] \\
y, z, x, DegLex &: I\left(z^2, y\,z, y^2, z\,x^2, y\,x^2, x^4\right) && N = [1, x, y, z, x^2, x\,y, x\,z, x^3] \\
z, y, x, DegLex &: I\left(z\,x, z\,y, z^2, y^3, y\,x^2, y^2\,x, x^4\right) && N = [1, x, y, z, x^2, x\,y, y^2, x^3]
\end{aligned}
$$

Wie viele Gröbnerbasen gibt es für ein gegebenes Ideal I? Endlich viele oder unendlich viele? Wann ergeben zwei Termordnungen dieselbe Gröbnerbasis?

Auf die zweite Frage können wir schnell antworten: Wenn die zugehörigen Gröbnerbasen dieselben Leitterme haben, denn dann sind die Menge der Standardterme und damit die reduzierten Normalformen eindeutig bestimmt. Für die erste Frage sei für ein Ideal $I \subset k[x_1, \ldots, x_n]$

$$Mon(I) = \{LT_>(I) : > \text{ eine noethersche Termordnung}\}$$

die Menge aller möglichen Leitterm-Ideale bzgl. verschiedener noetherscher Termordnungen.

Satz 22 *$Mon(I)$ ist endlich.*

Beweis: Wir beschreiben zunächst die Menge $\{LT_>(B) : > \text{ eine noethersche Termordnung}\}$ für eine endliche Menge $B = \{f_1, \ldots, f_s\} \subset R = k[x_1, \ldots, x_n]$.

Eine Auswahl $l : B \to T$ von Termen bezeichnen wir als *zulässig*, wenn es eine noethersche Termordnung gibt, bzgl. der die $l(f), f \in B$, die Leitterme der Polynome $f \in B$ sind. Um zu entscheiden, ob eine Auswahl l zulässig ist, betrachten wir den von

$$\mathbb{N}^n \cup \left\{a - b \mid x^a = l(f), x^b \in T(f)\right\} \subset \mathbb{Z}^n$$

erzeugten Kegel K. $\mathbb{N}^n \subset K$ sichert dabei, dass die ggf. konstruierbare Termordnung mit K als Positivkegel noethersch ist. Für K gilt

(1) Es gibt ein $a \neq 0, a \in \mathbb{Z}^n$ mit $a \in K$ und $-a \in K$ oder

(2) K ist ein Kegel mit Spitze und es existiert ein $w \in \mathbb{R}^n_+$ mit $w(a) > 0$ für alle $a \in K, a \neq 0$.

Eine Auswahl l ist genau im Fall (2) zulässig und jede Termordnung, welche die zu w assoziierte Gewichtsordnung verfeinert, ist eine noethersche Termordnung, für die $lt(f) = l(f)$ für alle $f \in B$ gilt. Dies ergibt sich unmittelbar aus dem Charakterisierungssatz für Termordnungen.

Nehmen wir nun an, dass $Mon(I)$ unendlich ist und starten mit einer Basis B des Ideals I. Jede zulässige Auswahl $l : B \to T$ von Termen dieser Basiselemente als Leitterme kann zu einer Gröbnerbasis mit Leittermen aus $Mon(I)$ fortgesetzt werden und umgekehrt ergibt sich jede solche Gröbnerbasis aus einer solchen Fortsetzung. Da es nur endlich viele Leittermkombinationen gibt, ist eine Leittermkombination Σ dabei, zu der es unendlich viele Fortsetzungen aus $Mon(I)$ gibt. Insbesondere ist $f_1, \ldots, f_s$ selbst noch keine Gröbnerbasis. Nimm $f_{s+1} \in I$, das bzgl. Σ komplett aus Standardtermen besteht (anderenfalls kann man f_{s+1} so weit reduzieren) und v2erfeinere die bisherigen Rechnungen für $B \cup \{f_{s+1}\}$. Es gibt Termordnungen, bzgl. der Σ die Leitterme der f_i bleiben und ein Term von f_{s+1} als Leitterm so gewählt wird, dass es unendlich viele Fortsetzungen aus $Mon(I)$ gibt. Das kann man unendlich oft immer weiter so machen. Das widerspricht aber dem Dicksonlemma. □

Eine entsprechende Liste von Idealbasen kann mit CoCoA berechnet werden.

```
L:=GroebnerFanIdeals(Ideal(B));
[[OrdMat(RingOf(i)),ReducedGBasis(i)] | i in L];
[[LT(i)] | i in L];
```

Für das angegebene Beispiel werden 40 verschiedene Gröbnerbasen berechnet.

5.10 Erste Anwendungen von Gröbnerbasen und Beispiele

Wir hatten bereits gesehen, dass Gröbnerbasen verwendet werden können, um das **Idealenthaltenseinsproblem** zu lösen:

$$f \in I(F) \;\Leftrightarrow\; \mathtt{NF(f, GBasis(F))} = \mathtt{0}.$$

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);
```

Beispiel: $I = I(x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z)$.
Geometrisch ist das der Schnitt von Kugel, Paraboloid und Ebene

```
Use R::=QQ[x,y,z],Lex;
I:=Ideal(x^2+y^2+z^2-1,x^2+z^2-y,x-z);
ReducedGBasis(I);
```

Besteht aus 4 Punkten.
Beispiel: ([CLO, S. 96]) Bestimme Maximum und Minimum der Funktion $f = x^3 + 2\,x\,y\,z - z^2$ auf der Sphäre $s = x^2 + y^2 + z^2 - 1$.
Diese Extremalproblem kann mit Lagrange-Faktoren gelöst werden:

$$\begin{aligned} B &= I(f_x - t\,c_x, f_y - t\,c_y, f_z - t\,c_z, c) \\ &= I(3\,x^2 + 2\,x\,y - 2\,t\,x, 2\,x\,z - 2\,t\,y, 2\,x\,y - 2\,z - 2\,t\,z, x^2 + y^2 + z^2 - 1) \end{aligned}$$

Groebnerbasis lex $t > x > y > z$. Erstes Polynom faktorisiert.

```
Use R::=QQ[t,x,y,z],Lex;
I:=Ideal(3*x^2+2*y*z-2*x*t, x*z-y*t, 2*x*y-2*z-2*z*t, x^2+y^2+z^2-1);
G:=ReducedGBasis(I);
[ReducedGBasis(Ideal(G)+Ideal(f))| f In factor(G[1]).factors];
```

Beispiel: Bestimmung impliziter Gleichungen für $V = \{x = t^4, y = t^3, z = t^2 \mid t \in \mathbb{C}\}$.
Berechnen wir die lex. Gröbnerbasis von $I = I(x - t^4, y - t^3, z - t^2)$ mit t als größter Variable, so sind alle t-freien Basiselemente im Verschwindungsideal $I = I(V) \subset k[x, y, z]$ enthalten.

```
Use R::=QQ[t,x,y,z],Lex;
I:=Ideal(x-t^4,y-t^3,z-t^2);
ReducedGBasis(I);
```

Wir erhalten $I = I(x - z^2, y^2 - z^3)$ als Kandidaten für das Verschwindungsideal. Es gilt $V(I) \supset V$. Es bleibt an dieser Stelle offen, ob Gleichheit gilt.
Beispiel: Tangentialfläche an die getwistete Kubik.

$$F = \left\{ \left(t + u, t^2 + 2\,u\,t, t^3 + 3\,u\,t^2\right) \ :\ t, u \in K \right\}$$

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

```
Use R::=QQ[t,u,x,y,z],Lex;
I:=Ideal(x-(t+u), y-(t^2+2*u*t), z-(t^3+3*u*t^2));
ReducedGBasis(I);
```

Beispiel: Finde die gemeinsamen Lösungen von

$$x^2 + y^2 = 2, x^3 + y^3 = 3, x^4 + y^4 = 4.$$

```
Use R::=QQ[x,y],Lex;
I:=Ideal(x^2 + y^2 - 2, x^3 + y^3 - 3, x^4 + y^4 - 4);
ReducedGBasis(I);
```

Die reduzierte Gröbnerbasis zeigt, dass I das triviale Ideal ist. Mit folgenden Kommandos kann eine Darstellung von 1 als polynomiale Linearkombination der drei Basiselemente gefunden werden.

```
S:=GenRepr(1,I);
ScalarProduct(S,Gens(I));
```

I ist also das triviale Ideal und damit $V(I) = \emptyset$. Über einem algebraisch abgeschlossenen Körper gilt auch die Umkehrung:

Satz 23 (Hilbertscher Nullstellensatz) *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.*

Zu beweisen ist nur die Implikation 1. $\Rightarrow$ 2., was auf einen späteren Zeitpunkt in der Vorlesung verschoben wird.

Mit einer Modifikation dieses Vorgehens können wir auch die Frage beantworten, für welche $a \in \mathbb{C}$ das System

$$B = \left\{x^2 + y^2 - 2, x^3 + y^3 - 3, x^4 + y^4 - a\right\}$$

Lösungen hat. Dazu führen wir dieselben Rechnungen wie oben aus:

```
Use R::=QQ[x,y,a],Lex;
B:=[x^2 + y^2 - 2, x^3 + y^3 - 3, x^4 + y^4 - a];
ReducedGBasis(Ideal(B));
[a^3 +6*a^2 -108*a +274,
 y^2 +(-1/3)*y*a^2 +(-11/3)*y*a +(62/3)*y +(1/2)*a^2 +5*a -31,
 x +y +(-1/3)*a^2 +(-11/3)*a +62/3]
------------------------------
```

Die reduzierte Gröbnerbasis enthält insbesondere ein Element $g(a) = a^3 + 6a^2 - 108a + 274$, welches nur von a abhängt und im Ideal liegt, welches von B in $R = \mathbb{C}[x, y, a]$ erzeugt wird. Also gibt es eine polynomiale Kombination

$$g(a) = \sum_{b \in B} h_b(x, y, a) \cdot b(x, y, a)$$

und für konkrete Zahlen $a_0 \in \mathbb{C}$ ist $g(a_0)$ im Ideal I_0 enthalten, welches von $B_0 = B[a \mapsto a_0]$ erzeugt wird. I_0 ist also *höchstens* dann nicht trivial, wenn $g(a_0) = 0$ gilt.

Da B und G beides Basen des Ideals $I = I(B) \subset k[x, y, a]$ sind, lassen sich die Elemente aus B als polynomiale Kombinationen der Elemente aus G und umgekehrt darstellen.

$$B^T = M_1 \cdot G^T \qquad G^T = M_2 \cdot B^T, \qquad M_1, M_2 \in Mat(R)$$

Dies gilt auch nach einer Substitution $a \mapsto a_0$: B_0 und $G_0 = G[a \mapsto a_0]$ erzeugen beide das Ideal I_0 – allerdings muss G_0 nicht unbedingt mehr Gröbnerbasis sein. Wählen wir a_0 mit $g(a_0) = 0$, so können wir die beiden Lösungen in unserem Fall aber aus G_0 unmittelbar ablesen. Jedes a mit $g(a) = 0$ kann also zu einer Lösung (x, y, a) fortgesetzt werden. Derartige Fragen studieren wir im nächsten Abschnitt genauer.

Das Polynom $g(a)$ bezeichnet man auch als die *Diskriminante* des (parametrischen) Gleichungssystems $B \subset k(a)[x, y]$

6 Eliminationstheorie

Viele konstruktive Fragestellungen der Algebra lassen sich auf Eliminationsprobleme zurückführen. Diese lassen sich ebenfalls mit Gröbnerbasen konstruktiv behandeln.

6.1 Der Eliminationssatz

Beispiel: $I(x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1)$. Berechne eine GBasis bzgl. der lex. Termordnung mit $x > y > z$.

```
Use R::=QQ[x,y,z],Lex;
B3:=[x^2+y+z-1, x+y^2+z-1, x+y+z^2-1];
ReducedGBasis(Ideal(B3));
```

$I \cap k[z] = I(z^6 - 4\,z^4 + 4\,z^3 - z^2)$, denn für jedes Element $f \in I$ muss $lt(f)$ ein Vielfaches eines $lt(g), g \in G$ sein. Ist $f \in k[z]$, so gibt es nur ein solches Basiselement. Ähnlich kann man für $I \cap k[y, z]$ argumentieren. Diese Ideale bezeichnet man als Eliminationsideale.

Das Verfahren funktioniert auch im Allgemeinen: Sei $B \subset R = k[\mathbf{x}]$ eine endliche Menge von Polynomen und die Menge der Variablen in zwei Teilmengen $\mathbf{x} = (x_1, \ldots, x_k, y_1, \ldots, y_m)$ aufgeteilt. Wir fragen nach den Polynomen im Ideal $I = I(B)$, die $x_1, \ldots, x_k$ nicht enthalten, also nach einer Basis des *Eliminationsideals*

$$I' = I(B) \bigcap k[y_1, \ldots, y_m].$$

Zu dessen Berechnung wählen wir auf $T(\mathbf{x})$ eine Termordnung, in der jeder Term, der eine Variable x_i enthält, größer ist als jeder Term, der nur Variablen y_j enthält. Solche Termordnungen bezeichnet man als *Eliminationsordnungen* für $(x_1, \ldots, x_k)$, da ein Polynom

$f(x_1,\dots,x_k,y_1,\dots,y_m)$ genau dann keine der Variablen $x_1,\dots,x_k$ enthält, wenn dies für dessen Leitterm $lt(f)$ gilt.

Neben der lexikografischen Ordnung gibt es eine Reihe anderer Eliminationsordnungen, bzgl. derer sich Gröbnerbasen gewöhnlich schneller ausrechnen lassen. So können wir etwa jede Matrix-Termordnung verwenden, deren erster Gewichtsvektor durch $w(x_i) = 1, w(y_j) = 0$ gegeben ist.

Satz 24 *Ist $R = k[x_1,\dots,x_k,y_1,\dots,y_m]$ und $G = GBasis(B)$ eine (min. reduzierte) Gröbnerbasis des Polynomsystems $B \subset R$ bzgl. einer Eliminationsordnung für $(x_1,\dots,x_k)$, so ist*

$$G' = \{g \in G : lt(g) \in T(y_1,\dots,y_m)\}$$

eine (min. reduzierte) Gröbnerbasis des Eliminationsideals $I' = I(B) \bigcap k[y_1,\dots,y_m]$.

Beweis: Offensichtlich gilt $G' \subset I'$. Ist $f \in I'$, so gilt $f \in I$ und folglich $NF(f,G) = 0$. Da bei der Reduktion aber nur solche $g \in G$ mit $lt(g) \le lt(f)$, also $g \in G'$ herangezogen werden, gilt $NF(f,G') = 0$. Diese Eigenschaft charakterisiert aber Gröbnerbasen. □

Die lexikografische Termordnung ist eine Eliminationsordnung für jedes Anfangssegment der Variablen. Damit hat eine Gröbnerbasis bgzl. dieser Ordnung eine „Dreiecksgestalt“, aus der heraus sich die Lösungsmenge eines polynomialen Gleichungssystems berechnen lässt.

Folgerung 4 *Ist $R = k[x_1,\dots,x_n]$ und $G = GBasis(B)$ eine (min. reduzierte) Gröbnerbasis von $B \subset R$ bzgl. der lexikografischen Termordnung, so ist*

$$G_i = \{g \in G : lt(g) \in T(x_i,\dots,x_n)\}$$

eine (min. reduzierte) Gröbnerbasis des Eliminationsideals $I(B) \bigcap k[x_i,\dots,x_n]$.

Insbesondere enthält G_n das Polynom $g(x_n) \in I$ kleinsten Grades, das nur von x_n abhängt, wenn es ein solches Polynom gibt und G eine minimale reduzierte Gröbnerbasis ist.

Die letzte Aussage folgt unmittelbar aus der Tatsache, dass $k[x_n]$ ein Hauptidealring ist. $G_i, i < n$ kann dagegen mehr als $n - i$ Polynome enthalten.

Dies liefert ein **induktives Verfahren zum Lösen polynomialer Gleichungssysteme**:

> Kennt man eine gemeinsame Nullstelle $(a_{i+1},\dots,a_n)$ von G_{i+1}, so enthält $G_i \backslash G_{i+1}$ alle Polynome, die zur Bestimmung von solchen a_i verwendet werden können, dass $(a_i,\dots,a_n)$ eine Nullstelle von G_i ist.

Dies entspricht der Triangulierung eines linearen Gleichungssystem durch den Gauß-Algorithmus.

Hierzu müssen *partielle Lösungen* $(a_{i+1},\dots,a_n)$ zu Lösungen $(a_i,\dots,a_n)$ erweitert werden. Ist $G_i \setminus G_{i+1} = \{g_1,\dots,g_r\} \subset k[x_i,x_{i+1},\dots,x_n]$, so muss a_i eine gemeinsame Lösung von

$$g_1(x_i,a_{i+1},\dots,a_n) = \dots = g_r(x_i,a_{i+1},\dots,a_n) = 0$$

sein. Das sind univariate Polynome, deshalb kann man den gcd bestimmen, wenn man in $k(a_{i+1},\dots,a_n)[x_i]$ rechnen kann.

Allerdings kann man nicht jede Lösung fortsetzen.

Beispiel: $\{xy = 1, xz = 1\}$. Es gilt $I_1 = I(y-z)$, aber die Lösung (a,a) lässt sich nur für $a \neq 0$ fortsetzen.

Satz 25 (Extension Theorem) *Sei $K \supset k$ ein algebraisch abgeschlossener Körper, $B = \{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n]$, $I = I(B)$, $I_1 = I \cap k[x_2, \ldots, x_n]$, $(c_2, \ldots, c_n) \in V_K(I_1)$ und*

$$f_i = g_i(x_2, \ldots, x_n)\, x_1^{N_i} + < \textit{kleinere Terme} >$$

die Basiselemente, die x_1 enthalten. Gilt $(c_2, \ldots, c_n) \notin V_K(g_1, \ldots, g_s)$, so kann diese Nullstelle zu $(c_1, c_2, \ldots, c_n) \in V_K(I)$ fortgesetzt werden.

Beweis machen wir später.

Wesentlich ist, dass K algebraisch abgeschlossen ist.

Beispiel: $B = \left\{x^2 = y, x^2 = z\right\}$ über $\mathbb{R}$. Eliminationideal ist $y - z$, Nullstelle (a, a) kann aber nur für $a \geq 0$ fortgesetzt werden.

Beispiel: $B = \{xy = 1, xz = 1\}$ illustriert das Theorem.

Satz kann mehrfach angewendet werden.

Beispiel: $B = \left\{x^2 + y^2 + z^2 - 1, x\,y\,z - 1\right\}$.

```
Use R::=QQ[x,y,z],Lex;
I:=Ideal(x^2+y^2+z^2-1, x*y*z-1);
ReducedGBasis(I);
```

$$\left[y^4\, z^2 + y^2\, z^4 - y^2\, z^2 + 1, x + y^3\, z + y\, z^3 - y\, z\right]$$

$I_1 = I(g_1 = y^4z^2 + y^2z^4 - y^2z^2 + 1)$, $I_2 = I(0)$. Also kann $z = c$ für jedes $c \in \mathbb{C}$ sein. Erste Erweiterung geht klar für $c \notin V(z^2)$, also für $c \neq 0$. Für $c = 0$ ist $g_1(c) = 1 \neq 0$, also kann $c = 0$ nicht fortgesetzt werden. $c \neq 0$ kann auch auf x fortgesetzt werden.

Folgerung 5 *Ist eines der Polynome g_i konstant, so ist $(a_2, \ldots, a_n)$ immer fortsetzbar.*

Satz 26 *k sei ein unendlicher Körper, $f \in k[x_1, \ldots, x_n]$ nicht konstant und $t_2, \ldots, t_n \in k$ genügend allgemein. Dann führt die Substitution $x_i \to x_i + t_i x_1$ in f zu einem Polynom*

$$a x_1^d + g_1(x_2, \ldots, x_n) x^{d-1} + \cdots + g_d(x_2, \ldots, x_n)$$

mit $a \in k, a \neq 0$ und $g_i \in k[x_2, \ldots, x_n]$.

Beweis: Sei $f = \sum_a c_a \mathbf{x}^a$ mit $\mathbf{x}^a = x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$. Substituieren wir in jedem Term $x_i \to x_i + t_i x_1$ und multiplizieren aus, so entsteht jeweils $\mathbf{t}^a \cdot x_1^{a_1 + \cdots + a_n}$ als höchste x_1-Potenz. Ist $a = \max(a_1 + \cdots + a_n | \mathbf{x}^a \in T(f))$, so gilt

$$f = \left(\sum_a{}^{*} c_a \mathbf{t}^a\right) x_1^a + < \text{kleinere Terme} >,$$

wobei in $\sum^*$ über die $\mathbf{x}^a \in T(f)$ summiert wird, für die $a_1 + \cdots + a_n = a$ gilt. Da über einem unendlichen Körper nur das Nullpolynom die Nullfunktion ist, gibt es eine Belegung der $\mathbf{t}$ mit Elementen aus k, für die $\sum_a^* c_a \mathbf{t}^a \neq 0$ ist. $\square$

Beispiel: Statt $\{xy = 1, xz = 1\}$ zu lösen, führen wir die Substitution $y = y_1 + x, z = z_1 + x$ durch und lösen $\{x(x + y_1) = 1, x(x + z_1) = 1\}$.

```
Use R::=QQ[x,y1,z1],Lex;
I:=Ideal(x*(x+y1)-1, x*(x+z1)-1);
ReducedGBasis(I);
```

$$\left[y_1 - z_1, x^2 + x\,z_1 - 1\right]$$

Nach diesem Koordinatenwechsel gibt es keinen Ausnahmelokus mehr. Allerdings ist die Lösungsmenge auch komplizierter parametrisiert: Wegen $x = \frac{1}{z} = \frac{1}{x+z_1}$ gibt es zu jedem Wert $y_1 = z_1 = c$ *zwei* Werte für x.

Beispiel:

```
Use R::=QQ[x,y,z],Lex;
B:=[x^2 + y + z - 3, x + y^2 + z - 3, x + y + z^2 - 3];
I:=Ideal(B);
G:=ReducedGBasis(I); G;
[z^6 -10*z^4 +4*z^3 +19*z^2 -8*z -6,
 y*z^2 -2*y +(1/2)*z^4 +(-5/2)*z^2 +3,
 y^2 -y -z^2 +z,
 x +y +z^2 -3]
------------------------------
```

Die Gröbnerbasis enthält mit $f = z^6 - 10z^4 + 4z^3 + 19z^2 - 8z - 6$ ein Polynom allein in z, dessen Nullstellen bestimmt werden können. Nach dem Extension Theorem kann man jede dieser Nullstellen zu Nullstellen (x, y, z) von B fortsetzen. Das geht hier besonders einfach.

```
------------------------------
Factor(G[1]).factors;
[z +3, z -1, z^2 -2, z^2 -2*z -1]
------------------------------
```

Fügen wir die einzelnen Faktoren zu G hinzu, ergeben sich weitere Vereinfachungen.

```
GBasis(Ideal(G)+Ideal(z-1));
```

$$[[z+3, y+3, x+3], [z-1, y-1, x-1],$$
$$[z^2-2, y^2-y+z-2, x+y-1], [z^2-2\,z-1, y+z-1, x+z-1]]$$

Wir können daraus die Lösungen $(x, y, z) = (1, 1, 1)$ und $(x, y, z) = (-3, -3, -3)$ leicht ablesen. Die anderen beiden Teile entsprechen Lösungen mit $z = \pm\sqrt{2}$ und $z = 1 \pm \sqrt{2}$. Diese können aus

$$[z^2 - 2\,z - 1, y + z - 1, x + z - 1]$$

besonders einfach abgelesen werden, da hier zu einer Nullstelle $z = c$ von $z^2 - 2\,z - 1$ die Erweiterung auf $(x, y, z) = (1 - c, 1 - c, c)$ unmittelbar berechnet werden kann. Für

$$[z^2 - 2, y^2 - y + z - 2, x + y - 1]$$

ist das schwieriger, denn dazu müssen die Nullstellen von $y^2-y+c-2$ in $k(c)$ für die Nullstelle $z = c(= \pm\sqrt{2})$ von $z^2 - 2$ bestimmt, also Rechnungen über der Körpererweiterung $k(c)$ von c ausgeführt werden.

Allgemein gilt: Ist $f = f_1 \cdot \ldots \cdot f_k$ eine Zerlegung in Faktoren und F eine Menge weiterer Polynome, so gilt offensichtlich

$$V(F \cup \{f\}) = \bigcup_k V(F \cup \{f_k\})$$

Bessere Ergebnisse liefert eine integrierte Variante von Buchbergeralgorithmus und Faktorisierung, der **Gröbnerfaktorisierer** der aber nur in wenigen CAS implementiert bzw. nicht explizit zugänglich ist.

Beispiel: $x\,y = 4, y^2 = x^3 - 1$. GBasis ist $(16\,x - y^2 - y^4, y^5 + y^3 - 64)$. $y^5 + y^3 - 64$ ist irreduzibel, kann also nicht weiter vereinfacht werden.

6.2 Resultanten und der Beweis des Extension Theorems

Resultanten und Nullstellen

Lemma 1 *$f, g \in k[x_1, \ldots, x_n]$ haben einen gemeinsamen Faktor h mit $\deg_{x_1}(h) > 0$ genau dann, wenn sie einen gemeinsamen Faktor h' mit $\deg_{x_1}(h') > 0$ in $k(x_2, \ldots, x_n)[x_1]$ haben.*

Folgt unmittelbar aus der Eindeutigkeit der Faktorzerlegung für Polynome: $f = h'f_1', g = h'g_1'$ in $k(x_2, \ldots, x_n)[x_1]$ mit $\deg_{x_1}(h') > 0$ haben gemeinsamen Hauptnenner $d \in k[x_2, \ldots, x_n]$. Dann gilt $d^2 f = h_1\, f_1, d^2 g = h_1\, g_1$ in $k[x_1, \ldots, x_n]$. Nimm nun irreduziblen Faktor von h_1 von positivem x_1-Grad.

Lemma 2 *$f, g \in k[x]$ vom Grad $l, m > 0$. Haben einen gemeinsamen nichttrivialen Faktor genau dann, wenn Polynome $A, B \in k[x]$ existieren mit*

(1) $A, B \neq 0$,

(2) $\deg_x(A) \leq m - 1$, $\deg_x(B) \leq l - 1$,

(3) $A\,f + B\,g = 0$.

Ist $f = h\,f_1, g = h\,g_1$, so ist $g_1 f - f_1 g = 0$ und man kann $A = g_1, B = -f_1$ nehmen.

Es ist $B \neq 0$ vorausgesetzt. Hätten die Polynome keinen gemeinsamen Faktor, dann wäre $\gcd(f, g) = 1$ und es gäbe Kofaktoren A', B' mit $A'f + B'g = 1$. Dann wäre

$$B = (A'f + B'g)B = A'B\,f + B'B\,g = A'B\,f - B'A\,f = (A'B - B'A)f.$$

Dann hätte B aber wenigstens den Grad l.

Die Frage der Existenz von A, B mit $A\,f + B\,g = 0$ kann auf lineare Algebra zurückgeführt werden. Setze mit unbestimmten Koeffizienten an

$$A = c_0 x^{m-1} + \cdots + c_{m-1}, B = d_0 x^{l-1} + \cdots + d_{l-1}$$

Die $(m+l)$-reihige Matrix zu diesem Problem der linearen Algebra bezeichnet man als die *Sylvester-Matrix* $Syl(f,g,x)$, ihre Determinante

$$Res(f,g,x) = det(Syl(f,g,x))$$

als *Resultante* der Polynome f und g.

Satz 27 *Für $f,g \in k[x]$ von positivem Grad ist $Res(f,g,x) \in k$ ein ganzzahliges Polynom in den Koeffizienten von f und g. f und g haben genau dann einen gemeinsamen nichttrivialen Faktor in $k[x]$, wenn $Res(f,g,x) = 0$ ist.*

Nach dem vorher Bewiesenen offensichtlich.

Beispiel: $f = 2\,x^2+3\,x+1$, $g = 7\,x^2+x+3$. Sylvestermatrix ist (4×4)-Matrix, $Res(f,g,x) = 153$.

Beispiel: $f = x\,y-1$, $g = x^2+y^2-4$. Als Polynome in x Sylvestermatrix (3×3)-Matrix, Determinante $y^4-4\,y^2+1$ ist Polynom in y.

Satz 28 *Für $f,g \in k[x]$ von positivem Grad $\deg(f) = l, \deg(g) = m$ gibt es Polynome $A,B \in k[x]$ vom Grad $\deg(A) \le m-1$, $\deg(B) \le l-1$ mit $A\,f + B\,g = Res(f,g,x)$.*

Beweis: Für $Res(f,g,x) = 0$ ist das klar. Sei also $Res(f,g,x) \neq 0$. Wir suchen eine Darstellung $A'f + B'g = 1$ mit $\deg(A') \le m-1$, $\deg(B') \le l-1$ und setzen dazu

$$A' = c_0x^{m-1} + \cdots + c_{m-1}, B' = d_0x^{l-1} + \cdots + d_{l-1} \tag{1}$$

mit unbestimmten Koeffizienten an. Als Bestimmungssystem erhalten wir ein lineares Gleichungssystem mit der Sylvestermatrix als Koeffizientenmatrix. Da für deren Determinante $\Delta = Res(f,g,x) \neq 0$ gilt, hat (1) eine eindeutig bestimmte Lösung und diese kann mit der Cramerschen Regel $\frac{\Delta_i}{\Delta}$ aufgeschrieben werden. Durchmultiplizieren mit Δ ergibt die behauptete Beziehung. $\square$

Anmerkung: Die Δ_i und damit auch A und B sind ganzzahlige polynomiale Kombinationen in den Koeffizienten von f und g.

Gegeben seien $f,g \in k[x_1,\ldots,x_n]$, $l,m > 0$

$$f = a_0x_1^l + \ldots + a_l, \quad g = b_0x_1^m + \cdots + b_m$$

mit $a_i, b_j \in k[x_2,\ldots,x_n]$ und $a_0 \neq 0, b_0 \neq 0$. Dann gilt:

- $Res(f,g,x_1)$ liegt im ersten Eliminationsideal $I(f,g) \cap k[x_2,\ldots,x_n]$.
- $Res(f,g,x_1) = 0$ genau dann, wenn f und g einen gemeinsamen Faktor in $k[x_1,\ldots,x_n]$ mit positivem x_1-Grad haben.

Folgt unmittelbar aus dem bisher gesagten. Sei K eine algebraisch abgeschlossene Erweiterung von k.

Lemma 3 *Für $f,g \in k[x]$ ist $Res(f,g,x) = 0$ genau dann, wenn f und g eine gemeinsame Nullstelle in K haben.*

Satz 29 *Seien $f, g \in k[x_1, \ldots, x_n]$, a_i, b_i wie oben und $I_1 = I(f,g) \cap k[x_2, \ldots, x_n]$ das erste Eliminationsideal. Ist $c = (c_2, \ldots, c_n) \in V_K(I_1) - V_K(a_0, b_0)$, so existiert ein $c_1 \in K$ mit $(c_1, c_2, \ldots, c_n) \in V_K(f,g)$.*

Beweis: Wir wissen $h = Res(f, g, x_1) \in I_1$, deshalb ist $h(c) = 0$. Sind $a_0(c), b_0(c) \neq 0$, so ist $h(c)$ genau die Resultante der Polynome $f(x_1, c)$ und $g(x_1, c)$ in $k(c)[x_1]$. $f(x_1, c)$ und $g(x_1, c)$ haben dann also eine gemeinsame Nullstelle c_1 wie behauptet.

Nach Voraussetzung kann aber einer der beiden Koeffizienten verschwinden (aber nicht beide). Sei also $a_0(c) \neq 0$, $b_0(c) = \cdots = b_{q-1}(c) = 0$, $b_q(c) \neq 0$. Ist $S = Syl(f, g, x_1)$, so entsteht $S' = Syl(f(x_1, c), g(x_1, c), x_1)$ durch Streichen der ersten q Zeilen und Spalten von S. $det(S')$ kann andererseits aus $det(S)$ durch Entwickeln nach den ersten q Spalten berechnet werden und es gilt $det(S) = a_0^q det(S')$. Also gilt $h(c) = a_0^q \cdot Res(f(x_1, c), g(x_1, c), x_1) = 0$ und es folgt wieder die Existenz einer gemeinsamen Nullstelle von $f(x_1, c)$ und $g(x_1, c)$. $\square$

In [COS] wird anders argumentiert: Ersetze im zweiten Fall das Paar (f, g) durch $(f, g + x_1^N f)$ mit genügend großem N. Dann haben beide Polynome den Leitkoffizienten a_0.

Verallgemeinerte Resultanten

Um das Extension Theorem im allgemeinen Fall zu beweisen, wird die *verallgemeinerte Resultante* eingeführt. Gegeben $f_1, \ldots, f_s$. Führe neue Variable $u_2, \ldots, u_s$ ein und setze

$$Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) u^\alpha$$

Die Resultante liegt im Ring $k[u_2, \ldots, u_s, x_2, \ldots, x_s]$ und $h_\alpha \in k[x_2, \ldots, x_s]$. Die Polynome h_α werden als *verallgemeinerte Resultante* bezeichnet.

Die h_α liegen in $I_1 = I(f_1, \ldots, f_s) \cap k[x_2, \ldots, x_n]$: Wir haben Kofaktoren

$$A\, f_1 + B(u_2 f_2 + \cdots + u_s f_s, x_1) = Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = h,$$

die sich als $A = \sum_\alpha A_\alpha u^\alpha$ und $B = \sum_\alpha B_\alpha u^\alpha$ mit $A_\alpha, B_\alpha \in k[x_1, \ldots, x_n]$ schreiben lassen.

$$\begin{aligned} h = \sum_\alpha h_\alpha u^\alpha &= \left(\sum_\alpha A_\alpha u^\alpha\right) f_1 + \left(\sum_\beta B_\beta u^\beta\right)\left(\sum_{i \geq 2} u^{e_i} f_i\right) \\ &= \sum_\alpha (A_\alpha f_1) u^\alpha + \sum_{i,\beta} B_\beta f_i u^{\beta + e_i} \\ &= \sum_\alpha (A_\alpha f_1) u^\alpha + \sum_\alpha \left(\sum_{\beta + e_i = \alpha} B_\beta f_i\right) u^\alpha \\ &= \sum_\alpha \left(A_\alpha f_1 + \sum_{\beta + e_i = \alpha} B_\beta f_i\right) u^\alpha \end{aligned}$$

Damit gilt

$$h_\alpha = \left(A_\alpha f_1 + \sum_{\beta + e_i = \alpha} B_\beta f_i\right) \in I_1.$$

Beweis des Extension Theorems

Beweis: Es sei $c = (c_2, \ldots, c_n)$ eine Nullstelle von I_1, die wir mit einer gemeinsamen Nullstelle $c_1 \in K$ von $f_1(x_1, c), \ldots, f_s(x_1, c)$ fortsetzen wollen, wobei wir $g_1(c) \neq 0$ annehmen können. Wir berechnen

$$h = \sum_\alpha h_\alpha u^\alpha = Res(f_1, u_2 f_2 + \cdots + u_s f_s, x_1).$$

Wie oben gezeigt gilt $h_\alpha \in I_1$ und damit $h_\alpha(c) = 0$ für alle α. Damit gilt aber auch $h(x_1, c, u_2, \ldots, u_s) = 0$.
Sei nun

$$g_2(c) \neq 0 \text{ und } f_2 \text{ habe einen größeren } x_1\text{-Grad als } f_3, \ldots, f_s. \tag{2}$$

Dann ist

$$h(x_1, c, u_2, \ldots, u_s) = Res(f_1(x_1, c), u_2 f_2(x_1, c) + \cdots + u_s f_s(x_1, c), x_1),$$

da die höchsten Terme nicht verschwinden. Aus dem Verschwinden der Resultante folgt, dass $f_1(x_1, c)$ und $t = u_2 f_2(x_1, c) + \cdots + u_s f_s(x_1, c)$ einen gemeinsamen Faktor in $K[x_1, u_2, \ldots, u_s]$ haben. Als Faktor von $f_1(x_1, c)$ kann er die u_i nicht enthalten. Als Teiler von t teilt er auch $f_2(x_1, c), \ldots, f_s(x_1, c)$, setze dazu $u_i = \delta_{ij}$.
Ist (2) nicht erfüllt, so ersetze die Basis durch

$$I = I(f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s)$$

mit einer geeignet hohen Potenz von x_1. Die Basis erfüllt dann (2). □

Der schwache Hilbertsche Nullstellensatz

Satz 30 *Ist über einem algebraisch abgeschlossenen Körper $V_K(I)$ die leere Menge, so gilt $I = k[x_1, \ldots, x_n]$.*

Beweis: Beweis mit Induktion nach n. Für $n = 1$ ist das gerade der Fundamentalsatz der Algebra.
Induktionsschritt: $I = I(f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ mit $V(I) = \emptyset$. Wir können annehmen, dass f_1 die Gestalt

$$f_1(x_1, \ldots, x_n) = c\, x_1^N + < \text{Terme mit } x_1\text{-Grad kleiner als } N >$$

mit $c \in K, c \neq 0$ hat. Anderenfalls mache nach Satz 26 Koordinatentransformation $x_i = x_i' + a_i\, x_1'$ mit geeigneten a_i und betrachte die Polynome in den neuen Variablen.
Betrachte nun das erste Eliminationsideal I_1. Wenn $V(I_1)$ nicht leer wäre, dann kann eine Nullstelle $(c_2, \ldots, c_n)$ nach dem Extension Theorem wegen $c \in k$ immer zu einer Nullstelle $(c_1, c_2, \ldots, c_n)$ von $V(I)$ fortgesetzt werden. Aber $V(I)$ ist leer, also auch $V(I_1)$ und damit $1 \in I_1$. Es folgt auch $1 \in I$. □

Der allgemeine Hilbertsche Nullstellensatz

Satz 31 *Ein Polynom $h \in k[x_1, \ldots, x_n]$ verschwindet auf den gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_s$ genau dann, wenn*

$$\exists n(h^n \in I(f_1, \ldots, f_s)).$$

Beweis: Ist $h^n \in I(f_1, \ldots, f_s)$, so folgt $V(h^n) = V(h) \supset V = V(f_1, \ldots, f_s)$.
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 J. 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 $r_0, r_\alpha \in S$ mit

$$1 = \sum r_\alpha(\mathbf{x}, t) f_\alpha(\mathbf{x}) + r_0(\mathbf{x}, t) \cdot (1 - h(\mathbf{x}) \cdot t).$$

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

$$h(\mathbf{x})^N = \sum \tilde{r}_\alpha(\mathbf{x}) f_\alpha(\mathbf{x}) + \tilde{r}_0(\mathbf{x}) \cdot 0,$$

also $h^N \in J$. □

6.3 Geometrie des Eliminationssatzes

Satz 32

(1) Sind $S_1 \subset S_2$ zwei Teilmengen des $\mathbb{A}^n$, so gilt $I(S_1) \supset I(S_2)$.

(2) Sind $I_1 \subset I_2$ zwei Ideale im Ring $R = k[x_1, \ldots, x_n]$, so gilt $V(I_1) \supset V(I_2)$.

(3) Ist W eine affine Varietät $W = V(f_1, \ldots, f_s)$ im $\mathbb{A}^n$, so gilt $V(I(W)) = W$.

(4) Ist S eine Teilmenge des $\mathbb{A}^n$, so ist $\overline{S} = V(I(S))$ der affine Abschluss von S.

Beweis: (1) und (2) sind offensichtlich.
(3) Jedes $f \in I(W)$ verschwindet nach Definition auf W, also gilt $W \subset V(I(W))$. Umgekehrt gilt $f_1, \ldots, f_s \in I(V)$ nach Definition von $I(V)$, also mit (1) $W = V(f_1, \ldots, f_s) \supset V(I(V))$ und folglich Gleichheit.
(4) Ist $W \supset S$ eine affine Varietät, so gilt mit (1) und (2) $W = V(I(W)) \supset V(I(S)) \supset S$. $V(I(S))$ ist also die kleinste affine Varietät, die S umfasst. □

Eliminationsideal und Projektionsabbildung

$V = V(f_1, \ldots, f_s) \subset \mathbb{C}^n$.
Projektionsabbildung $\pi_k : \mathbb{C}^n \to \mathbb{C}^{n-k}$ mit $\pi_k(a_1, \ldots, a_n) = (a_{k+1}, \ldots, a_n)$.
$I_k = I(f_1, \ldots, f_s) \cap k[x_{k+1}, \ldots, x_n]$

Lemma 4 $\pi_k(V) \subset V(I_k)$

$\pi_k(V)$ besteht aus genau den partiellen Lösungen, die sich zu einer vollständigen Lösung fortsetzen lassen.

Beispiel: $xy = 1, xz = 1$. $\pi_1(V) = \{(a, a) : a \neq 0\}$ echte Teilmenge von $V(I_1)$.

Aus dem Extension Theorem folgt unmittelbar

$$V(I_1) = \pi_1(V) \cup (V(g_1, \ldots, g_s) \cap V(I_1)).$$

Was kann über den „Rest“ $W = V(g_1, \ldots, g_s) \cap V(I_1)$ gesagt werden?

Beispiel: $(y - z)x^2 + xy = 1, (y - z)x^2 + xz = 1$ beschreibt dasselbe V wie $xy = 1, xz = 1$, aber $W = V(y - z) = V(I_1)$. Also kann in diesem Fall nichts über die Fortsetzung partieller Lösungen gesagt werden.

Da kann man aber nachbessern.

Satz 33 (Closure Theorem) *$V = V(f_1, \ldots, f_s) \subset \mathbb{C}^n$, I_k k-tes Eliminationsideal. Dann gilt*

(1) $V(I_k)$ ist die kleinste affine Varietät, die $\pi_k(V)$ enthält, d.h. es gilt $V(I_k) = \overline{\pi_k(V)}$.

(2) Ist $V \neq \emptyset$, dann gibt es eine Varietät $W \subsetneq V(I_k)$, so dass $V(I_k) - W \subset \pi_k(V)$.

Beweis: (1) Es ist zu zeigen, dass $V(I_k) = V(I(\pi_k(V)))$ gilt. Wegen $\pi_k(V) \subset V(I_k)$ (Lemma) ist nur $V(I_k) \subset V(I(\pi_k(V)))$ zu zeigen.

Sei $f \in J = I(\pi_k(V))$, also ein Polynom in $k[x_{k+1}, \ldots, x_n]$ mit $f(a_{k+1}, \ldots, a_n) = 0$ für alle $(a_{k+1}, \ldots, a_n) \in \pi_k(V)$. Betrachten wir f als Polynom in $k[x_1, \ldots, x_n]$ (in dem die Variablen $x_1, \ldots, x_k$ nicht vorkommen), so gilt $f(a_1, a_2, \ldots, a_n) = 0$ für alle $(a_1, a_2, \ldots, a_n) \in V$. Nach Hilberts Nullstellensatz gibt es dann ein $N > 1$ mit $f^N \in I(f_1, \ldots, f_s)$. Andererseits ist $f^N \in k[x_{k+1}, \ldots, x_n]$ und somit auch $f^N \in I_k$. Damit gilt $V(J) \supset V(I_k)$: Ist $a \in V(I_k)$, so verschwinden auch alle $f \in J$ auf a, denn es ist $f^N \in I_k$ und damit $f(a)^N = 0$, also auch $f(a) = 0$.

(2) wird nur für $k = 1$ gezeigt. Bezeichnungen wie aus dem Extension Theorem und $W = V(g_1, \ldots, g_s) \cap V(I_1)$. Ist $W \subsetneq V(I_1)$ so sind wir fertig. Ist $V(g_1, \ldots, g_s) \supset V(I_1)$, so gilt

$$V = V(f_1, \ldots, f_s) = V(f_1, \ldots, f_s, g_1, \ldots, g_s)$$

$\supset$ ist klar, da rechts mehr Polynome stehen. Sei $a = (a_1, \ldots, a_n) \in V$. Da $(a_2, \ldots, a_n) \in \pi_1(V) \subset V(I_1)$, verschwinden nicht nur die f_i, sondern auch die g_i auf a.

Ersetze nun $f_i' = f_i - g_i x_1^{N_i}$. Es gilt

$$V(f_1, \ldots, f_s, g_1, \ldots, g_s) = V(f_1', \ldots, f_s', g_1, \ldots, g_s)$$

und die f_i' sind entweder gleich null oder haben einen x_1-Grad kleiner als N_i. Nun können wir das Spiel fortsetzen, bis entweder $W \subsetneq V(I_1)$ oder alle f_i' gleich null werden. Dann enthält das letzte System aber kein x_1 und alle $x_1 \in \mathbb{C}$ sind Lösung. In dem Fall ist $\pi_1(V) = V(I_1)$. □

Beispiel: $(y - z)\, x^2 + x\, y = 1, (y - z)\, x^2 + x\, z = 1$. $g_1 = g_2 = y - z$. $W = I(y - z) = I_1$.

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

7 Das algebraisch-geometrische Wörterbuch

7.1 Das Radikal eines Ideals

Betrachten wir die Beziehung zwischen den Operatoren $I()$ und $V()$, die einer gegebenen Teilmenge $W \subset \mathbb{A}^n_K$ das Ideal der auf ihr verschwindenden Polynome bzw. einem gegebenen Ideal $J \subset R$ die Menge seiner gemeinsamen Nullstellen (über einer algebraisch abgeschlossenen Erweiterung K des Grundkörpers k) zuordnet.

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

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

Definition 11 *Für ein Ideal $J \subset R$ bezeichnen wir die Menge*

$$rad(J) := \{f \in R \ : \ \exists\, m \ f^m \in J\}$$

als das Radikal *von J.*

Das Radikal eines Ideals ist wieder ein Ideal (Übungsaufgabe).

Satz 34 *Ist $f = f_1^{a_1} \cdot \ldots \cdot f_s^{a_s}$ die Faktorzerlegung von f, so wird $rad(f)$ von $f_{red} = f_1 \cdot \ldots \cdot f_s$ erzeugt.*

Beweis: $g \in rad(f)$, dann ist $g^m \in (f)$, also $g^m = f\,a$ und damit $f_1 | g$ für $i = 1, \ldots, s$. □

Der Hilbertsche Nullstellensatz lässt sich auch in folgender Form anschreiben.

Satz 35 *Ist $J \subset R = k[x_1, \ldots, x_n]$ ein Ideal und $V = V_K(J)$, so gilt $I(V) = rad(J)$.*

Definition 12 *Ein Ideal $J \subset R$ mit $J = rad(J)$ nennen wir* Radikalideal.

Für ein Polynom f mit der Zerlegung $f = f_1^{a_1} \cdot \cdots \cdot f_k^{a_k}$ in irreduzible Faktoren bezeichnet man $f_{red} = f_1 \cdot \cdots \cdot f_k$ als *quadratfreien Anteil.*

Satz 36 *Das Radikal des Ideals $I(f)$ wird von f_{red} erzeugt.*

Diese Aussage folgt unmittelbar aus der Eindeutigkeit der Faktorzerlegung.

Im Allgemeinen ist es schwierig, eine Basis von $\mathrm{rad}(I)$ zu berechnen.

Ein Radikalenthaltenseinstest

Satz 37 *Für ein Ideal $I = I(f_1, \ldots, f_s) \subset R = k[x_1, \ldots, x_n]$ und $f \in I$ gilt*

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

Beweis: Sei $J = I \cdot R[t] + I(1 - t\,f)$. Dann gilt $1 \equiv t\,f \pmod{J}$. Ist $f \in \mathrm{rad}(I)$, so gilt $f^N \in I$ für ein $N > 0$ und damit $1 \equiv (t\,f)^N \equiv 0 \pmod{J}$, also $J = I(1)$.
Ist umgekehrt $J = I(1)$, so gibt es wie im Beweis des allgemeinen Hilbertschen Nullstellensatzes eine Darstellung

$$1 = \sum r_\alpha(\mathbf{x}, t) f_\alpha(\mathbf{x}) + r_0(\mathbf{x}, t) \cdot (1 - f(\mathbf{x}) \cdot t)$$

und wie dort weiter hergeleitet eine Darstellung

$$f(\mathbf{x})^N = \sum \tilde{r}_\alpha(\mathbf{x}) f_\alpha(\mathbf{x}),$$

also $f^N \in I$. $\square$
Dieses Kriterium kann zum Test $f \in \mathrm{rad}(I)$ verwendet werden, womit der **Radikalenthaltenseinstest** auf die Frage des Erkennens eines trivialen ideals zurückgeführt ist.
Beispiel:

```
Use R::=QQ[t,x,y,z],Lex;
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];
F:=x*z-y^2;
```

Wir wollen untersuchen, ob $f \in \mathrm{rad}(I(B))$ gilt.
Wir berechnen dazu die Gröbnerbasis von $I + (1 - f\,t)$

```
G:=Ideal(B)+Ideal(F*t-1);
GBasis(G);
```

$$[-1]$$

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

```
NF(F^2,Ideal(B));
```

$$0$$

Für den Radikalenthaltenseinstest kann eine beliebige Termordnung gewählt werden.

Der Korrespondenzsatz, Teil 1

Es gilt folgender Zusammenhang zwischen affinen Varietäten, Idealen und Radikalidealen:

Satz 38 *Sei*

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

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

1. *die Bilder unter V sind genau die affinen Teilmengen des $\mathbb{A}^n$,*
2. *die Bilder unter I sind genau die Radikalideale in R,*
3. *für jede Teilmenge $W \in \mathbb{A}^n$ gilt $V(I(W)) = \overline{W}$,*
4. *für jedes Ideal $J \subset R$ gilt $I(V(J)) = rad(J)$,*
5. *$J_1 \subseteq J_2 \Rightarrow V(J_1) \supseteq V(J_2)$,*
6. *$V_1 \subseteq V_2 \Rightarrow I(V_1) \supseteq I(V_2)$.*

Beweis: $V(I(V)) = V$: $V = V(f_1, \ldots, f_s)$. Jedes $f \in I(V)$ verschwindet auf V, also $V \subset V(I(V))$. Umgekehrt $f_1, \ldots, f_s \in I(V)$ und damit $I(f_1, \ldots, f_s) \subset I(V)$. Dann aber auch $V(I(V)) \supset V(f_1, \ldots, f_s) = V$. Damit folgt $V(I(V)) = V$.

4. folgt aus dem Hilbertschen Nullstellensatz.

Zu 3.: Ist $W \subset V$ für eine affine Varietät V, so gilt $I(W) \supset I(V)$ und weiter $V(I(W)) = V(I(V))$ und wie eben gezeigt $V(I(V)) = V$. Also ist $V(I(W))$ in allen affinen Varietäten enthalten, die W enthalten.

Es sind nur noch die Aussagen 5. und 6. zu zeigen. Deren Gültigkeit ist aber offensichtlich. □

7.2 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 Linearkombinationen zugelassen werden.

Beispiel: $J_1 = I(x_1 + x_2, x_2x_3, x_3^2 - x_4x_5),\ J_2 = I(x_1 + x_2, x_2x_4, x_4^2 - x_5^2)$

Definition 13 *Als Summe der Ideale $J_1, J_2 \subset R$ bezeichnet man die Menge*

$$J_1 + J_2 := \{j_1 + j_2 \ : \ j_1 \in J_1,\ j_2 \in J_2\}$$

Beispiele:

$J_1 + J_2 = I(x_1 + x_2, x_2x_3, x_2x_4, x_3^2 - x_4x_5, x_4^2 - x_5^2)$

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

Satz 39 *Die Summe von zwei Idealen ist wieder ein Ideal. Sind B_i Basen der Ideale $J_i, i = 1, 2$, so ist $B = B_1 \bigcup B_2$ eine Basis von $J_1 + J_2$.*

Betrachten wir die analoge Konstruktion für das Produkt statt der Summe.

Definition 14 *Als Produkt der Ideale $J_1, J_2 \subset R$ bezeichnet man die Menge*

$$J_1 \cdot J_2 := \left\{ \sum_k j_{1k} \cdot j_{2k} \ : \ j_{1k} \in J_1, \ j_{2k} \in J_2 \right\}$$

Beispiele:
$J_1 \cdot J_2 = I((x_1+x_2)^2, (x_1+x_2)x_2x_4, \ldots, (x_3^2 - x_4x_5)(x_4^2 - x_5^2))$ (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 40 *Das Produkt von zwei Idealen ist wieder ein Ideal. Sind B_i Basen der Ideale $J_i, i = 1, 2$, so ist $B = \{f \cdot g \ : \ f \in B_1, \ g \in B_2\}$ eine Basis von $J_1 \cdot J_2$.*

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

Satz 41 *Der Durchschnitt zweier Ideale ist wieder ein Ideal und es gilt stets $J_1 \cdot J_2 \subseteq J_1 \cap J_2$.*

Beispiel: Betrachten wir den Polynomring $k[x]$ in einer Variablen. Das ist ein Hauptidealring. Für $J_1 = I(f), J_2 = I(g)$ gilt

$$J_1 + J_2 = I(\gcd(f,g)) \qquad J_1 \cdot J_2 = I(f \cdot g) \qquad J_1 \cap J_2 = I(\operatorname{lcm}(f,g)).$$

Das gilt allgemein für Ideale, die von einem Element erzeugt werden: $I(f) \cap I(g) = I(\operatorname{lcm}(f,g))$. Folgt aus der Eindeutigkeit der Faktorzerlegung.
Summe, Produkt und Durchschnitt von PP-Idealen sind wieder PP-Ideale, denn für PP-Ideale $I_1, I_2 \subset R$ gilt offensichtlich

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

Beispiel: $I(x^3y, y^4) \cap I(x^5, x^2y^2) = I(x^2y^4, x^3y^2, x^5y)$
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.) $J_1 \cap J_2 = I(x_2x_3x_5^2, x_2x_4x_5, x_2x_3x_4, x_1 + x_2, (x_4^2 - x_5^2)(x_3^2 - x_4x_5))$
Die Basis eines Idealdurchschnitts kann jedoch im Allgemeinen nicht nach einer einfachen Vorschrift aus den Basen der Teilideale berechnet werden. Dafür verhält sich der Durchschnitt zweier Ideale besser bzgl. der Korrespondenz zwischen Idealen und Varietäten als das Produkt.

Berechnung des Idealdurchschnitts

Betrachten wir die beiden Ideale

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

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

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

Hinweis: Dazu sind nur für alle möglichen Leittermkombinationen der Basiselemente die jeweiligen S-Polynome zu untersuchen.

Grundlage des Verfahrens zur Berechnung des Idealdurchschnitts ist der folgende

Satz 42 *Sind I_1, I_2 zwei Ideale im Polynomring $R = k[\boldsymbol{x}]$ und t eine neue Variable, so gilt*

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

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. $f(x) \in I_1 \cdot t\,R[t] + I_2 \cdot (1-t)\,R[t]$ 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 den Idealdurchschnitt mit CoCoA:

```
Use R::=QQ[t,x,y],Lex;
I1:=[x^3-x^2*y,x*y^2-y^3];
I2:=[x^3-x*y^2,x^2*y-y^3];
J:=Concat([t*F | F In I1],[(1-t)*F | F In I2]);
ReducedGBasis(Ideal(J));
[tx^2y - ty^3 - x^2y + y^3, txy^2 - ty^3,
    x^3 - x^2y - xy^2 + y^3, x^2y^2 - y^4]
-------------------------------
Elim(t,Ideal(J));
Ideal(-x^3 + x^2y + xy^2 - y^3, -x^2y^2 + y^4)
-------------------------------
```

Dies liefert den Idealdurchschnitt

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

Alternativ hätten wir auch gleich `Intersection(Ideal(I1),Ideal(I2))` berechnen können.

Aufgabe: Berechnen Sie den Idealdurchschnitt

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

Diesen Algorithmus kann man folgendermaßen auf die Berechnung des Durchschnitt mehrerer Ideale erweitern:

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

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

Der Beweis verläuft wie im oben betrachteten Fall.

CoCoA kennt zur Berechnung von Idealdurchschnitten die Kommandos

```
Intersection(E_1:IDEAL,...,E_n:IDEAL):IDEAL
IntersectionList(L:LIST):OBJECT
```

Verallgemeinerung des Chinesischen Restsatzes

Gegeben sind Ideale $I_1 \ldots, I_k \subset R = k[x_1, \ldots, x_n]$ und Polynome $f_1, \ldots, f_k \in R$. Untersuche, ob das System

$$\begin{aligned} h &\equiv f_1 \pmod{I_1} \\ &\ldots \\ h &\equiv f_k \pmod{I_k} \end{aligned}$$

eine Lösung hat und bestimme diese gegebenenfalls.

Antwort: Mit $J = I_1\, y_1 + \ldots I_k\, y_k + I(y_1 + \ldots + y_k - 1)$ und $f = y_1 f_1 + \cdots + y_k f_k$ berechne $h = NF(f, J)$ bzgl. einer Ordnung, die $y_1, \ldots, y_k$ eliminiert. Das System ist genau dann lösbar, wenn $h \in k[x_1, \ldots, x_n]$ gilt.

Ist das System lösbar, so gilt wegen $y_i h \equiv y_i f_i \pmod{J}$

$$f = (y_1 + \cdots + y_k)h \equiv h \pmod{J}$$

Ist umgekehrt $h = NF(f, J) \in k[x_1, \ldots, x_n]$, so können wir $y_i = 1$ und $y_j = 0$ für $j \neq i$ setzen. f reduziert dabei zu f_i, h ändert sich nicht. Aus $f \equiv h \pmod{J}$ folgt dann $f_i \equiv h \pmod{I_i}$ für $i = 1, \ldots, k$.

7.2.1 Korrespondenzsatz, Teil 2

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

Satz 43 *(Korrespondenzsatz, Teil 2) Mit den Bezeichnungen aus dem Korrespondenzsatz, Teil 1, gilt für Ideale $J_1, J_2 \subset R$ weiterhin*

7. $V(J_1 + J_2) = V(J_1) \bigcap V(J_2)$ *und*
8. $V(J_1 \cdot J_2) = V(J_1 \bigcap J_2) = V(J_1) \bigcup V(J_2)$.

Beweis: Wegen $J_1 \cdot J_2 \subseteq J_1 \cap J_2 \subseteq J_1, J_2$ gilt

$$V(J_1 \cdot J_2) \supseteq V(J_1 \cap J_2) \supseteq V(J_1) \cup V(J_2).$$

Es bleibt also nur $V(J_1 \cdot J_2) \subseteq V(J_1) \cup V(J_2)$ zu zeigen. $a \in V(J_1 \cdot J_2)$ heißt aber insbesondere $f(a)g(a) = 0$ für alle $f \in J_1, g \in J_2$. Ist $a \notin V(J_1)$, so gibt es ein $f \in J_1$ mit $f(a) \neq 0$, was $g(a) = 0$ für alle $g \in J_2$ nach sich zieht. Also wäre dann $a \in V(J_2)$. $\square$

Aufgabe: 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. (Übungsaufgabe)

Idealquotienten

Betrachte $V \setminus W$ für affine Varietäten. Ist im Allgemeinen keine affine Varietät, aber wir können nach dem Zarisski-Abschluss $\overline{V \setminus W}$ fragen.

Als *Idealquotienten* bezeichnet man

$$I : J = \{f \in R \ : \ \forall g \in J : f\, g \in I\}\,.$$

Als *stabilen Idelaquotienten* bezeichnet man

$$I : J^\infty = \{f \in R \ : \ \forall g \in J \exists\, n : f\, g^n \in I\}.$$

Beides sind Ideale.

Satz 44 *Sind I, J Ideale in $k[x_1, \ldots, x_n]$. Dann gilt*

$$V(I : J) \supset \overline{V(I) \setminus V(J)}.$$

Ist darüber hinaus k algebraisch abgeschlossen und I ein Radikalideal, so gilt $V(I : J) = \overline{V(I) \setminus V(J)}$.

Beweis: Es ist zu zeigen $I(V(I : J)) = I(V(I) \setminus V(J))$.

Zeige $I : J \subset I(V(I) \setminus V(J))$. Sei $f \in I : J$ und $x \in V(I) \setminus V(J)$. Dann ist $f\, g \in I$ für alle $g \in J$. Wähle ein g mit $g(x) \neq 0$. Wegen $f\, g \in I$ ist $f(x)g(x) = 0$ und damit $f(x) = 0$. Es ist also $f \in I(V(I) \setminus V(J))$.

Daraus folgt $V(I : J) \supset V(I(V(I) \setminus V(J)) = \overline{V(I) \setminus V(J)}$.

Für die zweite Behauptung zeige $I(V(I : J)) \supset I : J \supset I(V(I) \setminus V(J))$. Sei $x \in V(I : J)$, was äquivalent ist zu folgender Aussage über h

$$\text{Ist } hg \in I \text{ für alle } g \in J, \text{ so ist } h(x) = 0.$$

Sei $h \in I(V(I) \setminus V(J))$. Für $g \in J$ verschwindet hg auf $V(I)$, weil h auf $V(I) \setminus V(J)$ verschwindet und g auf $V(J)$. Nach dem Nullstellensatz gilt also $hg \in rad(I) = I$ und damit $h \in I : J$.
Also ist $I(V(I) \setminus V(J)) \subset I : J$ und damit $V(I(V(I) \setminus V(J)) = \overline{V(I) \setminus V(J)} \supset V(I : J)$ □

Satz 45 *Sind V und W Varietäten im k^n, so gilt*

$$I(V) : I(W) = I(V \setminus W).$$

Beweis: $I = I(V)$, $J = I(W)$. Aus $V(I : J) \supset \overline{V(I) \setminus V(J)}$ folgt $I : J \subset I(V(I : J)) \subset I(V(I) \setminus V(J)) = I(V \setminus W)$. Ist umgekehrt $f \in I : J$ und $x \in V \setminus W$, so wähle $g \in J$ mit $g(x) \neq 0$. Dann ist $fg \in I$, verschwindet also auf x und damit $f(x) = 0$. Also $f \in I(V - W)$.
□

Eigenschaften:

$$J : (f) \subseteq J : (f^2) \subseteq \ldots \subseteq J : (f^\infty)$$

und es gilt Gleichheit nach endlich vielen Schritten, da $J : (f^\infty)$ eine endliche Basis hat, da $f^n \cdot r \in J$ nur auf dessen Basiselementen $r_1, \ldots, r_k$ geprüft werden muss.

Aufgabe: Zeigen Sie, dass aus $J : (f^m) = J : (f^{m+1})$ bereits $J : (f^m) = J : (f^\infty)$ folgt.

Aufgabe: Zeigen Sie, dass für ein Radikalideal J stets $J : (f) = J : (f^\infty)$ gilt und dieses Ideal wieder ein Radikalideal ist.

Zeigen Sie weiter, dass für ein beliebiges Ideal $\mathrm{rad}(J : (f^\infty)) = \mathrm{rad}(J : (f)) = \mathrm{rad}(J) : (f)$ gilt.

Berechnung von Idealquotienten und stabilen Idealquotienten

Für $J = I(f_1, \ldots, f_r)$ gilt

$$I : J = \cap_k \left(I : (f_k)\right) \qquad \text{und} \qquad I : J^\infty = \cap_k \left(I : (f_k^\infty)\right),$$

so dass man die Berechnung dieser Ideale auf die Berechnung von Idealquotienten bzgl. Polynomdivisoren und die Berechnung von Idealdurchschnitten zurückführen kann.

Damit kann man die Berechnung der Quotienten von Idealen auf die Berechnung der Quotienten bzgl. eines einzelnen Polynoms reduzieren. 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* (oder Saturation) von I nach c.

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

Satz 46 *Ist $R = k[\boldsymbol{x}]$, $I \subset R$ ein Ideal, $c(x) \in R$ und t eine neue Variable, so gilt*

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

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 $B = \{f_1(x), \ldots, f_s(x)\}$ 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

$$f\,c^k = r_1(x)f_1(x) + \ldots + r_s(x)f_s(x)$$

in R und damit

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

Ist umgekehrt

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

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

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

Damit haben wir den Satz bewiesen. □

Die Berechnung von $I : J$ bzw. $I : J^\infty$ kann nun auf die Berechnung von Idealdurchschnitten zurückgeführt werden.

Alternativ kann man die Berechnung der Quotienten bzgl. eines Ideals auch auf die Berechnung des Quotienten bzgl. eines Polynoms in einer zusätzlichen Variablen zurückführen, was den Aufwand deutlich vermindert: Sei $J = I(c_0, \ldots, c_s)$ und $c(y) := c_0 + c_1\,y + \ldots + c_s\,y^s \in R[y]$ ein Polynom in einer neuen Variablen y. Ist $I \subset R$ ein Ideal und $f(x,y) \in I\,R[y]$ ein Polynom im Erweiterungsideal, so kann f in seine y-homogenen Komponenten $f = f_0 + f_1\,y + \ldots + f_k y^k$ mit $f_i \in R$ zerlegt werden. Man überzeugt sich leicht, dass aus $f \in I\,R[y]$ stets $f_i \in I$ für alle i folgt.

Satz 47 *Es gilt*

$$I : J = \cap(I : c_i) = (I\,R[y] : c(y)) \cap R$$

und

$$I : J^\infty = \cap(I : c_i^\infty) = (I\,R[y] : c(y)^\infty) \cap R$$

Beweis: Für $f \in R$ gilt $f \in I : J$ genau dann, wenn

$$f \cdot c(y) = (fc_0) + (fc_1)y + \ldots + (fc_k)y^k \in I\,R[y],$$

da (fc_i) die homogene Komponente vom y-Grad i in $f \cdot c(y)$ ist. □

CoCoA kennt zur Berechnung von Idealquotienten deshalb nur die Kommandos

```
Colon(M:IDEAL,N:IDEAL):IDEAL /* oder */ M : N
Saturation(I:IDEAL,J:IDEAL):IDEAL
```

Die Idealberechnung bzgl. eines Polynoms als Divisor kann durch das davon erzeugte Hauptideal als Divisor simuliert werden.

Idealquotienten und Primideale:

Satz 48 *Ist P ein Primideal, so gilt*

$$P : (f) = P : (f^\infty) = \begin{cases} (1) & \text{für } f \in P \\ P & \text{für } f \notin P \end{cases}$$

Beweis: Zu zeigen ist nur $P : (f^\infty) \subseteq P$ für $f \notin P$. Für $r \in P : (f^\infty)$ gilt aber $f^m r \in P$ für ein $m \in \mathbb{N}$ und wegen der Primidealeigenschaft auch $r \in P$. □

7.3 Irreduzible Komponenten

Der Darstellung affiner Varietäten als Vereinigung anderer solcher Varietäten entsprechen Durchschnitte der zugehörigen Verschwindungsideale. Es ergibt sich die Frage, ob eine solche Zerlegung stets nach endlich vielen Schritten mit nicht weiter zerlegbaren Komponenten endet.

Unabhängig von einer Antwort auf diese Frage definieren wir deshalb

Definition 15 *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.

Satz 49 *V ist genau dann eine irreduzible Varietät, wenn $P = I(V)$ ein Primideal ist.*

Beweis: Ist V eine 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 $J := I(V)$ einer irreduziblen Varietät ist also ein Primideal.

Umgekehrt, wäre für ein Primideal P die Varietät $V = V(P) = V_1 \cup V_2$ Vereinigung zweier echter Teilvarietäten, so wäre $P = I(V) = I(V_1) \cap I(V_2) = J_1 \cap J_2$ der Durchschnitt zweier echt größerer Ideale. Wählen wir $f_1 \in J_1 \setminus P,\ f_2 \in J_2 \setminus P$, so ist $f_1 \cdot f_2 \in J_1 \cdot J_2 \subset J_1 \cap J_2 = P$, was der Primidealeigenschaft von P widerspricht. □

Satz 50 *Ist f irreduzibel, so ist $V(f)$ irreduzibel.*

Beweis: Wäre $V(f) = V_1 \cup V_2$, so wäre $I(V(f)) = I(f) \subset I(V_1) \cap I(V_2)$. Für $f_1 \in I(V_1) \setminus I(f), f_2 \in I(V_2) \setminus I(f)$ ist also $f_1 f_2 \in I(f)$ und damit $f_1 f_2 = f\,a$. Dann muss aber eins der beiden f_i durch f teilbar sein, ein Widerspruch. □

Satz 51 *Für $a_1, \ldots, a_n \in k$ ist $I = I(x_1 - a_1, \ldots, x_n - a_n)$ ein maximales Ideal. Ist k algebraisch abgeschlossen, so gilt auch die Umkehrung.*

Beweis: Sei $f \notin I$, Dann ist $NF(f, I(x_1 - a_1, \ldots, x_n - a_n))$ ein Polynom vom Grad 0 und damit invertierbar. Also ist I maximal.

Umgekehrt ist nach dem Hilbertschen Nullstellensatz $V(I) \neq \emptyset$, also gibt es $(a_1, \ldots, a_n) \in V(I)$. Dann gilt

$$I(x_1 - a_1, \ldots, x_n - a_n) \supset I(V(I)) = rad(I) \supset I.$$

Da I maximal ist, gilt Gleichheit. $\square$

Im Fall eines algebraisch abgeschlossenen Körpers k gibt es also eine eineindeutige Korrespondenz zwischen Punkten $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ und maximalen Idealen in $R = k[x_1, \ldots, x_n]$.

Parametrisierte Varietäten

Regulär parametrisierte Varietäten

Sei k ein unendlicher Körper, V eine regulär parametrisierte Varietät sowie

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

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.

ϕ induziert eine 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 $V = \overline{im(\phi)}$ mit $im(\phi) = \big\{(\phi_1(a), \ldots, \phi_n(a)) : a \in \mathbb{A}^d\big\}$ genau für $f(\phi_1(a), \ldots, \phi_n(a)) = f(\phi(a)) = 0$, d.h. wenn $f \in ker(\phi^*)$ gilt. Hierbei steht $ker(\phi^*) = \{u \in R : \phi^*(u) = 0\}$ für den *Kern* des Ringhomomorphismus $\phi^* : R \longrightarrow R'$.

Die Abbildung $\phi : \mathbb{A}^d \longrightarrow \mathbb{A}^n$ kann man durch

$$\mathbb{A}^d \xrightarrow{\phi_0} \mathbb{A}^d \times \mathbb{A}^n \xrightarrow{\pi} \mathbb{A}^n$$

führen, wobei $\phi_0 : \mathbb{A}^d \longrightarrow \mathbb{A}^d \times \mathbb{A}^n$ durch $(t_1, \ldots, t_d) \mapsto (t_1, \ldots, t_d, \phi_1(\mathbf{t}), \ldots, \phi_n(\mathbf{t}))$ definiert wird ($im(\phi_0)$ bezeichnet man auch als den Graphen von ϕ) und $\pi : \mathbb{A}^d \times \mathbb{A}^n \longrightarrow \mathbb{A}^n$ die Projektion auf den zweiten Summanden ist. π^* ist dann die Einbettung von $k[x_1, \ldots, x_n]$ in $k[t_1, \ldots, t_d, x_1, \ldots, x_n]$ und

$$ker(\phi^*) = ker(\phi_0^* \circ \pi^*) = ker(\phi_0^*) \cap k[x_1, \ldots, x_n]$$

das Ideal, das man aus $ker(\phi_0^*) \subset k[t_1, \ldots, t_d, x_1, \ldots, x_n]$ durch Elimination der Variablen $t_1, \ldots, t_d$ bekommt.

Dieses Ideal kann man aber genau beschreiben: $ker(\phi_0^*)$ fällt mit

$$J := I(x_1 - \phi_1(\mathbf{t}), x_2 - \phi_2(\mathbf{t}), \ldots, x_n - \phi_n(\mathbf{t}))$$

zusammen. Offensichtlich gilt $ker(\phi_0^*) \supseteq J$, da die Basiselemente von J unter ϕ_0^* verschwinden. Wegen $x_i \equiv \phi_i(t) \pmod J$ gilt für $f \in k[t_1, \ldots, t_d, x_1, \ldots, x_n]$ aber auch

$$f(t_1, \ldots, t_d, x_1, \ldots, x_n) \equiv f(t_1, \ldots, t_d, \phi_1(\mathbf{t}), \ldots, \phi_n(\mathbf{t})) = \phi_0^*(f) \pmod J.$$

Aus $f \in \ker(\phi_0^*)$ folgt also $f \equiv 0 \pmod J$ und somit bereits $f \in J$.
Damit bekommen wir die folgende Beschreibung des Verschwindungsideals einer regulär parametrisierten affinen Varietät:

Satz 52 *Ist $V = \overline{im(\phi)}$ eine regulär parametrisierte Varietät im $\mathbb{A}^n$ und $\phi : \mathbb{A}^d \longrightarrow \mathbb{A}^n$ die zugehörige Parametrisierungsabbildung, so gilt*

$$I(V) = ker(\phi^*) = I(x_1 - \phi_1(\boldsymbol{t}), x_2 - \phi_2(\boldsymbol{t}), \ldots, x_n - \phi_n(\boldsymbol{t})) \cap k[x_1, \ldots, x_n].$$

Beispiel: Betrachten wir noch einmal die Tangentialfläche T an die Kubik

$$C = \left\{(t, t^2, t^3) \ : \ t \in \mathbb{C}\right\},$$

die durch die Abbildung $(t, u) \mapsto \left(x = t + u, y = t^2 + 2\,u\,t, z = t^3 + 3\,u\,t^2\right)$ gegeben ist. $I(T)$ können wir berechnen, indem wir im Ideal

$$I = I\left(x - (t + u), y - \left(t^2 + 2\,u\,t\right), z - \left(t^3 + 3\,u\,t^2\right)\right)$$

die Parameter t und u eliminieren.

```
Use R::=QQ[t,u,x,y,z],Lex;
I:=Ideal(x-(t+u), y-(t^2+2*u*t), z-(t^3+3*u*t^2));
Elim([t,u],I);
ideal(4*x^3*z -3*x^2*y^2 -6*x*y*z +4*y^3 +z^2)
```

Das Verschwindungsideal $I(T)$ wird (wie für eine Fläche im $\mathbb{A}^3$ 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.
Durch Parametrisierungen gegebene Varietäten sind irreduzibel.

Satz 53 *Sei k ein unendlicher Körper. Eine Varietät V, die durch eine polynomiale Parametrisierung*

$$x_i = \phi_i(t_1, \ldots, t_d), i = 1, \ldots n$$

gegeben ist, ist irreduzibel.

Beweis: $I(V) = ker(\phi^*) = {\phi^*}^{-1}(0)$ ist als Urbild eines Primideals unter einem Ringhomomorphismus selbst wieder ein Primideal. □

Rational parametrisierte Varietäten

Ähnliche Aussagen sind auch für rational parametrisierte Varietäten möglich.
Gegeben ist eine Varietät

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

wobei $\phi_i(\mathbf{t}) \in k(\mathbf{t})$ rationale Funktionen in $\mathbf{t} = (t_1, \ldots, t_d)$ sind und W die Varietät, auf der eine dieser rationalen Funktionen nicht definiert ist. Gesucht ist das Verschwindungsideal $I(V)$ dieser Varietät.
Wir können annehmen, dass die rationalen Funktionen $\phi_i(\mathbf{t}) = f_i(\mathbf{t})/g(\mathbf{t})$ 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

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

mit $W = V(g)$ auffassen, wobei $V = \overline{im\,\phi}$ und $I(V) = Ker\,(\phi^*)$ gilt. ϕ^* ist hierbei die Abbildung

$$\phi^* : k[\mathbf{x}] \longrightarrow k(\mathbf{t}) \qquad \text{via} \qquad x_i \mapsto \frac{f_i(\mathbf{t})}{g(\mathbf{t})},$$

wobei $\mathbf{x} = (x_1, \ldots, x_n)$ 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.

$$k[\mathbf{x}] \xrightarrow{\psi_1} k[\mathbf{t}, y] \xrightarrow{\psi_2} k(\mathbf{t})$$

Wie im Fall regulärer Parametrisierungen erweitern wir ψ_1 zu einer Abbildung

$$k[\mathbf{x}] \longrightarrow k[\mathbf{x}, \mathbf{t}, y] \xrightarrow{\psi_1} k[\mathbf{t}, y] \xrightarrow{\psi_2} k(\mathbf{t}),$$

wobei $k[\mathbf{x}] \to k[\mathbf{x}, \mathbf{t}, y]$ die Einbettungsabbildung ist. Im Ring $k[\mathbf{x}, \mathbf{t}, y]$ betrachten wir das von $B = \{x_1 - f_1(\mathbf{t})\,y,\ x_2 - f_2(\mathbf{t})\,y, \ldots,\ x_n - f_n(\mathbf{t})\,y\}$ erzeugte Ideal. B ist nach dem Hauptsyzygienkriterium eine Gröbnerbasis bzgl. einer Termordnung mit $\mathbf{x} \gg y, \mathbf{t}$ und für $F(x_1, \ldots, x_n) \in k[\mathbf{x}]$ gilt (wie im Fall regulärer Parametrisierungen)

$$F_0 := \psi_1(F) = F(f_1 y, \ldots, f_n y) = \mathrm{NF}(F(x_1, \ldots, x_n), B)$$

d. h. $F \equiv F_0 \pmod{I(B)}$ in $k[\mathbf{x}, \mathbf{t}, y]$. Da $\phi^*(F) = \psi_2(F_0)$ und $F_0 \in k[\mathbf{t}, y]$, gilt weiter

$$F \in Ker\,(\phi^*) \quad \Longleftrightarrow \quad F_0 \in Ker\,(\psi_2).$$

Berechnen wir deshalb zuerst $Ker\,(\psi_2)$. Offensichtlich gilt $I(g\,y - 1) \subset Ker\,(\psi_2)$. Sei umgekehrt $p(\mathbf{t}, y) = \sum_{i=0}^{n} p_i(\mathbf{t}) y^i \in Ker\,(\psi_2)$. Dann ist $\sum_{i=0}^{n} \frac{p_i}{g^i} = 0$ und damit auch

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

in $k[\mathbf{t}, y]$. Wegen

$$(g\,y)^n = ((g\,y-1)+1)^n \equiv 1 \pmod{(g\,y-1)}$$

gilt schließlich auch

$$p(\mathbf{t}, y) \equiv (g\,y)^n p(\mathbf{t}, y) \equiv 0 \pmod{(g\,y-1)}$$

und somit

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

Also gilt

$$F \in Ker\,(\phi^*) \quad \Longleftrightarrow \quad \mathrm{NF}(F_0, (g\,y-1)) = 0.$$

Wir haben damit folgenden Satz bewiesen:

Satz 54 (Implizite Darstellung rational parametrisierter Varietäten) *Sei*

$$V = \left\{ \left(\frac{f_1(a)}{g(a)}, \ldots, \frac{f_n(a)}{g(a)} \right) \mid a \in \mathbb{A}^d \setminus V(g) \right\}$$

eine rational parametrisierte Varietät mit $\gcd(f_1, \ldots, f_n, g) = 1$. *Dann gilt*

$$I(V) = I(x_1 - f_1(\boldsymbol{t})\,y, \ldots, x_n - f_n(\boldsymbol{t})\,y, g(\boldsymbol{t})\,y - 1) \cap k[\boldsymbol{x}],$$

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

Aufgabe: Zeigen Sie, dass

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

gilt. Letzteres Ideal spielte bei der Berechnung des stabilen Idealquotienten von

$$I_2 = I(g\,x_1 - f_1,\ \ldots,\ g\,x_n - f_n)$$

nach g eine Rolle. 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 $\{g^i,\ i \in \mathbb{N}\}$ 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 $S := \{g^i,\ i \in \mathbb{N}\}$ schreiben wir auch kurz R_g. Für $R = k[\mathbf{t}]$ besteht dieser Ring aus genau den auf $\mathbb{A}^d \setminus V(g)$ regulären Funktionen.

$I : g^\infty = I \cdot R_g \cap R$ heißt deshalb auch *Saturierung* von I bzgl. g.

Beispiel: $C = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2\,t}{1+t^2} \right) : t \in \mathbb{R} \right\}$

```
Use R::=QQ[w,t,x,y];
B:=[(1+t^2)*x-(1-t^2),(1+t^2)*y-2*t];
Elim(t,Ideal(B));
```

$$I(x^2 + y^2 - 1)$$

Hier muss man das Element $tw - 1$ nicht dazugeben.

Beispiel: $F = \left\{ \left(\frac{u^2}{v}, \frac{v^2}{u}, u \right) : u, v \in \mathbb{C} \right\}$

In diesem Beispiel führt das Ideal $I(x\,v - u^2, y\,u - v^2, z - u)$ nicht zum richtigen Ergebnis. Es muss wirklich von $I(x\,v - u^2, y\,u - v^2, z - u, t\,u\,v - 1)$ ausgegangen werden.

```
Use R::=QQ[t,u,v,x,y,z],Lex;
I:=Ideal(x*v-u^2,y*u-v^2,z-u);
ReducedGBasis(I);
```

$$I\left(x^2\,y\,z - z^4, v\,z^2 - x\,y\,z, v\,x - z^2, v^2 - y\,z, u - z\right)$$

```
Elim(t..v,I);
```

$$I(x^2\,y\,z - z^4)$$

```
I:=Ideal(x*v-u^2,y*u-v^2,z-u,t*u*v-1);
ReducedGBasis(I);
```

$$I\left(x^2\,y - z^3, v\,z - x\,y, v\,x - z^2, v^2 - y\,z, u - z, t\,z^3 - x, t\,y\,z^2 - v, t\,x\,y - 1\right)$$

```
Elim(t..v,I);
```

$$I(x^2\,y - z^3)$$

Auch rational parametrisierte Varietäten sind irreduzibel.

Satz 55 *Sei k ein unendlicher Körper. Eine Varietät V, die durch eine rationale Parametrisierung*

$$x_i = \frac{f_i(t_1, \ldots, t_d)}{g(t_1, \ldots, t_d)}, i = 1, \ldots n$$

gegeben ist, ist irreduzibel.

Beweis: $\phi : \mathbb{A}^d \setminus V(g) \to \mathbb{A}^n$. $\phi^* : k[x_1, \ldots, x_n] \to k[t_1, \ldots, t_d]_g$, wobei R_g die Lokalisierung nach der multiplikativen Menge der Potenzen von g ist.

$$R_g = \left\{ \frac{f}{g^n} : f \in R, n \in \mathbb{N} \right\}$$

$f \in ker(\phi^*)$, genau wenn $f \circ \phi = 0$. Ist nun $\phi^*(fg) = 0$, so gilt $fg \circ \phi = (f \circ \phi)(g \circ \phi) = 0$. $f \circ \phi = 0$ heißt aber, dass dieses Polynom als Polynom in $t_1, \ldots, t_d$ verschwindet. Aus $(f \circ \phi)(g \circ \phi) = 0$ folgt also $(f \circ \phi) = 0$ oder $(g \circ \phi) = 0$. $I(V)$ ist damit ein Primideal. □

7.4 Zerlegung in irreduzible Komponenten

Jede affine Varietät lässt sich als endliche Vereinigung irreduzibler Varietäten darstellen genau dann, wenn sich jedes Radikalideal im Ring R als endlicher Durchschnitt von Primidealen darstellen lässt. Die letztere Aussage ergibt sich als Folgerung unmittelbar aus dem Hilbertschen Basissatz.

Beispiel: $V = V(x\,z - y^2, x^3 - y\,z)$. Ist bzgl. $y > x$ bereits eine deglex. Gröbnerbasis. Lexikographische Ordnung bringt Elemente zum Vorschein, die Faktor y enthalten.

```
Use R::=QQ[x,y,z],Lex;
I:=Ideal(x*z-y^2,x^3-y*z);
ReducedGBasis(I);
```

$$\left[y^6 - y\,z^4, x\,z - y^2, x\,y^4 - y\,z^3, x^2\,y^2 - y\,z^2, x^3 - y\,z\right]$$

Wir berechnen also $I : (y) = I(x\,z - y^2, x^3 - y\,z, x^2\,y - z^2)$ als größeres Ideal, also $V(I : (y)) \subset V$.

```
Intersection(I,Ideal(y));
Colon(I,Ideal(y));
```

Analog kann man $I : (x)$ berechnen und erhält

$$I : (x) = I : (y) = I : I(x, y) = I + I(x^2y - z^2).$$

$V_1 = V(x\,z - y^2, x^3 - yz\,, x^2y - z^2)$ ist die durch (t^3, t^4, t^5) parametrisierte Kurve und damit irreduzibel.

```
I1:=Ideal(x*z-y^2,x^3-y*z,x^2*y-z^2);
I2:=Colon(Ideal(B),Ideal(x^2*y -z^2));
```

Der Quotient schneidet die Komponente V_1 weg. Übrig bleibt $V_2 = V(x, y)$. Man kann zeigen, dass $V = V_1 \cup V_2$ gilt. Berechne dazu

```
Intersection(I1,I2);
```

Satz 56 *Jedes Radikalideal lässt sich als Durchschnitt endlich vieler Primideale darstellen. Damit ist jede affine Varietät zugleich die endliche Vereinigung irreduzibler Varietäten.*

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 wie oben $V(I) = (V(I) \cap V(f)) \cup (V(I) \cap V(g))$ und folglich

$$I = \operatorname{rad}(I + (f)) \bigcap \operatorname{rad}(I + (g)).$$

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. □

Satz 57 *Jede affine Varietät $V \subset \mathbb{A}^n$ hat eine minimale Zerlegung $V = V_1 \cup \cdots \cup V_m$ in irreduzible Komponenten, d.h. $V_i \not\subset V_j$ für alle i, j, und diese Darstellung ist eindeutig bis auf die Reihenfolge.*

Beweis: Die Existenz minimaler Zerlegungen ergibt sich sofort durch Weglassen von Komponenten V_i mit $V_i \subset V_j$. Zum Nachweis der Eindeutigkeit sei $V = V_1' \cup \cdots \cup V_l'$ eine andere minimale Zerlegung. Es gilt

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_l') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_l').$$

Da V_i irreduzibel ist, muss $V_i = V_i \cap V_j'$ und damit $V_i \subset V_j'$ für ein j gelten. Analog argumentiert man, dass $V_j' \subset V_k$ für ein k gelten muss. Dann ist aber $V_i \subset V_k$ und aus der Minimalität folgt $i = k$ und $V_i = V_j'$. Jedes V_i kommt also in der Zerlegung $V_1' \cup \ldots V_l'$ vor. Umgekehrt gilt dasselbe, also sind beide Zerlegungen identisch bis auf die Reihenfolge. □

Satz 58 *Jedes Radikalideal I in $k[x_1, \ldots, x_n]$ kann als endlicher Durchschnitt $I = P_1 \cap \cdots \cap P_r$ von Primidealen geschrieben werden mit $P_i \not\subset P_j$ für $i \neq j$. Eine solche Zerlegung bezeichnet man auch als* Primzerlegung.

Beweis: Das folgt unmittelbar aus dem zuletzt bewiesenen Satz. □

Die kleinsten affinen Varietäten sind Punkte. Ihnen entsprechen die größten Verschwindungsideale.

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

Ein solches Ideal ist in keinem nichttrivialen Ideal enthalten, ist also ein maximales Ideal.

Satz 59 *Sei $I = \cap_i P_i$ die Primzerlegung des Radikalideals I. Die P_i sind genau die echten Primideale in der Menge $\{I : (f), f \in R\}$. Auch daraus folgt die Eindeutigkeit der Primzerlegung.*

Beweis: Für ein Primideal P gilt

$$P : (f) = \begin{cases} P \text{ wenn } f \notin P \\ 1 \text{ wenn } f \in P \end{cases}$$

In der Tat $g \in P : (f)$ genau dann, wenn $fg \in P$. Aber P ist prim, also $f \in P$ oder $g \in P$.

$I : (f) = \cap_i (P_i : f)$ ist also, wenn prim, dann eines der minimalen Primideale. Umgekehrt nimm $f \in (\cap_{i \neq j} P_i) - P_j$, dann kommt als Durchschnitt genau P_j heraus. □

Wir können damit eine weitere geometrische Interpretation des Idealquotienten geben:

Satz 60 *Ist $V = V(J) = \cup V_\alpha$ die Zerlegung von V in irreduzible Komponenten und $P_\alpha = I(V_\alpha)$ die zugehörigen Primideale, so ist*

$$V(J : (f^\infty)) = \bigcup_{\alpha : f \notin P_\alpha} V_\alpha$$

die Vereinigung derjenigen Komponenten, auf denen f nicht vollkommen verschwindet.

Beweis: OBdA können wir J als Radikalideal voraussetzen, so dass $J = \cap_\alpha P_\alpha$ gilt und damit

$$J : (f^\infty)) = \bigcap_\alpha P_\alpha : (f^\infty)) = \bigcap_{\alpha: f \notin P_\alpha} P_\alpha$$

wegen Satz 48. □

Beispiel: $I = I(x\,z - y^2, z^3 - x^5)$. Berechne lex. GBasis. Die enthält Polynome, die in Faktoren zerfallen. Damit ist $V(I)$ nicht irreduzibel. Berechne Teile durch Quotientenbildung.

```
Use R::=QQ[t,x,y,z],Lex;
I:=Ideal(x*z-y^2,z^3-x^5);
ReducedGBasis(I); // enthält x^4*y^2-z^4
I1:=Colon(I,Ideal(x^2*y-z^2));
I2:=Colon(I,Ideal(x^2*y+z^2));
```

Beweise, dass I_1 und I_2 die Verschwindungsideale der Kurven $C_1 = \left\{(t^3, t^4, t^5)\right\}$ und $C_1 = \left\{(t^3, -t^4, t^5)\right\}$ sind. Damit sind die Ideale Primideale. Beweise, dass der Durchschnitt genau I ist.

7.5 Die Primärzerlegung eines Ideals

Für Polynome und damit für Hauptideale kann jedes Polynom als Produkt von Potenzen irreduzibler Polynome dargestellt werden. So einfach geht das bei Idealen nicht mehr.

Beispiel: $I = I(x, y^2)$ ist keine Potenz eines Ideals.

Definition 16 *Ein Ideal $I \subset k[x_1, \ldots, x_n]$ heißt* Primärideal, *wenn aus $fg \in I$ entweder $f \in I$ oder $\exists m : g^m \in I$ gilt.*

Primideale und das oben betrachtete Ideal $I(x, y^2)$ sind Primärideale.

Lemma 5 *Ist I ein Primärideal, so ist $rad(I)$ ein Primideal und das kleinste Primideal, das I umfasst.*

Beweis: $f\,g \in rad(I) \Rightarrow f^m g^m \in I$. Dann ist aber $f^m \in I$ und damit f in $rad(I)$ oder $g^{ms} \in I$ und damit g in $rad(I)$. □

Definition 17 *Ein Primärideal I mit $P = rad(I)$ heißt auch P-primär.*

Satz 61 *Jedes Ideal kann als endlicher Durchschnitt von Primäridealen geschrieben werden.*

Der Beweis ergibt sich aus den folgenden Überlegungen.

Definition 18 *I heißt* irreduzibel, *wenn aus $I = I_1 \cap I_2$ folgt $I = I_1$ oder $I = I_2$.*

Jedes Ideal kann als endlicher Durchschnitt irreduzibler Ideale dargestellt werden. Das folgt aus der Kettenbedingung für Noethersche Ringe.

Satz 62 *Jedes irreduzible Ideal ist primär.*

Beweis: Sei I irreduzibel, $f\,g \in I$ und $f \notin I$. Betrachte die Ideale $I : (g^n)$. Es gilt

$$I : (g) \subset I : (g^2) \subset I : (g^3) \subset \dots$$

Es existiert N mit $I : (g^N) = I : (g^{N+1})$. Dann gilt

$$(I + (g^N)) \cap (I + (f)) = I.$$

In der Tat, für ein Element aus dem Durchschnitt gilt

$$a\,g^N \equiv b\,f \pmod{I} \Rightarrow a\,g^{N+1} \equiv b\,f\,g \equiv 0 \pmod{I}.$$

Also ist $a \in I : g^{N+1} = I : g^N$ und damit $a\,g^N \in I$.
Da I irreduzibel ist, folgt $I + (g^N) = I$ und damit $g^N \in I$. $\square$

Lemma 6 *Sind I und J primär mit $P = rad(I) = rad(J)$, so ist $I \cap J$ primär.*

Beweis: $f g \in I \cap J$. Ist $f \notin P$, so folgt $g^m \in I$ und $g^s \in J$ und damit $g^{m+s} \in I \cap J$. Sind $f, g \in P$ und $f \notin I \cap J$, so sind genügend hohe Potenzen von g in $I \cap J$. $\square$

Definition 19 *Eine Zerlegung $I = \cap Q_i$ eines Ideals I als Durchschnitt von Primäridealen heißt* Primärzerlegung. *Die Zerlegung heißt* minimal, *wenn alle $rad(Q_i)$ verschieden sind und $Q_i \not\supset \cap_{i \neq j} Q_j$ gilt.*

Satz 63 *Jedes Ideal $I \subset k[x_1, \dots, x_n]$ hat eine minimale Primärzerlegung.*

Beweis: Nach Lemma kann man alle Primärideale mit demselben Radikal zusammenfassen. Weiter kann man die überflüssigen Ideale, die den Durchschnitt der anderen umfassen, weglassen. $\square$

Im Gegensatz zum Fall der Ideale sind Primärzerlegungen nicht eindeutig.

Beispiel:

$$(x^2, xy) = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, y)$$

Aber die zugehörigen Primideale sind eindeutig.

Auch muss nicht jede Potenz eines Primideals primär sein.

Beispiel: $R = k[x, y, z]/(x\,y - z^2)$, $P = (x, z)$, $I = P^2 = (x^2, x\,z, z^2)$. Es ist $x\,y = z^2 \in I$, aber $x \notin I$ und alle $y^n \notin I$. Also ist I nicht primär. Aber es ist $x^2 \in I$.

In $R = k[x, y, z]$ sieht das für die Urbilder dieser Ideale so aus: $P = (x, z)$ nicht maximal, $I = (x^2, x\,z, z^2, x\,y)$;

Primärzerlegung ist $(x) \cap (x^2, x\,z, y)$

```
Use R::=QQ[x,y,z],DegLex;
I:=Ideal(x^2,x*z,z^2,x*y);
Intersection(Ideal(x,z^2),Ideal(x^2,x*z,y,z^2));
```

Satz 64 *Ist P ein maximales Ideal, so ist $Q \subset P$ genau dann P-primär, wenn es ein n gibt mit $P^n \subset Q \subset P$.*

Beweis: Betrachte den Ring $A = R/Q$. Wegen $rad(Q) = P$ ist P in beiden Beweisrichtungen das einzige maximale Ideal. Ist $fg = 0$ und $f \notin P$, dann ist f eine Einheit in A und damit $g = 0$. Ist $f \in P$, so existiert n mit $f^n = 0$, da $rad(Q) = P$. Für eine Basis $f_1, \ldots, f_s$ von P gilt ebenfalls: Es gibt N, so dass $f_1^N, \ldots, f_s^N \in Q$ und damit die letzte Behauptung. □

Lemma 7 *Ist I primär, $P = rad(I)$ und $f \in R$, dann gilt*

$$I : f \quad \begin{cases} = (1) \text{ wenn } f \in I \\ \text{ist } P\text{-primär, wenn } f \notin I \\ = I \text{wenn } f \notin P \end{cases}$$

Beweis: Fall $f \in I$ ist klar. $gh \in I : f$, dann $fgh \in I$, $g \notin I : f$, dann $fg \notin I$, dann $h^m \in I$. Das zeigt, dass $I : f$ primär ist. $g \in I : f$, dann ist $fg \in I$ und $f \notin I$, also $g^n \in I$ und damit $g \in P$. Das zeigt, dass $rad(I : f) = P = rad(I)$ gilt. Für die dritte Aussage ist $I \subset I : (f)$ klar. Sei $q \in I : (f)$, $q \notin I$. Dann ist $fq \in I$ und es existiert n, so dass $f^k \in Q$. Dann wäre aber $f \in P$. □

Satz 65 *Ist $I = \cap Q_i$ eine minimale Primärzerlegung und $P_i = rad(Q_i)$. Dann sind die P_i genau die echten Primideale in der Menge $\{rad(I : f) : f \in R\}$ und damit eindeutig bestimmt.*