Skript zum Kurs
Mechanisiertes Theorembeweisen in der Geometrie
Wintersemester 1996/97

Hans-Gert Gräbe, Univ. Leipzig

4. Februar 1997

1 Einige Sätze aus der ebenen Geometrie

1.1 Die Sätze über die Ecktransversalen im Dreieck

1. Satz und Beweis über den Schnittpunkt der Winkelhalbierenden

2. Satz und Beweis über den Schnittpunkt der Mittelsenkrechten

3. Satz und Beweis über den Schnittpunkt der Seitenhalbierenden

4. Satz vom Höhenschnittpunkt und Beweis

5. Der Satz des Menelaos:
Schneidet eine Transversale eines Dreiecks $\Delta\, ABC$, die nicht durch einen Eckpunkt geht, die Dreiecksseiten oder deren Verlängerungen in den Punkten D, E und F, so gilt für die (vorzeichenbehafteten) Längen der einzelnen Teilstrecken

$$\frac{l(BD)}{l(DC)} \cdot \frac{l(CE)}{l(EA)} \cdot \frac{l(AF)}{l(FB)} = -1.$$

Liegen umgekehrt die Punkte D, E und F auf den entsprechenden Dreiecksseiten und ist das Produkt der genannten Teilverhältnisse gleich -1, so sind D, E und F kollinear.

6. Der Satz des Ceva:
Drei Ecktransversalen des Dreiecks $\Delta\, ABC$ mögen die gegenüberliegenden Seiten in den Punkten D, E, F schneiden. Diese drei Ecktransversalen gehen genau dann durch einen Punkt, wenn

$$\frac{l(BD)}{l(DC)} \cdot \frac{l(CE)}{l(EA)} \cdot \frac{l(AF)}{l(FB)} \cdot = 1$$

gilt.

Folgerung: Neue Beweise der Sätze vom Schnittpunkt der Winkelhalbierenden und vom Höhenschnittpunkt.

Aufgaben:

1. Zeigen Sie, daß die Transversalen zu den Berührungspunkten des Inkreises sich in einem Punkt schneiden.

2. Zeigen Sie, daß sich die Transversalen zu den drei Berührungspunkten der Ankreise in einem Punkt schneiden.

1.2 Weitere Sätze am Dreieck

Die Eulersche Gerade:
In einem Dreieck liegen der Höhenschnittpunkt H, der Schwerpunkt S und der Umkreismittelpunkt M auf einer Geraden. S teilt HM im Verhältnis 2:1.

Im Beweis werden Dreiecke in Ähnlichkeitslage verwendet. Dazu braucht man den

Satz von Desargue:
1. Sind $\Delta\, ABC$ und $\Delta\, A'B'C'$ in Ähnlichkeitslage, d.h. $AB \| A'B', AC \| A'C'$ und $BC \| B'C'$, so sind AA', BB' und CC' konkurrent oder parallel.
2. Sind umgekehrt AA', BB' und CC' konkurrent oder parallel und $AB \| A'B', AC \| A'C'$, so gilt auch $BC \| B'C'$.

Der Satz vom Feuerbachschen Kreis:
Der Mittelpunkt N von HM ist der Mittelpunkt eines Kreises, auf dem neun ausgezeichnete Punkte des Dreiecks $\Delta\, ABC$ liegen, und zwar

- die drei Seitenmitten,
- die drei Höhenfußpunkte und
- die drei Mitten der oberen Höhenabschnitte

Dieser Kreis hat eine weitere, mit elementargeometrischen Mitteln nur schwer zu beweisende ([5, S. ??] ist nicht schlüssig[1]) Eigenschaft: Er berührt den Inkreis des Dreiecks $\Delta\, ABC$.

Hilfssatz: Der Satz vom Höhenfußpunktdreieck

Aufgabe: Beweisen Sie den Satz vom Höhenfußpunktdreieck.

1.3 Sätze am Dreieck aus der neueren Forschung

Der Miquelsche Punkt:
Nimmt man auf jeder Seite eines Dreiecks $\Delta\, ABC$ einen Punkt beliebig an und zeichnet durch jede Ecke und die beiden Punkte, die auf den zu dieser Ecke inzidenten Seiten liegen, Kreise, so gehen diese durch einen gemeinsamen Punkt.

Umgekehrt kann man zu jedem Punkt P im Inneren des Dreiecks $\Delta\, ABC$ Punkte A_1, B_1, C_1 so auf den Dreiecksseiten finden, daß P der zugehörige Miquelsche Punkt ist.

Aufgabe: Es gibt mehrere Tripel (A_1, B_1, C_1), die denselben Miquelschen Punkt liefern. Zeigen Sie, daß all diese Fußpunktdreiecke $\Delta\, A_1B_1C_1$ zueinander ähnlich sind.

Nach dem Thalessatz bekommt man bei vorgegebenem P ein spezielles Tripel (A_1, B_1, C_1) aus den Lotfußpunkten von P auf die Dreiecksseiten. Zeigen Sie, daß für den Flächeninhalt dieses Dreiecks gilt (r = Umkreisradius des $\Delta\, ABC$)

$$F(A_1B_1C_1) = \frac{r^2 - MP^2}{4r^2} F(ABC)$$

Die Simsonsche Gerade:
Fällt man von einem Punkt P außerhalb eines Dreiecks $\Delta\, ABC$ die Lote auf die Dreiecksseiten oder deren verlängerungen, so liegen die drei Fußpunkte der Lote genau dann auf einer Geraden, wenn P auf dem Umkreis des Dreiecks $\Delta\, ABC$ liegt.

Aufgabe: Finden Sie den Zusammenhang zwischen der Simsonschen Geraden und dem Miquelschen Punkt.

1.4 Sätze der projektiven Geometrie

Theorem von Pappus:
Sind A, C, E und B, D, F jeweils kollineare Punkte, so sind auch die Schnittpunkte $AB \cap DE, BC \cap EF$ und $CD \cap AF$ kollinear.

Beweis für den Fall der Parallelität: $AB \| DE, BC \| EF \Rightarrow CD \| AF$

Begriff der projektiven Transformation und Zurückführung des allgemeinen Beweises auf den obigen durch eine geeignete projektive Transformation.

[1] Ein Beweis unter Verwendung von Inversionen am Kreis ist in [4] enthalten.

Der Satz von Pascal:
sind A, B, C, D, E, F sechs Punkte der Ebene so gilt: Diese sechs Punkte liegen genau dann auf einer Kurve zweiten Grades, wenn $X = AB \cap DE, Y = BC \cap EF$ und $Z = CD \cap AF$ kollinear sind.

Beweis für einen Spezialfall (Parallele Geraden am Kreis).

Ein Sechseck $ABCDEF$ heißt *Pascalsches Sechseck*, wenn $X = AB \cap DE, Y = BC \cap EF$ und $Z = CD \cap AF$ kollinear sind.

Nach dem Satz von Pascal ist auch jede Permutation eines Pascalschen Sechsecks wieder ein solches. Das liefert Aussagen der ebenen Geometrie, zu deren Formulierung keine Kurven zweiter Ordnung benötigt werden. Solche Sätze heißen in [9] *Sätze vom Pascal-Typ*. Ein solcher wäre z.B. die folgende Aussage:

Sind $R = AB \cap DE, S = BC \cap EF, T = CD \cap AF$ kollinear, so sind auch $X = AD \cap CF, Y = BD \cap CE, Z = BF \cap AE$ kollinear.

2 Vektorgeometrische Methoden in der affinen Geometrie

2.1 Teilverhältnisse und baryzentrische Koordinaten

Allgemeine Darstellung eines Punktes auf einer Geraden: $X = a * A + (1 - a) * B$

Aus den (vorzeichenbehafteten) Längen der Strecken kann man den Parameter gewinnen zu $a = \frac{l(XB)}{l(AB)}$.

Allgemeine Darstellung eines Punktes der Ebene:

$$X = a * A + b * B + c * C \quad \text{mit} \quad a + b + c = 1$$

Aufgabe: Zeigen Sie, daß die Parameter a, b, c mit Flächeninhalten von Teildreiecken wie folgt zusammenhängen:

$$a = \frac{F(BCX)}{F(ABC)}, b = \frac{F(ACX)}{F(ABC)}, c = \frac{F(ABX)}{F(ABC)}.$$

2.2 Verschiedene Sätze in vektorgeometrischer Formulierung

1. Satz vom Schnittpunkt der Seitenhalbierenden

2. Satz vom Diagonalenschnittpunkt im Parallelogramm

Aufgabe: Beweisen Sie den Satz über iterierte Punktspiegelungen:
Bezeichnet σ_O die Punktspiegelung mit Zentrum im Punkt O, so gilt für drei Punkte O_1, O_2, O_3

$$(\sigma_{O_3} \circ \sigma_{O_2} \circ \sigma_{O_1})^2 = id$$

3. Der Satz von Ceva:
Gegeben $\Delta\, ABC$, Punkte D, E, F auf den Dreiecksseiten, so daß AD, BE, CF sich in einem gemeinsamen Punkt P schneiden.

Vektorgeometrische Formulierung der Voraussetzungen: $\exists\ a, b, c, d, e, f$ mit

$$\begin{gathered} aB + (1-a)C = D \\ bC + (1-b)A = E \\ cA + (1-c)B = F \\ (1-d)A + dD = P \\ (1-e)B + eE = P \\ (1-f)C + fF = P \end{gathered}$$

Behauptung: $abc - (1 - a)(1 - b)(1 - c) = 0$.

Lösungsidee: Eliminiere in obigen vier Beziehungen P, D, E, F. Die verbleibende Gleichung ist eine lineare Abhängigkeitsrelation zwischen den linear unabhängigen Ortsvektoren A, B, C, d.h. die symbolischen Ausdrücke, die polynomial in den Skalaren a, b, c sind, müssen verschwinden. Man erhält die Gleichungen

$$\begin{array}{rcccl} 1-d & = (1-b)e = & & cf & \\ ad & = & 1-e & = (1-c)f & \\ (1-a)d = & & be & = & 1-f, \end{array}$$

aus denen man d, e, f eliminiert. Es verbleibt eine Gleichung in a, b, c, die Behauptung.

Alternativ kann man die Gröbnerbasis des zugehörigen Polynome berechnen.

$$\{b\,e+f-1\,,\,d+e+f-2\,,\,c\,f-e-f+1\,,\,a\,e+a\,f-2\,a-e+1\,,$$
$$a\,b\,f-2\,a\,b-a\,f+a+b+f-1\,,\,2\,a\,b\,c-a\,b-a\,c+a-b\,c+b+c-1\}$$

Die letzte Gleichung entspricht gerade der Behauptung.

4. Vektorgeometrische Formulierung des Satzes von Desargue:

$$\begin{array}{c} AB \| A'B' \;\Rightarrow\; B'-A' = a(B-A) \\ BC \| B'C' \;\Rightarrow\; C'-B' = b(C-B) \\ CA \| C'A' \;\Rightarrow\; A'-C' = c(A-C) \end{array}$$

Daraus bekommt man die Beziehung zwischen den linear unabhängigen Ortsverktoren A, B, C

$$(a-b)B + (c-a)A + (b-c)C = 0,$$

also $a = b = c$ als Beziehung zwischen den bis dato unbekannten Skalaren. Damit folgt $A' - aA = B' - bB = C' - cC$ und man kann D so wählen, daß (für $a \neq 1$, sonst sind die drei Geraden parallel) der Vektor gleich $(1-a)D$ ist.

2.3 Modultermordnungen und Gröbnerbasen für Moduln

Allgemeine Formulierung der Aufgabenstellung:

Gegeben sind

- Skalare $a_1, \ldots, a_n$, die Teilverhältnisse, Lage von Punkten etc. beschreiben,
- Ortsvektoren $v_1, \ldots, v_m$,
- Formulierung der geometrischen Bedingungen als (lineare) Vektorgleichungen mit polynomialen Koeffizienten aus $R = k[a_1, \ldots, a_n]$,
- eine Teilmenge $v_1, \ldots, v_k$ linear unabhängiger Vektoren.

Gesucht sind die Beziehungen, die sich aus der linearen Unabhängigkeit von $v_1, \ldots, v_k$ auf die Skalare ergeben.

Algebraische Formulierung:

Die geometrischen Bedingungen erzeugen einen Untermodul des freien Moduls $F = R^m$. Die Vektoren $v_1, \ldots, v_k$ spannen ihrerseits einen Untermodul $F' = R^k \subset F$ auf. Gesucht sind alle geometrischen Bedingungen in $M \cap F'$.

Bei fixierter Basis $(e_1, \ldots, e_m)$ von F kann man jedes Element aus F in der Form $v = \sum f_i e_i$ mit $f_i \in R$ bzw. als Zeilenvektor

$$[\; f_1 \quad f_2 \quad \ldots \quad f_m \;]$$

darstellen. Einer Matrix mit Einträgen aus R entspricht dann der von ihren Zeilenvektoren erzeugte Untermodul von F.

Eine weitere Darstellungsart ist $v = \sum c_\alpha m_\alpha e_{i_\alpha}$ mit Koeffizienten $c_\alpha \in k$ und Termen $m_\alpha \in T(R)$. $v_\alpha = m_\alpha e_{i_\alpha}$ nennt man dabei einen *Modulterm* mit dem monomialen Bestandteil m_α und der Komponente i_α. Für diese Modulterme kann man das Konzept der Termordnung von $T(R)$ auf sogenannte *Modultermordnungen* ausdehnen.

Def.: Eine lineare Ordnung auf den Modultermen $T(F)$ heißt *Modultermordnung* wenn sie folgende zwei Eigenschaften erfüllt:

$$\begin{array}{cc} \forall m \in T(R) & v_\alpha < v_\beta \Rightarrow m \cdot v_\alpha < m \cdot v_\beta \\ \forall i & m_\alpha < m_\beta \Rightarrow m_\alpha e_i < m_\beta e_i \end{array}$$

Beispiele für solche Modultermordnungen sind
die MK-Ordnung (es werden erst Monome, dann Komponenten verglichen)

$$m_\alpha e_{i_\alpha} < m_\beta e_{i_\beta} \quad :\Leftrightarrow \quad \begin{array}{c} m_\alpha < m_\beta \\ \text{oder} \\ m_\alpha = m_\beta \text{ und } i_\alpha < i_\beta \end{array}$$

und die KM-Ordnung (es werden erst Komponenten, dann Monome verglichen)

$$m_\alpha e_{i_\alpha} < m_\beta e_{i_\beta} \quad :\Leftrightarrow \quad \begin{array}{c} i_\alpha < i_\beta \\ \text{oder} \\ i_\alpha = i_\beta \text{ und } m_\alpha < m_\beta \end{array}$$

Analog den Definitionen für Polynome führt man nun die Begriffe *Leitterm* $lt(v) = c_\alpha m_\alpha e_{i_\alpha}$, *Leitkoeffizient* $lc(v) = c_\alpha$, *Leitmonom* $lm(v) = m_\alpha$ sowie (neu) den Begriff der *Leitkomponente* $lk(v) = i_\alpha$ für Elemente $v = c_\alpha m_\alpha e_{i_\alpha} + \ldots \in F$ ein.

Beispiel: Dreieckstrisektion
Im Dreieck $\Delta\,ABC$ sei M die Mitte von AB, S die Mitte von CM und N der Schnittpunkt von AS und BC. Dann teilt N die Strecke BC im Verhältnis 2:1.

Die vektorgeometrischen Bedingungen

$$\begin{array}{c} M = \frac{1}{2}(A+B), \\ S = \frac{1}{2}(C+M), \\ N = aA + (1-a)S = bB + (1-b)C \end{array}$$

lassen sich als Zeilen der Matrix

$$M := \begin{pmatrix} 1 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 1 & 1 & -2 & 0 \\ a & 0 & 0 & 0 & -a+1 & -1 \\ 0 & b & -b+1 & 0 & 0 & -1 \end{pmatrix}$$

schreiben.

Das entsprechende Eliminationsproblem läßt sich hier direkt mit dem Gaußalgorithmus lösen. Dieser verwendet als Modultermordnung die KM-Fortsetzung einer (beliebigen) Termordnung auf R.

Mit dem REDUCE-Paket CALI erhält man:

```
> vars:={a,b}$ setring(vars,{},lex)$ M1:=interreduce(M);
```

$$M_1 = \begin{pmatrix} -1 & -1 & 0 & 2 & 0 & 0 \\ -1 & -1 & -2 & 0 & 4 & 0 \\ 0 & -b & b-1 & 0 & 0 & 1 \\ -3\,a-1 & a+4\,b-1 & 2\,a-2\,b+1 & 0 & 0 & 0 \end{pmatrix}$$

Extrahieren wir nun alle Zeilen der Matrix M_1, deren Leitkomponente höchstens 3 ist:

```
> M2:=matpart(M1,3);
```

$$\begin{pmatrix} -3\,a-1 & a+4\,b-1 & 2\,a-2\,b+1 & 0 & 0 & 0 \end{pmatrix}$$

Schließlich extrahieren wir alle Einträge und finden die Parameter, die gemeinsame Nullstellen dieser Polynome sind.

> `solve(interreduce mat2list M2,vars);`

$$\{\{a = \frac{-1}{3}, b = \frac{1}{3}\}\}$$

Dieses Vorgehen kann man wie folgt verallgemeinern:

Satz: Enthält M bzgl. einer KM-Ordnung für jedes $i > k$ eine Gleichung v mit $lt(v) = e_i$, so kann man $M \cap R^k$ durch einfache Gauss-Reduktion bestimmen.

Beispiel: Der Satz von Ceva

$$M = \begin{pmatrix} 0 & a & -a+1 & -1 & 0 & 0 & 0 \\ -b+1 & 0 & b & 0 & -1 & 0 & 0 \\ c & -c+1 & 0 & 0 & 0 & -1 & 0 \\ -d+1 & 0 & 0 & d & 0 & 0 & -1 \\ 0 & -e+1 & 0 & 0 & e & 0 & -1 \\ 0 & 0 & -f+1 & 0 & 0 & f & -1 \end{pmatrix}$$

> `vars:={a,b,c,d,e,f}$ setring(vars,{},lex)$ M1:=interreduce(M);`

$$M_1 = \begin{pmatrix} 0 & -a & a-1 & 1 & 0 & 0 & 0 \\ b-1 & 0 & -b & 0 & 1 & 0 & 0 \\ -c & c-1 & 0 & 0 & 0 & 1 & 0 \\ -c\,f & f\,(c-1) & f-1 & 0 & 0 & 0 & 1 \\ -b\,e-c\,f+e & c\,f-e-f+1 & b\,e+f-1 & 0 & 0 & 0 & 0 \\ c\,f+d-1 & -a\,d-c\,f+f & a\,d-d-f+1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

> `M2:=matpart(M1,3);`

$$M_2 = \begin{pmatrix} -b\,e-c\,f+e & c\,f-e-f+1 & b\,e+f-1 & 0 & 0 & 0 & 0 \\ c\,f+d-1 & -a\,d-c\,f+f & a\,d-d-f+1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Auch hier bekommt man die Beziehungen zwischen den skalaren Parametern heraus, indem man alle Koeffizienten in den linearen Abhängigkeitsrelationen zwischen den unabhängigen Basisvektoren $A = e_1, B = e_2, C = e_3$ aufsammelt:

> `interreduce mat2list M2;`

$$\{b \cdot e + f - 1, d + e + f - 2, c \cdot f - e - f + 1, a \cdot e + a \cdot f - 2 \cdot a - e + 1\}$$

Als Ergebnis bekommen wir dasselbe Relationenideal zwischen den skalaren Parametern wie schon oben.

Im allgemeinen muß man wie für Ideale eine kompliziertere algebraische Theorie verwenden. Ähnlich dem Fall des Ringes R kann man die Begriffe *Normalform* und *Gröbnerbasis* auch für Moduln einführen.

Beispiel: $M \subset F = R^4$ werde erzeugt von den vier Zeilen der Matrix

$$\begin{pmatrix} y & w & 0 & -x^2 \\ z & x & 0 & -w\,y \\ 0 & -y & w & -x\,z \\ 0 & -z & x & -y^2 \end{pmatrix}$$

Nach Ausführung aller möglichen Paarreduktionen erhalten wir als Gröbnerbasis die Vektoren

$$\begin{pmatrix} -w\,y^2 + x^2\,z & -w^2\,y + x^3 & 0 & 0 \\ -y^3 & -w\,y^2 + x^2\,z & x^3 & 0 \\ -x\,z^2 & -w\,y^2 + x^2\,z & w^2\,y & 0 \\ 0 & x\,z^2 - y^3 & w\,y^2 - x^2\,z & 0 \\ -y\,z & -w\,z + x\,y & w\,x & 0 \\ -y & -w & 0 & x^2 \\ -z & -x & 0 & w\,y \\ 0 & y & -w & x\,z \\ 0 & z & -x & y^2 \end{pmatrix}$$

Satz: Sei $M \subset F = R^m$ gegeben und $F' = R^k$ der von den ersten k Basisvektoren erzeugte freie Untermodul von F. Weiter sei G die Gröbnerbasis von M bzgl. einer KM-Ordnung. Dann ist $G \cap F'$ die Gröbnerbasis von $M \cap F'$.

Insbesondere ist also in obigem Beispiel für $k = 2$ der entsprechende Eliminationsmodul von dem einzigen Element

$$\begin{pmatrix} -w\,y^2 + x^2\,z & -w^2\,y + x^3 & 0 & 0 \end{pmatrix}$$

erzeugt.

3 Die Koordinatenmethode

3.1 Koordinatengeometrische Interpretation geometrischer Grundkonstruktionen

Das einfachste Verfahren zur Algebraisierung geometrischer Sachverhalte ist die Einführung von Koordinaten und die Verallgemeinerung der aus der (linearen und nichtlinearen) analytischen Geometrie bekannten Ansätze.

Die grundlegenden geometrischen Objekte, die wir zunächst betrachten wollen, sind Punkte und Geraden. In Koordinaten können wir sie als Paare bzw. Tripel (komplexer) Zahlen darstellen:

$P = (p_1, p_2)$ bezeichnet dabei den Punkt P mit den Koordinaten (p_1, p_2), während $g = (g_1, g_2, g_3)$ die Gerade $g_1 x_1 + g_2 x_2 + g_3 = 0$ bezeichnet. Letztere Darstellung nennt man *homogene Koordinaten* der Geraden g.

Drei Punkte liegen auf einer Geraden:

A, B, C kollinear genau dann, wenn $det \begin{pmatrix} a_1 & a_2 & 1 \\ b_1 & b_2 & 1 \\ c_1 & c_2 & 1 \end{pmatrix} = 0$

Drei Geraden gehen durch einen Punkt:

g, h, k konkurrent genau dann, wenn $\begin{vmatrix} g_1 & g_2 & g_3 \\ h_1 & h_2 & h_3 \\ k_1 & k_2 & k_3 \end{vmatrix} = 0$

Gerade durch zwei Punkte:

$$line(A, B) = (b_2 - a_2, a_1 - b_1, a_2 b_1 - a_1 b_2)$$

Parallelität:

$g \| h$ genau dann, wenn $g_1 h_2 - h_1 g_2 = 0$

Schnittpunkt zweier Geraden:

$$point(g, h) = (\frac{d_1}{d}, \frac{d_2}{d}) \quad where \quad d = \begin{vmatrix} g_1 & g_2 \\ h_1 & h_2 \end{vmatrix}, d_1 = \begin{vmatrix} g_2 & g_3 \\ h_2 & h_3 \end{vmatrix}, d_2 = \begin{vmatrix} g_3 & g_1 \\ h_3 & h_1 \end{vmatrix}$$

Weiter: Teilpunkt, Mittelpunkt, Punkt liegt auf einer Geraden
Lot von P auf die Gerade g:

$$lot(P,g) = (g_2, -g_1, g_1p_2 - g_2p_1)$$

Damit kann man schon einige Sätze aus der Dreiecksgeometrie beweisen.

4 Mechanisiertes Beweisen geometrischer Theoreme

4.1 Zur Algorithmisierung geometrischer Konstruktionen. Analytische Geometrie mit dem Computer

Um geometrische Konstruktionen zu algorithmisieren, wollen wir Mittel der analytischen Geometrie der Ebene verwenden. Wir fixieren dazu ein Koordinatensystem (x, y). Die elementaren geometrischen Objekte Punkt und Gerade (die Datentypen Point und Line) lassen sich dann als Paar P:Point=(p_1, p_2) bzw. Tripel g:Line=(g_1, g_2, g_3) komplexer Zahlen darstellen, wobei die Gerade g die Punktmenge $\{(x, y) : g_1x + g_2y + g_3 = 0\}$ symbolisiert. Geometrische Grundkonstruktionen können wir in diesem Kontext als Funktionen auffassen, die aus gegebenen Objekten neue konstruieren.

1) Die Gleichung der Geraden durch zwei Punkte $P = (p_1, p_2), Q = (q_1, q_2)$ erhalten wir aus der Zweipunktegleichung $(x - p_1)(q_2 - p_2) - (y - p_2)(q_1 - p_1) = 0$ als Funktion

`line(P,Q:Point):Line==`$(q_2 - p_2, p_1 - q_1, p_2q_1 - p_1q_2)$

P und Q sind dabei formale Parameter vom Typ Point, der Rückgabewert der Funktion vom Typ Line.

2) Analog können wir den Schnittpunkt zweier Geraden berechnen, indem wir das entsprechende lineare Gleichungssystem lösen. Es handelt sich dabei allerdings nur um eine partielle Funktion, denn wenn die beiden Geraden parallel sind, existiert kein bzw. kein eindeutig bestimmter Schnittpunkt. Die zu definierende Funktion bricht in diesem Fall mit einer Fehlermeldung ab.

```
point(a,b:Line):Point==
      d:=a1 b2 - a2 b1;
      if d = 0 then error ''Lines are parallel''
      else return ((a2 b3 - a3 b2)/d, (a3 b1 - a1 b3)/d)
```

Auch hier sind a und b formale Parameter, diesmal vom Typ Line.

3) Das Lot $l = (l_1, l_2, l_3)$ von einem Punkt P auf eine Gerade a ist ein Datum vom Typ Line. Seine Komponenten ergeben sich aus den Bedingungen, daß der Normalenvektor $(l_1, l_2) = (a_2, -a_1)$ senkrecht auf dem Normalenvektor von a steht und das Absolutglied der Bedingung $l_1p_1 + l_2p_3 + l_3 = 0$ genügt.

`lot(P:Point,a:Line):Line==`$(a_2, -a_1, a_1p_2 - a_2p_1)$

Die Parallele zu einer Geraden a durch einen Punkt P erhält man analog zu

`par(P:Point,a:Line):Line==`$(a_1, a_2, -a_1p_1 - a_2p_2)$

4) Ebenfalls kann man den (euklidschen) Abstand zwischen zwei Punkten P, Q berechnen. Um eine komplizierte Operation wie das Wurzelziehen zu vermeiden, wollen wir allerdings das *Abstandsquadrat* bestimmen.

`sqrdist(P,Q:Point):Complex==`$(p_1 - q_1)^2 + (p_2 - q_2)^2$

5) In verschiedenen geometrischen Konstruktionen kommt oft als ein Teilschritt die Auswahl eines beliebig gelegenen geometrischen Objekts vorgegebenen Typs, etwa die Auswahl eines Punktes oder einer Gerade der Ebene oder eines Punktes auf einer Geraden vor. Einen Generator zufälliger komplexer Zahlen vorausgesetzt ist diese Aufgabe für freie Punkte einfach zu erfüllen. Eine beliebige Gerade läßt sich durch die Auswahl zweier zufälliger Punkte erzeugen. Einen Punkt auf einer Geraden kann man etwa durch Auswahl seiner x-Koordinate fixieren; die y-Koordinate ergibt sich dann aus der Geradengleichung eindeutig. Allerdings darf dabei die Gerade nicht parallel zur y-Achse verlaufen. In diesem Fall kann die y-Koordinate frei gewählt werden. Eine entsprechende Funktion hätte also das folgende Aussehen:

```
choosePoint(a:Line,u:Complex):Point==
      if a2 = 0 then
            if a1 = 0 then error ''a is not a line''
            else return (-a3/a1, u)
      else return (u, -a3/a2)
```

Ist die Gerade a durch zwei Punkte P, Q definiert, so kann man wie im Kapitel "Vektorrechnung" einen solchen Punkt auch einheitlich durch die Funktion

`varPoint(P,Q:Point,u:Complex):Point==` $(u\,a_1 + (1-u)\,b_1, u\,a_2 + (1-u)\,b_2)$

erzeugen. Insbesondere liefert

`midPoint(P,Q:Point):Point==` $(\frac{1}{2}\,(a_1 + b_1), \frac{1}{2}\,(a_2 + b_2))$

den Mittelpunkt der Strecke PQ.

6) Aus diesen Funktionen kann man komplexere geometrische Funktionen zusammensetzen. So findet man etwa den Fußpunkt des Lots vom Punkt P auf die Gerade a als

`pedalPoint(P:Point,a:Line):Point==point(lot(P,a),a),`

die Mittelsenkrechte auf der Seite BC im Dreieck ABC als

`mp(A,B,C:Point):Line==lot(midPoint(B,C),line(B,C)),`

die Höhe entsprechend als

`altitude(A,B,C:Point):Line==lot(A,line(B,C))`

und die Seitenhalbierende als

`median(A,B,C:Point):Line==line(A,midPoint(B,C))`

7) Schließlich kann man testen, ob für gewisse Konfigurationen geometrische Bedingungen erfüllt sind. So kann man etwa testen, ob zwei gegebene Geraden a und b parallel oder orthogonal sind, indem man prüft, ob $a_1b_2 - a_2b_1$ bzw. $a_1b_1 + a_2b_2$ verschwindet, oder ob ein Punkt P auf einer Geraden a liegt. Entsprechende Funktionen haben folgende Spezifikation:

`parallel(a,b:Line):Boolean==`$(a_1b_2 - a_2b_1 = 0)$

bzw.

`orthogonal(a,b:Line):Boolean==`$(a_1b_1 + a_2b_2 = 0)$

`pointOnLine(P:Point,a:Line):Boolean==`$(a_1p_1 + a_2p_2 + a_3 = 0)$

Auch kompliziertere Bedingungen kann man auf diese Weise prüfen, insbesondere ob drei gegebene Punkte P, Q, R auf einer gemeinsamen Geraden liegen, d.h. *kollinear* sind. Dies ist äquivalent zur nichttrivialen Lösbarkeit eines homogenen Gleichungssystems, also zur Bedingung

$$\begin{vmatrix} p_1 & p_2 & 1 \\ q_1 & q_2 & 1 \\ r_1 & r_2 & 1 \end{vmatrix} = 0$$

Eine ähnliche Bedingung erhält man bei der Frage, ob drei gegebene Geraden a, b, c durch einen gemeinsamen Punkt gehen, d.h. *konkurrent* sind. Das entsprechende Gleichungssystem hat drei Gleichungen für die beiden unbekannten Koordinaten des Schnittpunkts, d.h. es muß wiederum

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} = 0$$

gelten. Allerdings ist dies nur eine notwendige und keine hinreichende Bedingung für die Existenz einer Lösung. Eine solche würde, das Verschwinden obiger Determinante vorausgesetzt, genau dann nicht existieren, wenn der Rang der Matrix des Gleichungssystems 1, der der erweiterten Koeffizientenmatrix dagegen 2 wäre. Geometrisch bedeutet dies, daß die drei betrachteten Geraden zueinander parallel wären. Wir nennen deshalb drei Geraden a, b, c, für die obige Determinante verschwindet, *algebraisch konkurrent*. Ähnlich können wir auch zwischen algebraischer und geometrischer Kollinearität unterscheiden, wenn wir die Entartungsfälle, daß zwei oder sogar alle drei Punkte zusammenfallen, in einem geometrischen Kontext ausschließen wollen (dies ist hier allerdings im Gegensatz zur Konkurrenz eine Definitionsfrage auf der Seite der Geometrie). Für den Test der entsprechenden algebraischen Bedingungen kann man damit wiederum Funktionen mit der Signatur `collinear(A,B,C:Point):Boolean` bzw. `concurrent(a,b,c:Line):Boolean` angeben.

Alle diese Funktionen lassen sich in der Tat in fast jeder Programmiersprache implementieren und erlauben es auf diese Weise, konkrete geometrische Konfigurationen "durchzurechnen".

Aufgabe: Entwerfen Sie geeignete Datentypen und geben Sie eine Implementierung der obigen Funktionen in einer klassischen Programmiersprache (Pascal oder C bzw. C++).

Mit diesem Arsenal kann man die Koordinaten auch komplizierterer geometrischer Objekte bestimmen und entsprechende geometrische Sätze in konkreten Konfigurationen überprüfen.

Beispiel 1: Der Satz vom Schnittpunkt der Mittelsenkrechten. Die Funktion

```
test(A,B,C:Point):Boolean==concurrent(mp(A,B,C),mp(B,C,A),mp(C,A,B))
```

prüft, ob für ein Dreieck, das durch seine Eckpunkt(koordinaten) A, B, C gegeben ist, die drei Mittelsenkrechten durch einen gemeinsamen Punkt gehen. Alternativ kann man wie im elementargeometrischen Beweis dieses Satzes auch zuerst die Koordinaten des Schnittpunkt zweier der Mittelsenkrechten bestimmen und dann zeigen, daß dieser Punkt auf der dritten Mittelsenkrechten liegt:

```
test(A,B,C:Point):Boolean==
      M:Point:=point(mp(A,B,C),mp(B,C,A));
      return pointOnLine(M,mp(C,A,B));
```

Letztere Funktion läßt sich dahingehend erweitern, daß man auch zeigen kann, das dieser Schnittpunkt der Mittelpunkt des Umkreises des Dreiecks $\Delta\, ABC$ ist. Dazu ist

$$sqrdist(M, A) = sqrdist(M, B) = sqrdist(M, C)$$

zu testen, d.h. die letzte Zeile durch

```
return (sqrdist(M,A) = sqrdist(M,B)) and (sqrdist(M,B) = sqrdist(M,C))
```

zu ersetzen.

Aufgabe: Finden Sie analoge Programme für den Test des Satzes vom Schnittpunkt der Höhen oder der Seitenhalbierdenden. Lassen Sie auch testen, daß die Produkte aus den Höhenabschnitten im Dreieck gleich sind bzw. der Schnittpunkt der Seitenhalbierenden diese im Verhältnis 2:1 teilt.

Beispiel 2: Der Satz von der Eulerschen Geraden:

```
test(A,B,C:Point):Boolean==
     M:Point:=point(mp(A,B,C),mp(B,C,A));
     H:Point:=point(altitude(A,B,C),altitude(B,C,A));
     S:Point:=point(median(A,B,C),median(B,C,A));
     return collinear(M,H,S);
```

Aufgabe: Modifizieren Sie das Programm so, daß es den Satz vom Feuerbachschen Kreis testet.

======> Weitere Beispiele:

Iterierte Spiegelungen

Dreieckstrisektion

Satz von Desargue

4.2 Symbolische analytische Geometrie

Dieselben Funktionen, die wir im letzten Abschnitt in einer klassischen Programmiersprache betrachtet haben, die es gestattet, Konfigurationen der analytischen Geometrie mit konkreten Koordinaten durchzurechnen, kann man auch in einem System implementieren, das symbolische Formelmanipulationen erlaubt.

Aufgabe: Implementieren Sie obige Palette von Funktionen in einem der gängigen Computeralgebrasysteme Maple, Mathematica, Reduce oder Macsyma.

Ein solches System bietet uns zusätzlich die Möglichkeit, die formalen Parameter in unseren Funktionen durch *Symbole* zu ersetzen. Da alle von uns bisher implementierten Funktionen boolesche Rückgabewerte oder aber Punkte oder Geraden liefern, deren Komponenten rationale Funktionen in den Komponenten der Eingabeparameter sind, erhalten wir in letzterem Fall als Ergebnis unserer Rechnungen (eine Fehlermeldung oder) *rationale* Ausdrücke in diesen Symbolen. Dies gilt ebenso für die Funktionen mit booleschem Rückgabewert, wenn man berücksichtigt, daß dieser sich stets aus einer Kombination von Nulltests rationaler Verknüpfungen von Eingabekomponenten ergibt.

Der Aufruf einer solchen Funktion mit (konkreten) Parametern, die ihrerseits wieder aus Funktionsaufrufen gewonnen werden, bedeutet in diesem Kontext, daß die Variablen eines rationalen Ausdrucks durch andere rationale Ausdrücke zu substituieren sind. Im Ergebnis erhalten wir wieder rationale Ausdrücke, die sich natürlich simplifizieren lassen. Bestimmen wir etwa die Koordinaten des Umkreismittelpunkts des Dreiecks ABC als Schnittpunkt der entsprechenden Mittelsenkrechten m, n, so bedeutet dies auf dem betrachteten symbolischen Niveau, daß beim Aufruf von `point(mp(A,B,C),mp(B,C,A))` in

$$point(m,n) = (\frac{m_2 n_3 - m_3 n_2}{m_1 n_2 - m_2 n_1}, \frac{m_3 n_1 - m_1 n_3}{m_1 n_2 - m_2 n_1})$$

die Komponenten von m, n durch die entsprechenden rationalen Ausdrücke

$$mp(A,B,C) = \{b_1 - c_1, b_2 - c_2, \tfrac{-b_1^2 - b_2^2 + c_1^2 + c_2^2}{2}\}$$

bzw.

$$mp(B,C,A) = \{-a_1 + c_1,\ -a_2 + c_2,\ \tfrac{a_1^2 + a_2^2 - c_1^2 - c_2^2}{2}\}$$

zu ersetzen sind. Diese Ausdrücke sind ihrerseits während des Aufrufs

```
>  mp(A,B,C)=lot(midPoint(B,C),line(B,C))
```

in einem Substitutions- und Simplifikationsprozeß (der Tiefe 2) nach demselben Prinzip entstanden.

Der Simplifikationsprozeß rationaler Funktionen liefert eine einfachere rationale Funktion, die für alle Parameterbelegungen mit komplexen Zahlen, die für die unsimplifizierte Funktion nicht zu einem Fehlerabbruch führen, denselben Wert hat wie diese. Der Definitionsbereich der simplifizierten rationalen Funktion kann allerdings größer sein als der der Ausgangsfunktion.

Läßt sich unsere geometrische Behauptung analytisch insbesondere auf das Verschwinden einer gewissen rationalen Kombination der Koordinaten der beteiligten geometrischen Objekte reduzieren, wie dies in allen oben betrachteten Beispielen der Fall war, so ist diese Bedingung sicher dann für alle zulässigen Parameterspezifikationen erfüllt, wenn die entsprechende rationale Funktion zu Null simplifiziert. Auf diesem Wege erhalten wir bereits allgemeingültige Beweise für eine Reihe der oben betrachteten Geometrie-Theoreme.

Beispiele und Übungsaufgaben aus geo.3 und geo.5, auch mit festgewählten Punkten.

Für geometrische Sachverhalte, die sich analytisch in die beschriebene Form bringen lassen, gibt ess also die folgenden Alternativen:

1) Der Funktionsaufruf bricht mit einer Fehlermeldung ab.

In allen oben beschriebenen Fällen tritt dies allerdings nur auf, wenn ein rationaler (Zwischen-)Ausdruck, der zulässig zu einem Wert verschieden Null spezifizieren muß, als rationale Funktion identisch Null ist.

2) Die durch den Funktionsaufruf zurückgegebene rationale Funktion simplifiziert zu Null.

Dann gilt der geometrische Satz für alle zulässigen Parameterspezifikationen.

3) Die durch den Funktionsaufruf zurückgegebene rationale Funktion simplifiziert nicht zu Null.

Dann gilt der geometrische Satz für fast alle zulässigen Parameterspezifikationen nicht. Der Satz gilt nur unter einer Zusatzbedingung, die analytisch durch das Zählerpolynom des simplifizierten Ausdrucks beschrieben wird.

Bei diesen Überlegungen bleibt der Begriff der *zulässigen Parameterspezifikation* offen. Dies bedeutet, daß die Parameter so zu wählen sind, daß alle konstruktiven Zwischenschritte analytisch ausführbar sind, d.h. in unserem Fall, daß bei konkreten Parameterbelegungen gewisse Nenner rationaler Funktionen nicht verschwinden. Es reicht dabei sicher nicht aus, den Nenner des Endergebnisses zu betrachten, weil eine Reihe von Simplifikationszwischenschritten bei konkreten Parameterspezifikationen auf Ausdrücke der Form $\frac{0}{0}$ führen können, deren Unbestimmtheit sich im weiteren Prozeß der Vereinfachung des entsprechenden rationalen Ausdrucks weghebt. Andererseits ist man daran interessiert, unzulässige Parameterspezifikationen zu erkennen, weil deren Kenntnis erlaubt, die geometrischen Voraussetzungen, unter denen die untersuchte Aussage gültig ist, weiter zu präzisieren.

Diese Bedingungen auf die Zulässigkeit von Parameterspezifikationen müssen im Laufe des Simplifikationsprozesses der rationalen Funktion aufgesammelt werden und haben die Form $f \neq 0$ für eine geeignete *polynomiale* Bedingung f. In der Liste der bisher definierten (elementaren) Funktionen können nur an zwei Stellen solche *Nichtdegenerationsbedingungen* auf die Parameterspezifikation entstehen, nämlich in den Funktionen `point` und `choosePoint`, wo die entsprechenden Nenner nicht verschwinden dürfen. Eine Modifikation der Funktionen erlaubt es, die (Zähler der) entsprechenden Nichtdegenerationsbedingungen in einer global definierten Liste aufzusammeln.

Siehe geo1.r

4.3 Der Mechanisierungssatz für geometrische Sätze vom konstruktiven Typ

Wir wollen nun geometrische Konfigurationen, auf die man das bisher beschriebene Mechanisierungsprinzip anwenden kann, genauer beschreiben. Die wichtigste gemeinsame Eigenschaft, die dabei ausgenutzt worden ist, war die Tatsache, daß sich die betrachtete geometrische Konfiguration mit einfachen Konstruktionsschritten auf einem "leeren Blatt Papier" Schritt für Schritt erzeugen ließ. Neben deterministischen Konstruktionsschritten gab es dabei auch solche, die gewisse Freiheiten bei der Auswahl von Punkten oder Geraden lassen. Um den Beweis allgemeingültig zu führen, sind alle diese Auswahlen zu untersuchen. Formal ist also ein solcher *Konstruktionsschritt* als Abbildung einer Menge geometrischer Konfigurationen in eine andere solche Menge zu betrachten.

In all unseren Beispielen ergaben sich diese geometrischen Konfigurationen alle aus einer einzigen *allgemeinen geometrischen Konfiguration* durch Spezifikation der Parameter, so daß gewisse degenerierte Lagebeziehungen vermieden wurden.

In diesen geomertischen Konfigurationen spielten geometrische Objekte (Punkte und Geraden) eine Rolle, die sich durch Parameterspezifikation aus *allgemeinen geometrischen Objekten* ergeben haben.

Um diese Begriffe genauer zu fassen, sei im folgenden $\{u_1, \ldots, u_n\}$ ein Satz algebraisch unabhängiger Parameter, $R = \mathbf{C}[u_1, \ldots, u_n]$ der Polynomring in $u_1, \ldots, u_n$ und $K = \mathbf{C}(u_1, \ldots, u_n)$ dessen Quotientenkörper. Weiterhin betrachten wir *Spezifikationen* $\phi : u_i \mapsto c_i$, die den Parametern komplexe Zahlen $c_i \in \mathbf{C}$ zuordnen. Eine solche Spezifikation definiert einen Ringhomomorphismus $\phi_R : R \to \mathbf{C}$ sowie einen partiellen Morphismus $\phi_K : K \to \mathbf{C}$, der genau für alle $r \in K$, die sich als $r = \frac{f}{g} \in K$ mit $\phi_R(g) \neq 0$ darstellen lassen, definiert ist.

Definition:

1) Als *allgemeine geometrische Objekte* (AGO) bezeichnen wir Paare $P = (p_1, p_2)$ (genannt *Punkte*) und Tripel $g = (g_1, g_2, g_3)$ (genannt *Geraden*) von Elementen $p_1, p_2, g_1, g_2, g_3 \in K$. Letztere bezeichnen wir auch als die *Komponenten* des AGO. Wir sagen, daß dieses AGO unter der Spezifikation ϕ *korrekt spezifiziert*, wenn ϕ_K für alle beteiligten Komponenten definiert ist.

2) Als *allgemeine geometrische Konfiguration* (AGK) bezeichnen wir ein Paar (M, f), bestehend aus einer Menge M von AGO's und einer *Nichtdegenerationsbedingung* $f \in R$, so daß für jede Spezifikation ϕ, für die $\phi_R(f) \neq 0$ gilt, die AGO's aus der Menge M korrekt spezifizieren.

3) Als (elementaren) *Konstruktionsschritt* bezeichnen wir eine Vorschrift, die aus einer gegebenen AGK (M, f) ein neues AGO g und eine Nichtdegenerationsbedingung $f' \in R$ konstruiert, so daß entweder $f' = 0$ gilt oder aber $(M \cup \{g\}, f')$ eine neue AGK ist.

4) Als *geometrische Behauptung vom konstruktiven Typ* (gBkT) bezeichnen wir eine AGK (M, f) zusammen mit einem polynomialen Ausdruck g in den Komponenten der verschiedenen AGO's aus der Menge M, welcher somit zugleich ein rationaler Ausdruck aus K ist.

Die Angabe des neuen AGO g in einem Konstruktionsschritt erfolgt meist durch einen rationalen Ausdruck, in den die Komponenten der einzelnen AGO's aus M eingehen. Die Anzahl der dabei neu verwendeten Parameter bezeichnet man als den *Freiheitsgrad* des entsprechenden Konstruktionsschritts. Ist $f' = 0$ als Polynom in R, so sprechen wir von *widersprüchlichen Voraussetzungen*, d.h. der gewünschte Konstruktionsschritt ist in der gegebenen AGK nicht ausführbar. Ein Vergleich mit 4) zeigt, daß die Widersprüchlichkeit der Voraussetzungen ihrerseits eine geometrische Behauptung vom konstruktiven Typ ist.

Definition:
Wir sagen, daß die betrachtete gBkT (M, f, g) *gilt*, wenn bei jeder Spezifikation ϕ der Parameter mit $\phi_R(f) \neq 0$ (und damit die Koordinaten der AGO's aus M korrekt spezifizieren) $\phi_K(g) = 0$ gilt.

Dies entspricht der Vorstellung, die wir von AGO's als Platzhalter konkreter geometrischre Konfigurationen haben: Für jede (zulässige) Belegung der Parameter mit komplexen Zahlen entsteht eine konkrete geometrische Konfiguration, in der die untersuchte geometrische Aussage auch tatsächlich erfüllt ist.

Betrachten wir die Liste unserer bisher programmierten elementaren geometrischen Konstruktionen, so erkennen wir, daß sie alle die geforderte Spezifikation erfüllen. Wir können also mit ihrer Hilfe geometrische Sätze vom konstruktiven Typ formulieren.

Satz (über das mechanisierte Beweisen geometrischer Sätze vom konstruktiven Typ):
Eine geometrische Behauptung g vom konstruktiven Typ in einer (nicht widersprüchlichen) AGK (M, f), die in endlich vielen Konstruktionsschritten aus der leeren AGK $\{\emptyset, 1\}$ gewonnen worden ist, gilt genau dann, wenn g als rationale Funktion in K identisch Null ist.

Beweis: Offensichtlich verschwindet für $g = 0 \in K$ jede zulässige Spezifikation $\phi_K(g)$. Ist umgekehrt $g = \frac{p}{q} \neq 0$ mit $p, q \in R \setminus (0)$, so ist $p \cdot q \cdot f \neq 0$ und es gibt eine zulässige Spezifikation ϕ mit $\phi_R(p) \cdot \phi_R(q) \neq 0$, d.h. $\phi_K(g) \neq 0$. *Box*

4.4 Nichtlineare geometrische Bedingungen. Unabhängige und abhängige Parameter.

Obwohl der bisherige Zugang bereits viele geometrische Sätze erfaßt, ist er noch verallgemeinerungsbedürftig, da er davon ausgeht, daß die Komponenten jedes geometrischen Objekts in endlich vielen Schritten aus einem gegebenen Satz von Parametern durch *rationale* Operationen, also im wesentlichen linear, herzustellen sind. Dies trifft aber auf viele Konstruktionen, die z.B. Kreislinien oder Winkelhalbierende enthalten, nicht zu.

Winkel und Winkelhalbierende

Allerdings kann man Winkelhalbierende mit einem anderen Konzept auch als geometrisches Objekt vom konstruktiven Typ einführen.

Aufgabe: Zeigen Sie auf folgende Weise, daß die Winkelhalbierenden sich in einem Punkt schneiden:
A und B seien gegeben und D sei der Schnittpunkt der Winkelhalbierenden aus A und B. Dann ist C der Schnittpunkt der Geraden, die aus AB durch Spiegelung an AD bzw. BD hervorgehen. CD ist genau dann Winkelhalbierende, wenn AC bei Spiegelung an CD in BC übergeht.

Punkte auf einem Kreis

Miguelscher Kreis

Satz von Simson

4.5 Geometrische Sätze vom Gleichungstyp

Idee: Hebe die Unterscheidung zwischen abhängigen und unabhängigen Variablen wieder auf. Rechne polynomial und versuche zu verstehen, was passiert:

Normalerweise verschwindet die geometrische Bedingung nicht auf der gesamten Varietät, sondern es sind noch gewisse Nichtdegenerationsbedingungen zu berücksichtigen.

Die verschiedenen Aufgabenstellungen und ihr idealtheoretisches Gewand.

4.6 Ideale und Nullstellengebilde

Zusammenhang Ideale und Nullstellengebilde.

Dekompositionssatz für Radikalideale.

Dekomposition und Nichtdegenerationsbedingungen. Der stabile Idealquotient.

4.7 Geometriebeweise und Gröbnerbasen

Ausdividieren bekannter Nichtdegenerationsbedingungen zum Geometriebeweis.

Ausdividieren der Behauptung, um noch unbekannte Nichtdegenerationsbedingungen zu erhalten.

4.8 Unabhängige Parameter II

Definition unabhängiger Variablenmengen mod I.

unabhängige Variablen und Dekomposition. Generische und spezielle Komponenten.

Zur Berechnung unabhängiger Mengen: streng unabhängige Mengen.

Zwei Sätze über Gröbnerbasen.

4.9 Unabhängige Parameter und Geometrietheoreme

Zerlegung der Varietäten, wenn sich die abhängigen Parameter $\mathbf{x}$ linear über den unabhängigen $\mathbf{u}$ ausdrücken lassen.

Beim letzten Mal hatten wir Geometriesätze betrachtet, von denen wir auch eine konstruktive Version kennen. Unsere Beobachtung war die folgende: Die geometrischen Bedingungen bestanden aus Gleichungen, in denen die abhängigen Parameter $\mathbf{x}$ linear von den unabhängigen Parametern $\mathbf{u}$ abhingen. Das erlaubt es uns, dieses Gleichungssystem über $k(\mathbf{u})[\mathbf{x}]$ zu lösen und die gefundene Lösung in die geometrische Behauptung einzusetzen in der Hoffnung, daß der entstehende rationale Ausdruck in $k(\mathbf{u})$ zu Null simplifiziert. Dies erinnert an unser Vorgehen bei Theoremen vom konstruktiven Typ und in der Tat können wir dieselben Aussagen treffen:

1) Führt die Simplifikation auf das Nullpolynom, so ist der Satz für alle zulässigen Spezifikationen der unabhängigen Variablen (d.h. solche, für die sich die abhängigen Parameter eindeutig und nur nach den hergeleiteten Formeln ergeben; was aber für fast alle Spezifikationen erfüllt ist) der Satz richtig. Im Gegensatz zu den Sätzen vom konstruktiven Typ kann die Simplifikation nicht mit einer Fehlermeldung abbrechen, weil die geometrsiche Behauptung als polynomial vorausgesetzt worden ist. Andererseits kann oft nicht ohne Zusatzaufwand festgestellt werden, welche Spezifikationen nicht zulässig sind, weil es dafür nicht ausreicht, nur die Nenner der Ausdrücke aufzusammeln, die die abhängigen durch die unabhängigen Variablen ausdrücken (vgl. Beweis des Satz von Pappus, wo $u_2 \neq 0$ sein mußte, x_1 und x_2 aber polynomial durch $u_{1\ldots5}$ ausgedrückt werden konnten). Hat das Gleichungssystem eine quadratische Koeffizientenmatrix, wie in den meisten Fällen, ist das Nichtverschwinden deren Determinante eine solche hinreichende Bedingung.

2) Die Simplifikation ergibt $\frac{P(\mathbf{u})}{Q(\mathbf{u})} \neq 0$. Dann ist der Satz für fast alle Spezifikationen falsch und höchstens unter der zusätzlichen Voraussetzung $P(\mathbf{u}) = 0$ richtig. Damit sind die Variablen $\mathbf{u}$ aber nicht mehr (algebraisch) unabhängig.

Aufgabe: Beweisen Sie auf diesem Weg den Satz des Apollonius.

Die Rechnungen wurden also in obigem Fall im Ring $S' = k(\mathbf{u})[\mathbf{x}]$ statt wie bisher im Ring $S = k[\mathbf{u}, \mathbf{x}]$ ausgeführt. Untersuchen wir zunächst weitere Beispiele mit nichtlinearen Bedingungen:

Beispiel: Miguelscher Punkt

```
A:={0,0};
B:={1,0};
C:={u1,u2};
D:=varpoint(B,C,u3);
E:=varpoint(A,C,u4);
F:=varpoint(A,B,u5);
X:={x1,x2};

polys:={
        four_points_on_a_circle(A,F,X,E),
        four_points_on_a_circle(B,F,X,D)};

con:=   four_points_on_a_circle(C,E,X,D);

setring(x,{},lex);
setideal(polys,polys);
con mod gbasis polys;
```

Es stellt sich heraus, daß die Behauptung nicht aus den Voraussetzungen folgt. Analysiert man *gbasis polys* genauer, erkennen wir, daß es die Struktur

$$\{p_1(\mathbf{u})x_1^2 + p_2(\mathbf{u})x_1, p_3(\mathbf{u})x_2 + u_2x_1 + u_2u_5 - u_2\}$$

hat. Dieses System hat zwei Lösungen (x_1, x_2), was der Existenz von zwei Schnittpunkten der Kreise durch A, F, E und B, F, D entspricht. Einer der beiden Schnittpunkte ist F, was der Lösung $x_1 = 0$ entspricht. Dieser Punkt muß sicherlich nicht auf dem dritten Kreis liegen. Der Gröbnerfaktorisierer

```
> groebfactor polys;
```

liefert in diesem Fall die erforderliche Aufspaltung in die beiden Zweige, wobei auf dem Zweig, der X entspricht, *con* zu Null reduziert.

Beispiel: Satz vom Schnittpunkt der Winkelhalbierenden

```
A:={0,0};
B:={1,0};
C:={u1,u2};
X:={x1,x2};

polys:={
        point_on_bisector(X,A,B,C),
        point_on_bisector(X,B,C,A)};

con:=   point_on_bisector(X,C,A,B);

setring(x,{},lex);

interreduce polys;
con mod ws;
```

Als Gröbnerbasis erhalten wir hier

$$\{(4\,u_2)\,x_2^4 - (8\,u_1^2 - 8\,u_1 + 8\,u_2^2)\,x_2^3 + (4\,u_1^2\,u_2 - 4\,u_1\,u_2 + 4\,u_2^3 - 4\,u_2)\,x_2^2 + (4\,u_2^2)\,x_2 - u_2^3,$$
$$(2\,u_1\,u_2^2 - u_2^2)\,x_1 + (2\,u_2)\,x_2^3 - (4\,u_1^2 - 4\,u_1 + 2\,u_2^2)\,x_2^2 - (2\,u_1^2\,u_2 - 2\,u_1\,u_2 + 2\,u_2)\,x_2 - (u_1\,u_2^2 - u_2^2)\}$$

d.h. dieses System hat 4 Lösungen, die den vier Schnittpunkten der möglichen Auswahlen der Halbierenden von Innen- und Außenwinkel von $\angle ABC$ und $\angle BCA$ entsprechen. Jeder von ihnen liegt auf der Halbierenden entweder des Innen- oder des Außenwinkels von $\angle CAB$.

Beispiel: Simsons Gerade

vgl. geo.4

Die Gröbnerbasis des entsprechenden Gleichungssystems:

$$\{x_2^2 - (u_1^2 - u_2^2),$$
$$x_3^2 - (u_1^2 - u_3^2),$$
$$x_4^2 - (u_1^2 - u_4^2),$$
$$(2\,u_1\,u_3)\,x_7 - u_3\,x_4 + u_4\,x_3 - (u_1\,u_3 - u_1\,u_4),$$
$$(2\,u_1\,u_2)\,x_5 - u_2\,x_4 + u_4\,x_2 - (u_1\,u_2 - u_1\,u_4),$$
$$(2\,u_1^2\,u_2 - 2\,u_1^2\,u_3)\,x_6 + u_2\,x_4\,x_3 + u_3\,x_4\,x_2 - u_4\,x_3\,x_2 - (u_1^2\,u_2 - u_1^2\,u_3 + u_1^2\,u_4 - u_2\,u_3\,u_4)\}$$

In allen hier betrachteten Fällen, gibt es im Gegensatz zum linearen Fall mehrere, aber stets endlich viele Lösungen für $\mathbf{x}$ in Abhängigkeit von den Parametern $\mathbf{u}$. In manchen Fällen wie etwa beim Miguelschen Punkt kann man die einzelnen Lösungen explizit in $k(\mathbf{u})$ ausdrücken. In anderen Fällen hätte man die einzelnen Zweige der Lösungsmenge durch mehr (Schnittpunkt der Winkelhalbierenden) oder weniger (Simsons Gerade) komplizierte Wurzelausdrücke in den unabhängigen

Variablen angeben können. Für Simsons Gerade etwa würde man

$$\begin{aligned}
x_2 &= \pm\sqrt{u_1^2-u_2^2},\\
x_3 &= \pm\sqrt{u_1^2-u_3^2},\\
x_4 &= \pm\sqrt{u_1^2-u_4^2},\\
x_7 &= \tfrac{u_3\,x_4-u_4\,x_3+u_1\,u_3-u_1\,u_4}{2\,u_1\,u_3},\\
x_5 &= \tfrac{u_2\,x_4-u_4\,x_2+u_1\,u_2-u_1\,u_4}{2\,u_1\,u_2},\\
x_6 &= \tfrac{-u_2\,x_4\,x_3-u_3\,x_4\,x_2+u_4\,x_3\,x_2+u_1^2\,u_2-u_1^2\,u_3+u_1^2\,u_4-u_2\,u_3\,u_4}{2\,u_1^2\,u_2-2\,u_1^2\,u_3}
\end{aligned}$$

erhalten.

Das ist im allgemeinen nicht mehr möglich, wenn Polynome vom Grad 5 oder höher auftreten. Aber selbst solche Wurzelausdrücke mit komplizierten symbolischen Ausdrücken als Radikanden sind von den heute verfügbaren Simplifikationssystemen nur unzureichend simplifizierbar. Statt dessen arbeiten die meisten CAS in einer solchen Situation heute mit RootOf-Symbolen. So liefert Reduce etwa für das zweite Beispiel auf

```
> solve(polys,x)
```

die Antwort

$$\begin{aligned}
x_2 = {} & \mathit{RootOf}((4\,u_2)\,X^4-(8\,u_1^2-8\,u_1+8\,u_2^2)\,X^3+(4\,u_1^2\,u_2-4\,u_1\,u_2+4\,u_2^3-4\,u_2)\,X^2\\
& +(4\,u_2^2)\,X-u_2^3,X),\\
x_1 = {} & \tfrac{(2\,u_2)\,x_2^3-(4\,u_1^2-4\,u_1+2\,u_2^2)\,x_2^2-(2\,u_1^2\,u_2-2\,u_1\,u_2+2\,u_2)\,x_2-(u_1\,u_2^2-u_2^2)}{u_2^2(1-2\,u_1)}
\end{aligned}$$

Die Einführung eines solchen Symbols bedeutet, in einer entsprechenden algebraischen Erweiterung zu rechnen, d.h. ein neues Symbol X einzuführen, von dem als Simplifikationsregel einzig die aus dem Minimalpolynom $p(X)=0$ hergeleitete Ersetzungsregel Verwendung findet. Dieser Ansatz unterscheidet insbesondere nicht zwischen den verschiedenen Wurzeln desselben Minimalpolynoms, sondern führt die Rechnungen in der entsprechenden algebraischen Erweiterung $K[X]/(p(X))$ direkt aus. Sind mehrere algebraische Symbole einzuführen, so kann man entweder versuchen, ein gemeinsames neues Symbol zu finden, durch das sich alle anderen ausdrücken lassen, oder aber die entsprechenden definierenden Gleichungen nebeneinander betrachten. Der zweite Lösungsansatz führt zur Betrachtung der Erweiterung $K[\mathbf{x}]/I$, wobei I das durch die definierenden Gleichungen der einzelnen algebraischen Elemente erzeugte Ideal ist. Selbst im Falle einfacher definierender Gleichungen ist aber nicht gesichert, daß dabei ein Körper entsteht, d.h. I ein Primideal ist. So zerfällt etwa das Ideal $\{x^2-2, y^2-3, z^2-6\}$ in die beiden Komponenten $\{z^2-6, 3\,x-y\,z, y^2-3\}$ und $\{z^2-6, 3\,x+y\,z, y^2-3\}$. Allerdings ist das Ideal I stets nulldimensional, da ja alle neu eingeführten Variablen algebraisch abhängig sind. Den Zusammenhang mit der bisherigen Betrachtung von verschiedenen Zweigen mehrdeutiger algebraischer (Wurzel-)funktionen bekommt man, wenn man die Nullstellen von I über dem algebraischen Abschluß $\bar{K}$ von K betrachtet. Da I nulldimensional ist, zerfällt seine Nullstellenmenge in endlich viele "Punkte" (mit Koordinaten in $\bar{K}$), was der Zerlegung in irreduzible Komponenten der Menge $Z_{\bar{K}}(I)$ entspricht, die wir im vorangegangenen Abschnitt betrachtet haben. Einsetzen verschiedener algebraischer Werte für die abhängigen Variablen in eine zu untersuchende polynomiale Bedingung entspricht also dem Verschwinden dieses Polynoms im betrachteten Punkt.

Die hier beschriebene Struktur entspricht genau der, die wir im Verlauf des Beweisens von Sätzen vom Gleichungstyp angetroffen haben: In unserem Kontext betrachten wir den Faktorring $K[\mathbf{x}]/I'$, wobei $K=k(\mathbf{u})$ der Körper der rationalen Funktionen in den unabhängigen Variablen und I' das durch die geometrischen Voraussetzungen bestimmte Ideal ist, allerdings nicht wie bisher in $S := k[\mathbf{u},\mathbf{x}]$ betrachtet, sondern im Ring $S' := K[\mathbf{x}]$, der S als Unterring enthält. Ist $h(\mathbf{x},\mathbf{u})$ das Polynom, das unsere geometrische Behauptung ausdrückt, so impliziert die etwa über Normalformberechnung bzgl. einer Gröbnerbasis von I' nachprüfbare Beziehung $h \in I'$, daß h auf allen "Punkten" von $Z_{\bar{K}}(I')$ verschwindet, d.h. h für alle zulässigen Spezifikationen der unabhängigen Variablen und jede der daraus ableitbaren endlich vielen Möglichkeiten für die abhängigen Parameter verschwindet, unser Geometrietheorem also "im allgemeinen" gültig ist. Es bleibt allerdings offen, was genau unter "im allgemeinen" zu verstehen ist.

4.10 Generisch gültige Geometrietheoreme

Wir wollen nun den Zusammenhang zwischen unserer Ausgangsfragestellung und der Antwort, die wir im vorigen Paragraph gegeben haben, genauer studieren.

Dazu betrachten wir ein Geometrietheorem vom Gleichungstyp, dessen Voraussetzungen B ein Ideal $I = I(B) \subset S := k[\mathbf{u}, \mathbf{x}]$ erzeugen. Die Menge der in den einzelnen Polynomen vorkommenden Variablen sei in eine Teilmenge $\mathbf{u}$ unabhängiger bzgl. I und eine Teilmenge $\mathbf{x}$ davon abhängiger Variablen zerlegt. Wir betrachten weiterhin den Körper $K := k(\mathbf{u})$ und den Polynomring $S' := K[\mathbf{x}]$, der S als Unterring enthält. B erzeugt also auch in diesem Ring ein Ideal $I' = I \cdot S'$, das *Erweiterungsideal* von I. Umgekehrt können wir mit einem Ideal $I' \subset S'$ das Ideal $c(I') := I' \cap S$ ins S verbinden, das sogenannte *Kontraktionsideal.* Sicherlich ist $I \subset c(I')$. Gegenstand unserer weiteren Untersuchungen soll eine genauere Analyse des Zusammenhangs zwischen diesen drei Idealen sein.

Die Elemente des Rings S' sind Polynome in den Variablen $\mathbf{x}$ mit rationalen Funktionen in $\mathbf{u}$ als Koeffizienten. Durch Hauptnennerbildung überzeugt man sich leicht, daß man jedes Element aus S' in der Form $\frac{z(\mathbf{x},\mathbf{u})}{n(\mathbf{u})}$ mit $z \in S$ und $n \in k[\mathbf{u}] \setminus (0)$ darstellen kann. Die Menge U ist *multiplikativ*, d.h. $n_1, n_2 \in U$ impliziert $n_1 n_2 \in U$, womit die üblichen Rechenregeln für Brüche Anwendung finden können. Wir schreiben deshalb auch

$$S' = U^{-1}S := \{\frac{z}{n} \ : \ z \in S, \ n \in U\}$$

und nennen den Ring S' die *Lokalisierung* von S nach der multiplkativen Menge U.

Zunächst wollen wir das Erweiterungsideal $I' = I \cdot S'$ genauer beschreiben. Ist $B = \{f_i, \ i = 1, \ldots, m\} \subset S$ eine Basis von I, so lassen sich alle Elemente aus I' in der Form

$$u = \sum_i \frac{z_i}{n_i} f_i = \frac{\sum_i h_i f_i}{n}$$

mit $z_i, h_i \in S, \ n_i, n \in U$ darstellen. Wir erkennen also, daß I' aus genau den Elementen von S' besteht, die sich in der Form $\frac{i}{n}$ mit $i \in I, n \in U$ darstellen lassen. Entsprechend besteht $c(I')$, das Kontraktionsideal, aus allen solchen Elementen, die außerdem noch polynomial auch in $\mathbf{u}$ sind, d.h. für die zusätzlich i vollständig durch n teilbar ist:

$$c(I') = \{u \in S : \ \exists\, n \in U \, (n \cdot u \in I)\}.$$

Das erinnert an die Definition des Idealquotienten. Allerdings kommen die Kofaktoren hier nicht aus einem Ideal.

Satz:

(1) Sein I ein Radikalideal und $I = \cap P_\alpha$ dessen zerlegung in Primkomponenten. Dann gilt

$$I' = I \cdot S' = \cap P_\alpha \cdot S'.$$

(2)

$$P_\alpha \cdot S' = \begin{cases} \text{ein Primideal } Q_\alpha \subset S' \text{ mit } c(Q_\alpha) = P_\alpha & \text{wenn } P_\alpha \cap U = \emptyset \\ (1) & \text{wenn } P_\alpha \cap U \neq \emptyset \end{cases}$$

Beweis:

(1) Wegen $I \subset \cap P_\alpha$ folgt $I \cdot S' \subset \cap P_\alpha \cdot S'$. Sei umgekehrt $u \in \cap P_\alpha \cdot S'$. Nach geeigneter Hauptnennerbildung hat es eine Darstellung der Form $u = \frac{z}{n}$ mit $z \in \cap P_\alpha = I, \ n \in U$, also $u \in I \cdot S'$.

(2) Sei $0 \neq s \in P_\alpha \cap U$. Dann ist $1 = \frac{s}{s} \in P_\alpha \cdot S'$.
Sei $P_\alpha \cap U = \emptyset$ und $Q_\alpha := P_\alpha \cdot S'$.
Q_α ist ein Primideal: Aus

$$u_1 u_2 = \frac{p_1}{n_1}\frac{p_2}{n_2} = \frac{p}{n} \in Q_\alpha$$

mit $p_1, p_2 \in S,\ p \in P_\alpha,\ n, n_1, n_2 \in U$ folgt $n \cdot p_1 p_2 \in P_\alpha$ und wegen $n \notin P_\alpha$ und dessen Primidealeigenschaft schließlich $p_1 p_2 \in P_\alpha$.
$c(Q_\alpha) = \{u \in S : \exists n \in U\,(n \cdot u \in P_\alpha)\}$. Wie eben folgt dann bereits $u \in P_\alpha$. $\square$

Folgerung:
Sei h ein Polynom in S, G eine Gröbnerbasis von I' in S' und $NF(h, G) = 0$, d.h. $h \in I'$. Dann gilt

$$h \in c(I') = \cap\{P_\alpha \ :\ P_\alpha \cap U = \emptyset\},$$

d.h. das Polynom verschwindet auf allen generischen Komponenten von $Z(I)$.

Wir sagen in diesem Fall, daß der geometrische Satz bzgl. der unabhängigen Variablenmenge $\mathbf{u}$ *generisch richtig ist*, was folgendes heißt: Der Satz $h = 0$ ist höchstens auf speziellen Komponenten von $Z(I)$, auf denen aber die Variablen $\mathbf{u}$ nicht mehr unabhängig sind, falsch. Jede solche Komponente enthält aber im definierenden Ideal ein Polynom $g_i(\mathbf{u})$. Das Produkt dieser Polynome können wir dann als Nichtdegenerationsbedingung nehmen. Ein geometrischer Satz ist also bzgl. $\mathbf{u}$ genau dann generisch richtig, wenn es eine Nichtdegenerationsbedingung $g \in k[\mathbf{u}]$ gibt, so daß

$$\{B,\ g \neq 0 \implies h = 0\}$$

gilt. Der Satz ist also für jede "genügend allgemeine" Belegung der unabhängigen Parameter richtig.
Generell, wenn $NF(h, G)$ nicht verschwindet, wie oben im Beispiel "Miguelscher Punkt", liefern uns Untersuchungen in S' Aussagen, die das Verhalten auf speziellen Komponenten ausblenden. In diesem Beispiel hat $Z(I)$ zwei generische Komponenten. Eine entspricht dem Schnittpunkt F der Kreise durch A, F, E und B, F, D, die andere dem gesuchten Schnittpunkt X. Auf der ersteren Komponente gilt der Satz nicht, auf der zweiteren sehr wohl. Der Gröbnerfaktorisierer zeigt, daß $Z(I)$ daneben noch wenigstens 5 weitere spezielle Komponenten hat, die die Bedingungen $u_2 = 0, u_5 = 0, u_3 = 1, u_5 = 1$ und $u_3 = u_5 = 1$ enthalten, also degenerierten Lagen entsprechen, wo z.B. zwei der drei Punkte, die einen Kreis bestimmen sollen, zusammenfallen. In einem solchen Fall ist aber der Kreis und damit auch der Schnittpunkt X nicht mehr eindeutig bestimmt, so daß wir auch nicht prüfen können, ob er auf dem dritten Kreis liegt.

Zur Bestimmung von g:
Obiger Weg über die Berechnung einer Primzerlegung ist zu aufwendig, um eine Nichtdegenerationsbedingung zu finden. Es stellt sich allerdings heraus, daß man g bereits aus einer Gröbnerbasis von B bzgl. einer speziell gewählten Termordnung ablesen kann.

Satz:
Sei $<$ eine Termordnung auf $T(\mathbf{u}, \mathbf{x})$ mit $\mathbf{u} \ll \mathbf{x}$ und $B \subset S$ eine (polynomiale) Basis von I.
Sei G eine Gröbnerbasis von I bzgl. $<$. Dann ist G auch eine Gröbnerbasis von $I' = I \cdot S'$ bzgl. der induzierten Termordnung auf $T(\mathbf{x}) \subset T(\mathbf{u}, \mathbf{x})$.

Beweis:
Für $f \in S$ ist $lt(f)$ ein Term in $\mathbf{x}$ und $\mathbf{u}$, läßt sich also eindeutig in seine Komponenten $lt(f) = lt_x(f)\, lt_u(f)$ in $T(\mathbf{x})$ und $T(\mathbf{u})$ zerlegen. Für die Gröbnerbasis G gilt

$$\forall\, f \in I\ \exists g \in G\ (lt(g)\,|\,lt(f)).$$

Letzteres bedeutet insbesondere $lt_x(g)\,|\,lt_x(f)$ und $lt_u(g)\,|\,lt_u(f)$. Ist nun $u = \frac{f}{n} \in I'$ mit $f \in I,\ n \in k[\mathbf{u}]$, so gilt $lt_x(u) = lt_x(f)$ und folglich auch $lt_x(g)\,|\,lt_x(u)$ in S'. $\square$

Obwohl G eine Gröbnerbasis von I' ist, muß es keine minimale reduzierte Gröbnerbasis sein.

Beispiel: geo.4 – Die Voraussetzungen des Satzes von Pappus

Wir wissen aber, daß man aus einer Gröbnerbasis eine minimale auswählen kann, indem man einfach die Elemente streicht, die nicht zu einer Minimalbasis des Leittermideal (in $T(\mathbf{x})$) gehören. Sei also $G' \subset G$ eine auf diese Weise konstruierte minimale Gröbnerbasis von I'.

4.11 Unabhängige Parameter und Geometrietheoreme

Zerlegung der Varietäten, wenn sich die abhängigen Parameter $\mathbf{x}$ linear über den unabhängigen $\mathbf{u}$ ausdrücken lassen.

Beim letzten Mal hatten wir Geometriesätze betrachtet, von denen wir auch eine konstruktive Version kennen. Unsere Beobachtung war die folgende: Die geometrischen Bedingungen bestanden aus Gleichungen, in denen die abhängigen Parameter $\mathbf{x}$ linear von den unabhängigen Parametern $\mathbf{u}$ abhingen. Das erlaubt es uns, dieses Gleichungssystem über $k(\mathbf{u})[\mathbf{x}]$ zu lösen und die gefundene Lösung in die geometrische Behauptung einzusetzen in der Hoffnung, daß der entstehende rationale Ausdruck in $k(\mathbf{u})$ zu Null simplifiziert. Dies erinnert an unser Vorgehen bei Theoremen vom konstruktiven Typ und in der Tat können wir dieselben Aussagen treffen:

1) Führt die Simplifikation auf das Nullpolynom, so ist der Satz für alle zulässigen Spezifikationen der unabhängigen Variablen (d.h. solche, für die sich die abhängigen Parameter eindeutig und nur nach den hergeleiteten Formeln ergeben; was aber für fast alle Spezifikationen erfüllt ist) der Satz richtig. Im Gegensatz zu den Sätzen vom konstruktiven Typ kann die Simplifikation nicht mit einer Fehlermeldung abbrechen, weil die geometrsiche Behauptung als polynomial vorausgesetzt worden ist. Andererseits kann oft nicht ohne Zusatzaufwand festgestellt werden, welche Spezifikationen nicht zulässig sind, weil es dafür nicht ausreicht, nur die Nenner der Ausdrücke aufzusammeln, die die abhängigen durch die unabhängigen Variablen ausdrücken (vgl. Beweis des Satz von Pappus, wo $u_2 \neq 0$ sein mußte, x_1 und x_2 aber polynomial durch $u_{1\ldots5}$ ausgedrückt werden konnten). Hat das Gleichungssystem eine quadratische Koeffizientenmatrix, wie in den meisten Fällen, ist das Nichtverschwinden deren Determinante eine solche hinreichende Bedingung.

2) Die Simplifikation ergibt $\frac{P(\mathbf{u})}{Q(\mathbf{u})} \neq 0$. Dann ist der Satz für fast alle Spezifikationen falsch und höchstens unter der zusätzlichen Voraussetzung $P(\mathbf{u}) = 0$ richtig. Damit sind die Variablen $\mathbf{u}$ aber nicht mehr (algebraisch) unabhängig.

Aufgabe: Beweisen Sie auf diesem Weg den Satz des Apollonius.

Die Rechnungen wurden also in obigem Fall im Ring $S' = k(\mathbf{u})[\mathbf{x}]$ statt wie bisher im Ring $S = k[\mathbf{u}, \mathbf{x}]$ ausgeführt. Untersuchen wir zunächst weitere Beispiele mit nichtlinearen Bedingungen B. In diesem Fall ist es nicht so einfach, die Gleichungen nach den abhängigen Variablen aufzulösen. In jedem Fall wird die Lösung mehrere Zweige umfassen und neben rationalen meist auch kompliziertere algebraische Operationen wie etwa Wurzeln enthalten. Alle Lösungen $\mathbf{x}^{(a)}(\mathbf{u})$ sind jedoch gemeinsame Nullstellen der Polynome $f \in B$. Ist deshalb die geometrische Behauptung g im Ideal $I(B)$ enthalten, so gilt auch $g(\mathbf{x}^{(a)}) = 0$ als (nicht mehr rationale, sondern nun algebraische) Funktion in $\mathbf{u}$ und unser Geometrietheorem ist aus ähnlichen Überlegungen wie für den Fall linearer Gleichungen im allgemeinen gültig. $g \in I(B)$ kann über die Normalformberechnung bzgl. einer (Gröbner-)Basis geprüft werden.

Beispiel: Miguelscher Punkt

```
A:={0,0};
B:={1,0};
C:={u1,u2};
D:=varpoint(B,C,u3);
E:=varpoint(A,C,u4);
F:=varpoint(A,B,u5);
X:={x1,x2};
```

```
polys:={
four_points_on_a_circle(A,F,X,E),
four_points_on_a_circle(B,F,X,D)};

con:= four_points_on_a_circle(C,E,X,D);

setring(x,{},lex);
setideal(polys,polys);
con mod gbasis polys;
```

Es stellt sich heraus, daß *con* $\in I(polys)$ nicht gilt, die Behauptung also im allgemeinen nicht aus den angegebenen Voraussetzungen folgt. Analysiert man die berechnete Gröbnerbasis genauer, erkennen wir, daß sie die Struktur

$$\{p_1(\mathbf{u})x_1^2 + p_2(\mathbf{u})x_1, p_3(\mathbf{u})x_2 + u_2x_1 + u_2u_5 - u_2\}$$

hat. Wir haben damit unser Ausgangssystem *polys* in eine Dreiecksgestalt gebracht, die es uns in diesem Fall erlaubt, die Lösungen explizit durch rationale Ausdrücke anzugeben. Es gibt zwei Lösungszweige (x_1, x_2), was der Existenz von zwei Schnittpunkten der Kreise durch A, F, E und B, F, D entspricht. Einer der beiden Schnittpunkte ist F, was der Lösung $x_1 = 0$ entspricht. Dieser Punkt muß sicherlich nicht auf dem dritten Kreis liegen. Setzen wir dagegen die andere Lösung

$$x_1 = -\frac{p_2(\mathbf{u})}{p_1(\mathbf{u})}, \quad x_2 = \frac{u_2(1 - u_5 - x_1)}{p_3(\mathbf{u})}$$

in die Behauptung *con* ein, simplifiziert die entsprechende rationale Funktion in $\mathbf{u}$ zu Null, was den Satz vom Miguelschen Punkt "im allgemeinen" beweist.

Beispiel: Satz vom Schnittpunkt der Winkelhalbierenden

```
A:={0,0};
B:={1,0};
C:={u1,u2};
X:={x1,x2};

polys:={
point_on_bisector(X,A,B,C),
point_on_bisector(X,B,C,A)};

con:= point_on_bisector(X,C,A,B);

setring(x,{},lex);

interreduce polys;
con mod ws;
```

Wir schließen *con* $\in I(B)$, d.h. die Gültigkeit des Satzes "im allgemeinen". Als Gröbnerbasis erhalten wir hier

$$\begin{aligned}&\{(4\,u_2)\,x_2^4 - (8\,u_1^2 - 8\,u_1 + 8\,u_2^2)\,x_2^3 + (4\,u_1^2\,u_2 - 4\,u_1\,u_2 + 4\,u_2^3 - 4\,u_2)\,x_2^2 + (4\,u_2^2)\,x_2 - u_2^3,\\ &(2\,u_1\,u_2^2 - u_2^2)\,x_1 + (2\,u_2)\,x_2^3 - (4\,u_1^2 - 4\,u_1 + 2\,u_2^2)\,x_2^2 - (2\,u_1^2\,u_2 - 2\,u_1\,u_2 + 2\,u_2)\,x_2 - (u_1\,u_2^2 - u_2^2)\}.\end{aligned}$$

polys hat also 4 Lösungszweige, die den vier Schnittpunkten der möglichen Auswahlen der Halbierenden von Innen- und Außenwinkel von $\angle\, ABC$ und $\angle\, BCA$ entsprechen. Jeder von ihnen liegt auf der Halbierenden entweder des Innen- oder des Außenwinkels von $\angle\, CAB$. Will man explizite Formeln für die Koordinaten der vier Schnittpunkte berechnen, so ist die Lösungsformel für Gleichungen vierten Grades anzusetzen, was zu extrem komplizierten Ausdrücken führt.

Beispiel: Simsons Gerade

```
M:={0,0};
A:={0,u1};
B:={u2,x2};
C:={u3,x3};
P:={u4,x4};
R:=varpoint(A,B,x5);
S:=varpoint(B,C,x6);
T:=varpoint(A,C,x7);

polys:={
orthogonal(line(A,B),line(P,R)),
orthogonal(line(A,C),line(P,T)),
orthogonal(line(B,C),line(P,S)),
        sqrdist(M,A)-sqrdist(M,P),
        sqrdist(M,B)-sqrdist(M,P),
        sqrdist(M,C)-sqrdist(M,P)};

con:=num collinear(R,S,T);

clear x,u; xvars:=reverse for i:=1:7 collect mkid(x,i);

setring(xvars,{},lex);

setideal(polys,polys);

gbasis polys;

con mod ws;
```

Wir erhalten wieder $con \in I(polys)$. Die Gröbnerbasis des entsprechenden Systems hat in diesem Fall die Gestalt

$$
\begin{aligned}
&\{x_2^2 - (u_1^2 - u_2^2),\\
&x_3^2 - (u_1^2 - u_3^2),\\
&x_4^2 - (u_1^2 - u_4^2),\\
&(2\,u_1\,u_3)\,x_7 - u_3\,x_4 + u_4\,x_3 - (u_1\,u_3 - u_1\,u_4),\\
&(2\,u_1\,u_2)\,x_5 - u_2\,x_4 + u_4\,x_2 - (u_1\,u_2 - u_1\,u_4),\\
&(2\,u_1^2\,u_2 - 2\,u_1^2\,u_3)\,x_6 + u_2\,x_4\,x_3 + u_3\,x_4\,x_2 - u_4\,x_3\,x_2 - (u_1^2\,u_2 - u_1^2\,u_3 + u_1^2\,u_4 - u_2\,u_3\,u_4)\}
\end{aligned}
$$

Die letzten drei Gleichungen erlauben es, $x_{5\ldots7}$ rational durch $\mathbf{u}$ und $x_{2\ldots4}$ auszudrücken. Mehrdeutigkeit der Lösung entsteht aus den ersten drei Gleichungen, die jeweils zwei Möglichkeiten für $x_{2\ldots4}$ zulassen. Dies entspricht der Auswahl der Parametrisierung von B, C, P. Auf dem betrachteten Kreis gibt es im allgemeinen zwei Punkte mit vorgegebener x-Koordinate. Dies kann man vermeiden, indem man eine rationale Parametrisierung der Punkte des Kreises verwendet, was in diesem Fall sogar auf ein Theorem vom konstruktiven Typ führt.

In allen hier betrachteten Fällen, gibt es im Gegensatz zum linearen Fall mehrere, aber stets endlich viele Lösungen für $\mathbf{x}$ in Abhängigkeit von den Parametern $\mathbf{u}$. In manchen Fällen wie etwa beim Miguelschen Punkt kann man die einzelnen Lösungen explizit in $k(\mathbf{u})$ ausdrücken. In anderen Fällen hätte man die einzelnen Zweige der Lösungsmenge durch mehr (Schnittpunkt der Winkelhalbierenden) oder weniger (Simsons Gerade) komplizierte Wurzelausdrücke in den unabhängigen

Variablen angeben können. Für Simsons Gerade etwa würde man

$$
\begin{aligned}
x_2 &= \pm\sqrt{u_1^2 - u_2^2},\\
x_3 &= \pm\sqrt{u_1^2 - u_3^2},\\
x_4 &= \pm\sqrt{u_1^2 - u_4^2},\\
x_7 &= \tfrac{u_3\,x_4 - u_4\,x_3 + u_1\,u_3 - u_1\,u_4}{2\,u_1\,u_3},\\
x_5 &= \tfrac{u_2\,x_4 - u_4\,x_2 + u_1\,u_2 - u_1\,u_4}{2\,u_1\,u_2},\\
x_6 &= \tfrac{-u_2\,x_4\,x_3 - u_3\,x_4\,x_2 + u_4\,x_3\,x_2 + u_1^2\,u_2 - u_1^2\,u_3 + u_1^2\,u_4 - u_2\,u_3\,u_4}{2\,u_1^2\,u_2 - 2\,u_1^2\,u_3}
\end{aligned}
$$

erhalten.

Eine solche Darstellung durch Radikale ist im allgemeinen nicht mehr möglich, wenn Polynome vom Grad 5 oder höher auftreten. Aber selbst solche Wurzelausdrücke mit komplizierten symbolischen Ausdrücken als Radikanden sind von den heute verfügbaren Simplifikationssystemen nur unzureichend simplifizierbar. Statt dessen arbeiten die meisten CAS in einer solchen Situation heute mit RootOf-Symbolen. So liefert Reduce etwa für das zweite Beispiel auf

```
> solve(polys,x)
```

die Antwort

$$
\begin{aligned}
x_2 = \mathrm{RootOf}(&(4\,u_2)\,X^4 - (8\,u_1^2 - 8\,u_1 + 8\,u_2^2)\,X^3\\
&+(4\,u_1^2\,u_2 - 4\,u_1\,u_2 + 4\,u_2^3 - 4\,u_2)\,X^2 + (4\,u_2^2)\,X - u_2^3, X),\\
x_1 = \tfrac{(2\,u_2)\,x_2^3 - (4\,u_1^2 - 4\,u_1 + 2\,u_2^2)\,x_2^2 - (2\,u_1^2\,u_2 - 2\,u_1\,u_2 + 2\,u_2)\,x_2 - (u_1\,u_2^2 - u_2^2)}{u_2^2(1 - 2\,u_1)}&
\end{aligned}
$$

Die Einführung eines solchen Symbols bedeutet, in einer entsprechenden algebraischen Erweiterung zu rechnen, d.h. ein neues Symbol X einzuführen, von dem als Simplifikationsregel einzig die aus dem Minimalpolynom $p(X) = 0$ hergeleitete Ersetzungsregel Verwendung findet. Dieser Ansatz unterscheidet insbesondere nicht zwischen den verschiedenen Wurzeln desselben Minimalpolynoms, sondern führt die Rechnungen in der entsprechenden algebraischen Erweiterung $K[X]/(p(X))$ direkt aus. Sind mehrere algebraische Symbole einzuführen, so kann man entweder versuchen, ein gemeinsames neues Symbol zu finden, durch das sich alle anderen ausdrücken lassen, oder aber die entsprechenden definierenden Gleichungen nebeneinander betrachten. Der zweite Lösungsansatz führt zur Betrachtung der Erweiterung $K[\mathbf{x}]/I$, wobei I das durch die definierenden Gleichungen der einzelnen algebraischen Elemente erzeugte Ideal ist. Selbst im Falle einfacher definierender Gleichungen ist aber nicht gesichert, daß dabei ein Körper entsteht, d.h. I ein Primideal ist. So zerfällt etwa das Ideal $\{x^2 - 2, y^2 - 3, z^2 - 6\}$ in die beiden Komponenten $\{z^2 - 6, 3\,x - y\,z, y^2 - 3\}$ und $\{z^2 - 6, 3\,x + y\,z, y^2 - 3\}$. Allerdings ist das Ideal I stets nulldimensional, da ja alle neu eingeführten Variablen algebraisch abhängig sind. Den Zusammenhang mit der bisherigen Betrachtung von verschiedenen Zweigen mehrdeutiger algebraischer (Wurzel-)funktionen bekommt man, wenn man die Nullstellen von I über dem algebraischen Abschluß $\bar{K}$ von K betrachtet. Da I nulldimensional ist, zerfällt seine Nullstellenmenge in endlich viele "Punkte" (mit Koordinaten in $\bar{K}$), was der Zerlegung in irreduzible Komponenten der Menge $Z_{\bar{K}}(I)$ entspricht, die wir im vorangegangenen Abschnitt betrachtet haben. Einsetzen verschiedener algebraischer Werte für die abhängigen Variablen in eine zu untersuchende polynomiale Bedingung entspricht also dem Verschwinden dieses Polynoms im betrachteten Punkt.

Die hier beschriebene Struktur ist dieselbe, die wir im Verlauf des Beweisens von Sätzen vom Gleichungstyp angetroffen haben: In unserem Kontext betrachten wir den Faktorring $K[\mathbf{x}]/I'$, wobei $K = k(\mathbf{u})$ der Körper der rationalen Funktionen in den unabhängigen Variablen und I' das durch die geometrischen Voraussetzungen bestimmte Ideal ist, allerdings nicht wie bisher in $S := k[\mathbf{u}, \mathbf{x}]$

betrachtet, sondern im Ring $S' := K[\mathbf{x}]$, der S als Unterring enthält. Ist $h(\mathbf{x},\mathbf{u})$ das Polynom, das unsere geometrische Behauptung ausdrückt, so hatten wir gesehen, daß $h \in I'$ das Verschwinden von h auf allen "Punkten" von $Z_{\bar{K}}(I')$ impliziert, d.h. h für alle zulässigen Spezifikationen der unabhängigen Variablen und jede der daraus ableitbaren endlich vielen Möglichkeiten für die abhängigen Parameter verschwindet, unser Geometrietheorem also "im allgemeinen" gültig ist, was im nächsten Abschnitt nun genauer untersucht werden soll.

4.12 Generisch gültige Geometrietheoreme

Betrachten wir ein Geometrietheorem vom Gleichungstyp, dessen Voraussetzungen B ein Ideal $I = I(B) \subset S := k[\mathbf{u},\mathbf{x}]$ erzeugen. Die Menge der in den einzelnen Polynomen vorkommenden Variablen sei in eine Teilmenge $\mathbf{u}$ unabhängiger bzgl. I und eine Teilmenge $\mathbf{x}$ davon abhängiger Variablen zerlegt. Wir betrachten weiterhin den Körper $K := k(\mathbf{u})$ und den Polynomring $S' := K[\mathbf{x}]$, der S als Unterring enthält. B erzeugt also auch in diesem Ring ein Ideal $I' = I \cdot S'$, das *Erweiterungsideal* von I. Umgekehrt können wir mit einem Ideal $I' \subset S'$ das Ideal $c(I') := I' \cap S$ ins S verbinden, das sogenannte *Kontraktionsideal*. Sicherlich ist $I \subset c(I')$. Gegenstand unserer weiteren Untersuchungen soll eine genauere Analyse des Zusammenhangs zwischen diesen drei Idealen sein.

Die Elemente des Rings S' sind Polynome in den Variablen $\mathbf{x}$ mit rationalen Funktionen in $\mathbf{u}$ als Koeffizienten. Durch Hauptnennerbildung überzeugt man sich leicht, daß man jedes Element aus S' in der Form $\frac{z(\mathbf{x},\mathbf{u})}{n(\mathbf{u})}$ mit $z \in S$ und $n \in U := k[\mathbf{u}] \setminus (0)$ darstellen kann. Die Menge U ist *multiplikativ*, d.h. $n_1, n_2 \in U$ impliziert $n_1 n_2 \in U$, womit die üblichen Rechenregeln für Brüche Anwendung finden können. Wir schreiben deshalb auch

$$S' = U^{-1}S := \{\frac{z}{n} \ : \ z \in S,\ n \in U\}$$

und nennen den Ring S' die *Lokalisierung* von S nach der multiplkativen Menge U.

Zunächst wollen wir das Erweiterungsideal $I' = I \cdot S'$ genauer beschreiben. Ist $B = \{f_i,\ i = 1,\dots,m\} \subset S$ eine Basis von I, so lassen sich alle Elemente aus I' in der Form

$$u = \sum_i \frac{z_i}{n_i} f_i = \frac{\sum_i h_i f_i}{n}$$

mit $z_i, h_i \in S,\ n_i, n \in U$ darstellen. Wir erkennen also, daß I' aus genau den Elementen von S' besteht, die sich in der Form $\frac{i}{n}$ mit $i \in I, n \in U$ darstellen lassen. Entsprechend besteht das Kontraktionsideal $c(I')$ aus allen solchen Elementen, die außerdem noch polynomial auch in $\mathbf{u}$ sind, d.h. für die zusätzlich i vollständig durch n teilbar ist:

$$c(I') = \{u \in S : \ \exists\, n \in U\, (n \cdot u \in I)\}.$$

Das erinnert an die Definition des Idealquotienten. Allerdings kommen die Kofaktoren hier nicht aus einem Ideal.

Satz:
(1) Sein I ein Radikalideal und $I = \cap P_\alpha$ dessen Zerlegung in Primkomponenten. Dann gilt

$$I' = I \cdot S' = \cap P_\alpha \cdot S'.$$

(2)

$$P_\alpha \cdot S' = \begin{cases} \text{ein Primideal } Q_\alpha \subset S' \text{ mit } c(Q_\alpha) = P_\alpha & \text{wenn } P_\alpha \cap U = \emptyset \\ (1) & \text{wenn } P_\alpha \cap U \neq \emptyset \end{cases}$$

Beweis:
(1) Wegen $I \subset \cap P_\alpha$ folgt $I \cdot S' \subset \cap P_\alpha \cdot S'$. Sei umgekehrt $u \in \cap P_\alpha \cdot S'$. Nach geeigneter Hauptnennerbildung hat u eine Darstellung der Form $u = \frac{z}{n}$ mit $z \in \cap P_\alpha = I,\ n \in U$, also $u \in I \cdot S'$.

(2) Sei $0 \neq s \in P_\alpha \cap U$. Dann ist $1 = \frac{s}{s} \in P_\alpha \cdot S'$.
Sei $P_\alpha \cap U = \emptyset$ und $Q_\alpha := P_\alpha \cdot S'$.
Q_α ist ein Primideal: Aus

$$u_1 u_2 = \frac{p_1}{n_1}\frac{p_2}{n_2} = \frac{p}{n} \in Q_\alpha$$

mit $p_1, p_2 \in S,\ p \in P_\alpha,\ n, n_1, n_2 \in U$ folgt $n \cdot p_1 p_2 \in P_\alpha$ und wegen $n \notin P_\alpha$ und dessen Primidealeigenschaft schließlich $p_1 p_2 \in P_\alpha$, also $p_1 \in P_\alpha$ oder $p_2 \in P_\alpha$.
$c(Q_\alpha) = \{u \in S :\ \exists n \in U\,(n \cdot u \in P_\alpha)\}$. Wie eben folgt dann bereits $u \in P_\alpha$. □

Folgerung:
Sei h ein Polynom in S, G eine Gröbnerbasis von I' in S' und $NF(h, G) = 0$, d.h. $h \in I'$. Dann gilt

$$h \in c(I') = \cap\{P_\alpha \ :\ P_\alpha \cap U = \emptyset\},$$

d.h. das Polynom verschwindet auf allen generischen Komponenten von $Z(I)$.

Wir sagen in diesem Fall, daß der geometrische Satz bzgl. der unabhängigen Variablenmenge $\mathbf{u}$ *generisch richtig ist*, was folgendes heißt: Der Satz $h = 0$ ist höchstens auf speziellen Komponenten von $Z(I)$, auf denen aber die Variablen $\mathbf{u}$ nicht mehr unabhängig sind, falsch. Jede solche Komponente enthält aber im definierenden Ideal ein Polynom $g_i(\mathbf{u})$. Das Produkt dieser Polynome können wir dann als Nichtdegenerationsbedingung nehmen. Ein geometrischer Satz ist also bzgl. $\mathbf{u}$ genau dann generisch richtig, wenn es eine Nichtdegenerationsbedingung $g(\mathbf{u}) \in k[\mathbf{u}]$ gibt, so daß

$$\{B,\ g(\mathbf{u}) \neq 0 \implies h = 0\}$$

gilt. Der Satz ist also für jede "genügend allgemeine" Belegung der unabhängigen Parameter richtig.
Generell, wenn $NF(h, G)$ nicht verschwindet, wie oben im Beispiel "Miguelscher Punkt", liefern uns Untersuchungen in S' Aussagen, die das Verhalten auf speziellen Komponenten ausblenden. In diesem Beispiel hat $Z(I)$ zwei generische Komponenten. Eine entspricht dem Schnittpunkt F der Kreise durch A, F, E und B, F, D, die andere dem gesuchten Schnittpunkt X. Auf der ersten Komponente gilt der Satz nicht, auf der zweiten sehr wohl. Der Gröbnerfaktorisierer zeigt, daß $Z(I)$ daneben noch wenigstens 5 weitere spezielle Komponenten hat, die die Bedingungen $u_2 = 0, u_5 = 0, u_3 = 1, u_5 = 1$ und $u_3 = u_5 = 1$ enthalten, also degenerierten Lagen entsprechen, wo z.B. zwei der drei Punkte, die einen Kreis bestimmen sollen, zusammenfallen. In einem solchen Fall ist aber der Kreis und damit auch der Schnittpunkt X nicht mehr eindeutig bestimmt, so daß wir auch nicht prüfen können, ob er auf dem dritten Kreis liegt.

Zur Bestimmung von g:
Obiger Weg über die Berechnung einer Primzerlegung ist zu aufwendig, um eine Nichtdegenerationsbedingung zu finden. Es stellt sich allerdings heraus, daß man g bereits aus einer Gröbnerbasis von B bzgl. einer speziell gewählten Termordnung ablesen kann.

Satz:
Sei $<$ eine Termordnung auf $T(\mathbf{u}, \mathbf{x})$ mit $\mathbf{u} \ll \mathbf{x}$ und $B \subset S$ eine (polynomiale) Basis von I.
Sei G eine Gröbnerbasis von I bzgl. $<$. Dann ist G auch eine Gröbnerbasis von $I' = I \cdot S'$ bzgl. der induzierten Termordnung auf $T(\mathbf{x}) \subset T(\mathbf{u}, \mathbf{x})$.

Beweis:
Für $f \in S$ ist $lt(f)$ ein Term in $\mathbf{x}$ und $\mathbf{u}$, läßt sich also eindeutig in seine Komponenten $lt(f) = lt_x(f)\, lt_u(f)$ in $T(\mathbf{x})$ und $T(\mathbf{u})$ zerlegen. Für die Gröbnerbasis G gilt

$$\forall\, f \in I\ \exists\, g \in G\ (lt(g) \,|\, lt(f)).$$

Letzteres bedeutet insbesondere $lt_x(g) \,|\, lt_x(f)$ und $lt_u(g) \,|\, lt_u(f)$. Ist nun $u = \frac{f}{n} \in I'$ mit $f \in I,\ n \in k[\mathbf{u}]$, so gilt $lt_x(u) = lt_x(f)$ und folglich auch $lt_x(g) \,|\, lt_x(u)$ in S'. □

Obwohl G eine Gröbnerbasis von I' ist, muß es keine minimale reduzierte Gröbnerbasis sein. Berechnen wir etwa für die Polynome

$$\begin{aligned}\{&x_1 \cdot (u_2 + u_3 - 1) - u_1 \cdot u_3 + u_1 - u_2 \cdot u_3,\\ &x_2 \cdot (u_1 \cdot u_4 - u_3) + u_4 \cdot (u_1 \cdot u_3 - u_1 + u_2 \cdot u_3),\\ &x_3 \cdot (-u_2 + 1) + x_4 \cdot u_1 - u_1,\\ &x_3 \cdot u_2 \cdot u_4 + x_4 \cdot (-u_1 \cdot u_4 + 1) - u_2 \cdot u_4\},\end{aligned}$$

die die Voraussetzungen des Satzes von Pappus ausdrücken, eine minimale Gröbnerbasis in S, so erhalten wir als Leitterme

$$\begin{aligned}\{&x_3 \cdot u_4,\, x_3 \cdot u_2,\, x_2 \cdot u_1 \cdot u_4,\, x_4 \cdot u_1 \cdot u_4,\, x_1 \cdot u_2,\, x_2 \cdot x_3 \cdot u_3,\, x_1 \cdot x_3 \cdot u_3,\, x_2 \cdot x_4 \cdot u_2,\\ &x_1 \cdot x_2 \cdot u_1 \cdot u_3,\, x_1 \cdot x_2 \cdot u_3^2 \cdot u_4,\, x_1 \cdot x_2 \cdot x_3 \cdot u_1\} \subset T(\mathbf{u}, \mathbf{x}).\end{aligned}$$

In S' haben die entsprechenden Polynome die Gestalt

$$\begin{aligned}G = \{&x_3\, p_1(\mathbf{u}) + \ldots\,,\, x_3\, p_2(\mathbf{u}) + \ldots\,,\, x_2\, p_3(\mathbf{u}) + \ldots\,,\\ &x_4\, p_4(\mathbf{u}) + \ldots\,,\, x_1\, p_5(\mathbf{u}) + \ldots\,,\, x_2\, x_3\, p_6(\mathbf{u}) + \ldots\,,\\ &x_1\, x_3\, p_7(\mathbf{u}) + \ldots\,,\, x_2\, x_4\, p_8(\mathbf{u}) + \ldots\,,\, x_1\, x_2\, p_9(\mathbf{u}) + \ldots\,,\\ &x_1\, x_2\, p_{10}(\mathbf{u}) + \ldots\,,\, x_1\, x_2\, x_3\, p_{11}(\mathbf{u}) + \ldots\end{aligned}$$

In dieser Basis sind eine Reihe von Polynomen noch überflüssig.

Wir wissen, daß man aus einer Gröbnerbasis eine minimale auswählen kann, indem man einfach die Elemente streicht, die nicht zu einer Minimalbasis des Leittermideal (in $T(\mathbf{x})$) gehören. In obigem Beispiel wäre also

$$\begin{aligned}G' = \{&x_3 \cdot u_4 + x_4 - u_4 \cdot (u_1 + u_2),\\ &x_2 \cdot (u_1 \cdot u_4 - u_3) + u_4 \cdot (u_1 \cdot u_3 - u_1 + u_2 \cdot u_3),\\ &x_4 \cdot (u_1 \cdot u_4 + u_2 - 1) + u_2 \cdot u_4 \cdot (-u_1 - u_2 + 1),\\ &x_1 \cdot (u_2 + u_3 - 1) - u_1 \cdot u_3 + u_1 - u_2 \cdot u_3\}\end{aligned}$$

eine minimale Gröbnerbasis von $I' = I \cdot S'$.

Satz: Sei $G' \subset G$ eine wie oben beschrieben konstruierte minimale Gröbnerbasis von I'. und $g(\mathbf{u}) \in k[\mathbf{u}]$ ein gemeinsames Vielfaches der $\{lc_x(g) \ : \ g \in G'\}$. Dann gilt

$$c(I') = I' \cap S = I :< g >,$$

d.h. g ist eine Nichtdegenerationsbedingung, die alle speziellen Komponenten von $Z(I)$ ausschließt.

Beweis: Sei $f \in I' \cap S$. Dann ist $NF(f, G') = 0$ in S', d.h. eine entsprechende Pseudonormalform von f liefert auch in S den Wert Null. Sei

$$f = f_1 \longrightarrow_{g_{i_1}} f_2 \longrightarrow_{g_{i_2}} \ldots \longrightarrow 0$$

mit $g_{i_k} \in G'$ die entsprechende Reduktionskette. In jedem Schritt wird dabei die Reduktion

$$f_k \longrightarrow_{g_{i_k}} f_{k+1} := lc_x(g_{i_k}) \cdot f_k - lc_x(f_k) \cdot g_{i_k} \cdot m$$

ausgeführt. Also ist (in S !)

$$f_{k+1} \equiv lc_x(g_{i_k}) \cdot f_k \ (mod\ I(G'))$$

und schließlich

$$0 \equiv lc_x(g_{i_1}) \cdot \ldots \cdot lc_x(g_{i_m}) \cdot f \ (mod\ I(G')).$$

Also ist $g^m \cdot f \in I(G') \subseteq I$ und damit $I :< g > \supseteq I' \cap S$. Die umgekehrte Inklusion ist offensichtlich.

In unserem Beispiel oben ist also

$$g := u_4 \cdot (u_1 \cdot u_4 - u_3) \cdot (u_1 \cdot u_4 + u_2 - 1) \cdot (u_2 + u_3 - 1)$$

eine Nichtdegenerationsbedingung, die die speziellen Komponenten von $Z(I)$ wegschneidet. Das ist in der Tat richtig, denn die entsprechende Zerlegung in Primkomponenten zeigt, daß $Z(I)$ aus 4 Komponenten besteht. Neben der generischen Komponente sind das die drei speziellen Komponenten

$$\begin{array}{l} \{u_3,\, u_1,\, u_2 - 1,\, x_3 \cdot u_4 + x_4 - u_4\}, \\ \{u_4 - 1,\, u_1 - u_3,\, u_2 + u_3 - 1,\, x_3 + x_4 - 1\}, \\ \{u_2,\, u_3 - 1,\, u_1 \cdot u_4 - 1,\, x_3 + x_4 \cdot u_1 - u_1\}, \end{array}$$

die jeweils dem Zusammenfallen der Punkte $C = D$, $D = E$ und $A = F$ entsprechen. In jedem der drei Fälle ist aber wenigstens einer der Schnittpunkte X, Y, Z nicht mehr eindeutig definiert, also die Aussage des geometrischen Satzes gegenstandslos.

Wir wollen diesen Abschnitt abschließen, indem wir generische Beweise weiterer Sätze der Elementargeometrie geben.

Beispiel: Satz vom Pascal-Typ

```
A:={0,0};
B:={1,0};
C:={u2,u3};
D:={u4,u5};
E:={u6,x1};
F:={0,1};

P:={x2,0}; % point_on_line(P,line(A,B)),
Q:={x3,x4};
R:={0,x5}; % point_on_line(R,line(F,A)),

S:={x6,x7};
T:={x8,x9};
U:={0,x10}; % point_on_line(U,line(A,F)),

polys:={point_on_line(P,line(D,E)), point_on_line(Q,line(B,C)),
point_on_line(Q,line(E,F)), point_on_line(R,line(C,D)),
point_on_line(T,line(C,D)), point_on_line(U,line(B,C)),
point_on_line(S,line(B,E)), point_on_line(S,line(A,D)),
point_on_line(T,line(E,F)),
collinear(P,Q,R)};

con:= collinear(S,T,U);
```

x_1 ist in obiger Konstellation als abhängiger Parameter zu wählen, weil ja die Bedingung $collinear(P, Q, R)$, die nach dem Satz von Pascal äquivalent dazu ist, daß sich die sechs Punkte A, B, C, D, E, F auf einer Quadrik befinden, für die Koordinaten dieser Punkte eine algebraische Abhängigkeitsrelation definiert. Ohne diese "geometrische Einsicht" könnten wir etwa mit den oben beschriebenen Mitteln prüfen, daß die (variablen) Koordinaten der sechs Punkte in der Tat nicht unabhängig $mod\ I(polys)$ sind.

Wir erhalten das Gleichungssystem

$$\begin{aligned}\{&x_2 \cdot (-u_5 + x_1) - u_4 \cdot x_1 + u_5 \cdot u_6,\\
&x_3 \cdot u_3 + x_4 \cdot (-u_2 + 1) - u_3,\\
&x_3 \cdot (-x_1 + 1) + x_4 \cdot u_6 - u_6,\\
&x_5 \cdot (u_2 - u_4) - u_2 \cdot u_5 + u_3 \cdot u_4,\\
&x_8 \cdot (-u_3 + u_5) + x_9 \cdot (u_2 - u_4) - u_2 \cdot u_5 + u_3 \cdot u_4,\\
&x_{10} \cdot (-u_2 + 1) - u_3,\\
&x_6 \cdot x_1 + x_7 \cdot (-u_6 + 1) - x_1,\\
&x_6 \cdot u_5 - x_7 \cdot u_4,\\
&x_8 \cdot (-x_1 + 1) + x_9 \cdot u_6 - u_6,\\
&x_2 \cdot x_4 - x_2 \cdot x_5 + x_3 \cdot x_5\},\end{aligned}$$

von dem wir eine Gröbnerbasis bzgl. der Variablenordnung $\{x_{10}, x_9, x_8, x_7, x_6, x_5, x_4, x_3, x_2, x_1\}$ berechnen wollen. Als Ergebnis erhalten wir rationale Ausdrücke in $\mathbf{u}$ für $x_{2\ldots 10}$ und einen Ausdruck der Form

$$p_1(\mathbf{u})x_1^2 + p_2(\mathbf{u})x_1 + p_3(\mathbf{u})$$

für x_1. Da $con \in I(polys)$, folgt die genrische Richtigkeit dieses Satzes.

Aufgabe: Führen Sie die entsprechenden Rechnungen aus.

Aufgabe: Zeigen Sie, daß man bei geschickter Wahl der Koordinaten die Gleichungen dieses Theorems auf ein lineares Gleichungssystem in $\mathbf{x}$ zurückführen kann. (Hinweis: Untersuchen Sie die Koordinaten $A = (u_1, u_2)$, $B = (1, 0)$, $C = (0, 0)$, $D = (0, x_9)$, $E = (u3_, u_4)$, $F = (u_5, u_6)$, $P = (x_1, x_2)$, $Q = (x_3, 0)$, $R = (0, x_4)$, $S = (x_5, x_6)$, $T = (0, x_7)$, $U = (x_8, 0)$).

Beispiel: Der Feuerbachsche Kreis berührt den Inkreis des Dreiecks und die drei Ankreise.

```
M:={0,u1}; % the center of (one of) the inscribed circle(s)
% Hence {0,0} is the pedal point and u1 the radius of
% the inscribed circle.


A:={u2,0}; B:={u3,0}; C:={x1,x2};

MA:=midpoint(B,C); MB:=midpoint(A,C); MC:=midpoint(A,B);

N:={x3,x4}; % the center of Feuerbach's circle

% x5 = |N.MA| = radius of Feuerbach's circle

polys:={point_on_bisector(M,C,A,B),
point_on_bisector(M,A,B,C),
num(sqrdist(N,MA)-x5^2),
num(sqrdist(N,MB)-x5^2),
num(sqrdist(N,MC)-x5^2)};
```

Wir erhalten das folgende Gleichungssystem:

$$\begin{aligned}\{&x_2 \cdot (u_1^2 - u_2^2) - 2 \cdot x_1 \cdot u_1 \cdot u_2 + 2 \cdot u_1 \cdot u_2^2,\\
&x_2 \cdot (u_1^2 - u_3^2) - 2 \cdot x_1 \cdot u_1 \cdot u_3 + 2 \cdot u_1 \cdot u_3^2,\\
&x_2^2 - 4 \cdot x_2 \cdot x_4 + 4 \cdot x_3^2 - 4 \cdot x_3 \cdot x_1 - 4 \cdot x_3 \cdot u_3 + 4 \cdot x_4^2 - 4 \cdot x_5^2 + x_1^2 + 2 \cdot x_1 \cdot u_3 + u_3^2,\\
&x_2^2 - 4 \cdot x_2 \cdot x_4 + 4 \cdot x_3^2 - 4 \cdot x_3 \cdot x_1 - 4 \cdot x_3 \cdot u_2 + 4 \cdot x_4^2 - 4 \cdot x_5^2 + x_1^2 + 2 \cdot x_1 \cdot u_2 + u_2^2,\\
&4 \cdot x_3^2 - 4 \cdot x_3 \cdot (u_2 + u_3) + 4 \cdot x_4^2 - 4 \cdot x_5^2 + u_2^2 + 2 \cdot u_2 \cdot u_3 + u_3^2\},\end{aligned}$$

dessen Gröbnerbasis einen rein quadratischen Term in x_5 und lineare Ausdrücke für $x_{1...4}$ liefert. Die Behauptung, daß der Feuerbachkreis und der Inkreis sich berühren, kann man auf folgende Aussage für Kreise zurückführen:

Lemma: Zwei Kreise berühren sich genau dann, wenn der Abstand zwischen ihren Mittelpunkten gleich der Differenz der Radien ist.

Beweis: Nimm Schnittpunkt X dieser beiden Kreise und betrachte das Dreieck XMN.

Algebraische Ausführung:

```
> con1:=sqrdist(N,M)-(x5-u1)^2;
```

führt leider nicht zum Erfolg, weil wir in obigem Lemma automatisch angenommen haben, daß sich die Kreise von innen berühren. Berühren sie sich von außen, dann ist die Differenz der radien durch deren Summe zu ersetzen. Beide Bedingungen kann man in eine Gleichung durch fortgesetztes Quadrieren integrieren:

```
> con2:=(sqrdist(N,M)-x5^2-u1^2)^2-4*x5^2*u1^2;
```

Dies reduziert tatsächlich zu Null.

Die Varietät $Z(I)$ zerfällt in diesem Fall in zwei Teile, weil sich das quadratische Polynom in x_5 in zwei Linearfaktoren

$$8 \cdot x_5 \cdot u_1 \cdot (u_1^2 + u_2 \cdot u_3) - u_1^4 + u_1^2 \cdot u_2^2 + u_1^2 \cdot u_3^2 + u_2^2 \cdot u_3^2 \text{ und}$$
$$8 \cdot x_5 \cdot u_1 \cdot (u_1^2 + u_2 \cdot u_3) + u_1^4 + u_1^2 \cdot u_2^2 + u_1^2 \cdot u_3^2 + u_2^2 \cdot u_3^2$$

zerlegen läßt. Der eine Zweig entspricht äußerer Berührung zwischen Feuerbachkreis und In/An-Kreis, der andere innerer Berührung. Davon überzeugt man sich leicht, indem man con_1 bzgl. des entsprechenden Zweiges reduziert.

Aufgaben: Beweisen Sie die folgenden Geometrietheoreme durch Zurückführung auf Sätze vom konstruktiven Typ oder vom Gleichungstyp. Versuchen Sie, ob sie auch elementargeometrische Beweise finden können.

1) $ABCD$ sei ein Quadrat, E so gewählt, daß der Punkt auf der Parallelen zu BD durch C liegt und $l(BD) = l(BE)$ für die Längen der entsprechenden Strecken gilt. F sei der Schnittpunkt von BE und CD. Zeigen Sie, daß dann $l(DE) = l(DF)$ gilt.

2) Beweisen Sie den Satz vom Höhenfußpunktdreieck: Ist $\Delta\,ABC$ ein Dreieck mit den Höhenfußpunkten D, E, F, so wird der Winkel $\angle\,DEF$ von der Höhe durch E halbiert.

Finden Sie auch die entsprechenden Nicht-Degenerations-Bedingungen.

3) Zeigen Sie weiter, daß die 6 Fußpunkte der Lote von den Höhenfußpunkten D, E, F auf die gegenüberliegenden Dreiecksseiten (oder deren Verlängerungen) auf einem gemeinsamen Kreis, dem *Taylorkreis*, liegen.

4) Seien A_1, A_2, A_3 und B_1, B_2, B_3 jeweils kollinear. Der Satz von Pappus trifft eine Aussage über die Kollinearität von drei Schnittpunkten, d.h. durch sie wird eine Gerade g bestimmt. Nennen wir diese Gerade *Pappus-Gerade* der Konfiguration. Permutation der Punkte B_1, B_2, B_3 führt zu insgesamt 6 solchen Geraden (Permutationen der Punkte auf der anderen Geraden haben keinen Einfluß: Ist (σ, τ) ein Paar von Permutationen der Punkte (A) und (B), so liefert die Permutation $(1, \sigma^{-1}\tau)$ dieselbe Pappus-Gerade). Zeigen Sie, daß je drei dieser Geraden durch einen gemeinsamen Punkt gehen.

5) Beweisen Sie die Umkehrung des Satzes von der Simsonschen Geraden: Sind die Lotfußpunkte R, S, T von einem Punkt P auf die Seiten des Dreiecks $\Delta\,ABC$ oder deren Verlängerungen kollinear, so liegt P auf dem Umkreis des Dreiecks.

6) Beweisen Sie auch folgende Verallgemeinerung:
Ist M der Umkreismittelpunkt des Dreiecks $\Delta\,ABC$ und P, R, S, T wie eben, so hängt der Flächeninhalt $F(\Delta\,RST)$ nur von $l(MP)$ ab. Finden Sie eine genaue Formel für diesen Flächeninhalt.

7) Beweisen Sie das Schmetterlingstheorem: Seien A, B, C, D vier Punkte auf einem Kreis mit Zentrum in M, P der Schnittpunkt der Geraden AC und BD und F bzw. G der Schnittpunkt des Lots in P auf MP mit AB bzw. CD. Dann gilt $l(PF) = l(PG)$.

8) Beweisen Sie die Flächeninhaltsformel

$$F(\Delta\, ABC) = \frac{a\, b\, c}{4\, R},$$

wobei a, b, c die Seitenlängen und R der Umkreisradius ist.

9) Beweisen Sie die Flächeninhaltsformel

$$F(\Delta\, ABC) = \rho \cdot \frac{a+b+c}{2},$$

wobei a, b, c die Seitenlängen und ρ der Inkreisradius ist.

10) Gegeben sei ein Kreis k, die Tangente von B an diesen Kreis, A der Berührungspunkt, M der Mittelpunkt von AB und D ein Punkt auf dem Kreis k. C sei der Schnittpunkt von DM mit k, E der Schnittpunkt von BD mit k und F der Schnittpunkt von BC mit k. Zeigen Sie, daß EF parallel zu AB ist.

4.4 Triangulare Systeme

Im letzten Kapitel hatten wir gesehen, daß wir in Geometrietheoremen statt der expliziten Angabe von Nichtdegenerationsbedingungen oft auf natürliche Weise einen Satz unabhängiger Koordinaten $\mathbf{u}$ fixieren können, von dem die verbleibenden Koordinaten $\mathbf{x}$ algebraisch abhängen. Setzen wir $K = k(\mathbf{u})$, so haben wir gesehen, daß das Erweiterungsideal $I' = I(B) \cdot S'$ in $S' = K[\mathbf{x}]$ die adäquate algebraische Struktur ist, in der wir eine durch Gleichungen $B \subset S = k[\mathbf{u}, \mathbf{x}]$ beschriebene geometrische Situation außerhalb spezieller Komponenten untersuchen können. Das Erweiterungsideal ist dabei ein nulldimensionales Ideal über K, hat also nur endlich viele Lösungen im entsprechenden algebraischen Abschluß.

In allen bisher betrachteten Fällen bestand die entsprechende Gröbnerbasis aus genau so vielen Gleichungen wie die Anzahl abhängiger Variablen betrug, wobei man diese Gleichungen so anordnen konnte, daß sich mit jeder neuen Gleichung die verschiedenen Lösungszweige einer weiteren der abhängigen Variablen ermitteln ließen. Um diese Beobachtung genauer zu fassen, fixieren wir eine Ordnung $x_1 > \ldots > x_n$ auf den abhängigen Variablen. Das transformierte Gleichungssystem hatte dann stets die folgende spezielle Gestalt

$$\begin{array}{lcl} f_1(x_1, \ldots, x_n) & = & 0 \\ f_2(x_2, \ldots, x_n) & = & 0 \\ \ldots\ldots\ldots\ldots\ldots & & \\ f_{n-1}(x_{n-1}, x_n) & = & 0 \\ f_n(x_n) & = & 0, \end{array}$$

wobei $f_k = f_k(x_k, \ldots, x_n)$, als Polynom im Ring $K[x_{k+1}, \ldots, x_n][x_k]$ betrachtet, einen Leitkoeffizienten hat, der frei von $(x_{k+1}, \ldots, x_n)$ und damit in K invertierbar ist.

Definition: Eine solche Menge von Polynomen $B := \{f_1, \ldots, f_n\}$ nennen wir ein *triangulares System.*

Dies ist eine natürliche Verallgemeinerung der Dreiecksgestalt linearer Gleichungssysteme. Die zugehörige Nullstellenmenge $Z(I(B))$ kann nämlich wie folgt gewonnen werden: Finde die Nullstellen $a_n^{(i)} \in \bar{K}$ des Polynoms $f_n(x_n) = 0$ und setze diese in $f_{n-1}(x_{n-1}, x_n) = 0$ ein. Da der Leitterm von f_{n-1} nicht von x_n abhängt, kann beim Einsetzen

$$f_{n-1}(x_{n-1}, a_n^{(i)}) \in K(a_n^{(i)})[x_{n-1}]$$

nicht verschwinden, ja nicht einmal den Grad ändern. Finde die Nullstellen $a_{n-1}^{(i)} \in \bar{K}$ dieses Polynoms, setze sie in f_{n-2} ein und löse die Gleichung

$$0 = f_{n-2}(x_{n-2}, a_{n-1}^{(i)}, a_n^{(i)}) \in K(a_{n-1}^{(i)}, a_n^{(i)})[x_{n-2}]$$

und so weiter. Die Anzahl der Lösungen ist also unter Beachtung der entsprechenden Multiplizitäten stets gleich $L := \prod_k deg_{x_k}\ f_k$.

Betrachten wir das Ideal $I = I(B)$, so ist S/I ein endlichdimensionaler K-Vektorraum mit der Basis $\{x_i^{k_i},\ i = 1,\ldots,n,\ k_i < deg_{x_i}\ f_i\}$. Seine Dimension stimmt also mit L überein.

Einzelne Lösungen $(a_1^{(i)},\ldots,a_n^{(i)})$ leben in einer algebraischen Erweiterung $K(a_1^{(i)},\ldots,a_n^{(i)})$ des Grundkörpers K, die sich als Körperturm

$$K(a_1^{(i)},\ldots,a_n^{(i)}) \supset K(a_2^{(i)},\ldots,a_n^{(i)}) \supset K(a_{n-1}^{(i)},a_n^{(i)}) \supset K(a_n^{(i)}) \supset K$$

durch sukzessive Hinzunahme neuer algebraischer Zahlen darstellen läßt. Ist f_n nicht irreduzibel, so ist es auch nicht das Minimalpolynom von $a_n^{(i)}$, so daß sich der Körperturm bereits an dieser Stelle verzweigt. Dies kann man vermeiden, wenn man bereits im System B alle Elemente in Faktoren zerlegt und die Nullstellenmenge entsprechend aufspaltet.

Genauso können auch für $k < n$ Verzweigungen des Körperturms auftreten, wenn

$$f_k(x_k, a_{k+1}^{(i)},\ldots,a_n^{(i)}) \in K(a_{k+1}^{(i)})[x_k]$$

reduzibel ist. Dies kann selbst dann auftreten, wenn $f_k(x_k,\ldots,x_n)$ irreduzibel als Polynom in $K[x_k,\ldots,x_n]$ ist, wie das folgende Beispiel zeigt:

$$f_1 = x_1^2 - 6,\ f_2 = x_2^2 - 2,\ f_3 = x_3^2 - 3.$$

Es gibt vier mögliche Lösungen $(a_2^{(i)},a_3^{(i)}) = (\pm\sqrt{2},\pm\sqrt{3})$ für (x_2,x_3), deren Koordinaten alle in der Körpererweiterung $K = \mathbf{Q}(\sqrt{2},\sqrt{3})$ von $\mathbf{Q}$ vom Grad 4 liegen. Das Polynom $x_1^2 - 6$, das über $\mathbf{Q}$ irreduzibel ist, läßt sich aber über K in die Linearfaktoren $(x_1 + \sqrt{2}\sqrt{3})(x_1 - \sqrt{2}\sqrt{3})$ zerlegen. Deshalb bekommen wir zu jeder der vier Lösungen zwei Zweige $a_1 = a_2\,a_3$ und $a_1 = -a_2\,a_3$. Dies entspricht der schon früher betrachteten Zerlegung des Ideals $I(f_1,f_2,f_3)$ in Primkomponenten.

Im allgemeinen Fall gilt der folgende Satz, der eine weitere Verallgemeinerung des Chinesischen Restklassensatzes darstellt:

Satz: Sei $I \subset K[\mathbf{x}]$ ein nulldimensionales Radikalideal und $I = \cap P_\alpha$ dessen Zerlegung in Primkomponenten. Dann sind die Faktoren S/P_α endliche Körpererweiterungen von K und die natürliche Abbildung

$$S/I \longrightarrow \oplus S/P_\alpha$$

ein Isomorphismus. Insbesondere sind die Dimensionen als K-Vektorräume beider Seiten gleich.

Beweis: Betrachten wir den natürlichen Ringhomomorphismus $\phi : S \longrightarrow \oplus S/P_\alpha$ und zeigen zuerst, daß er surjektiv ist.

Als nulldimensionale Ideale sind alle P_α nicht nur prim, sondern sogar (paarweise verschiedene) maximale Ideale. Für jedes Paar α,β ist deshalb $P_\alpha + P_\beta = (1)$. Damit gibt es Elemente $p_{\alpha\beta} \in P_\alpha, p_{\beta\alpha} \in P_\beta$, so daß $p_{\alpha\beta} + p_{\beta\alpha} = 1$ gilt. Betrachten wir nun das Produkt

$$1 = \prod_{\beta\,|,\beta\neq\alpha} (p_{\alpha\beta} + p_{\beta\alpha})$$

und multiplizieren es aus, so ist ein Summand

$$p_\alpha := \prod_{\beta\,|,\beta\neq\alpha} p_{\beta\alpha} \in \bigcap_{\beta\,|,\beta\neq\alpha} P_\beta,$$

während die anderen Summanden alle in P_α enthalten sind. Es gilt also

$$p_\alpha \equiv \begin{cases} 1\ (mod\ P_\alpha) & \\ 0\ (mod\ P_\beta) & \text{für } \beta \neq \alpha. \end{cases}$$

Für vorgegebene (u_α) aus S ist also

$$u := \sum_\alpha u_\alpha p_\alpha \equiv u_\alpha \ (mod\ P_\alpha)$$

für alle α, d.h. $(u_\alpha) = \phi(u)$.

Weiter ist $ker\ \phi = \cap P_\alpha = I$, was die Aussage des Satzes beweist.

Die Zerlegung in Primkomponenten entspricht also auch hier der Zerlegung in verschiedene Zweige der Berechnung der Lösungsmenge. Wir sehen zugleich, daß die Summe der Grade der Körpererweiterungen $dim_K\ S/P_\alpha$ mit L zusammenfällt.

Es stellt sich allerdings heraus, daß längst nicht jedes nulldimensionale Ideal ein triangulares System als Basis hat.

Beispiel: $B = \{x^2+y+z-3,\ x+y^2+z-3,\ x+y+z^2-3\}$
Die Gröbnerbasis dieses Ideals hat die Elemente

$$\begin{array}{l} \{x+y+z^2-3, \\ y^2-y-z^2+z, \\ 2\cdot y\cdot z^2-4\cdot y+z^4-5\cdot z^2+6, \\ z^6-10\cdot z^4+4\cdot z^3+19\cdot z^2-8\cdot z-6\} \end{array}$$

Da bzgl. der Gradordnung genau die Terme x^2, y^2, z^2 modulo I ersetzt werden können, sehen wir, daß $L := dim_K\ S/I = 8$ gilt. Es ist also unklar, woher hier ein Polynom vom Grad 6 kommt.

Generell wissen wir von nulldimensionalen Idealen das folgende:

Satz: $I \subset S$ ist ein nulldimensionales Ideal, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

1. S/I ist ein endlich-dimensionaler K-Vektorraum.
2. Eine / jede Gröbnerbasis von I enthält Polynome $p_i,\ i=1,\ldots,n$, deren Leitterme jeweils reine Potenzen in x_i sind.
3. I enthält Polynome $q_i(x_i),\ i=1,\ldots,n$, die jeweils nur von x_i abhängen.

Aufgabe: Nehmen wir an, die $q_i(x_i)$ sind so gewählt, daß sie kleinstmöglichen Grad haben. Zeigen Sie, daß I genau dann ein Radikalideal ist, wenn die q_i quadratfreie Polynome sind, d.h. jede Nullstelle nur mit der Vielfachheit 1 auftritt. (Das ist äquivalent zu $gcd(q_i, q_i') = 1$)

Es stellt sich allerdings heraus, daß wenigstens Primideale stets Gröbnerbasen haben, die triangulare Systeme sind:

Satz:
Ist $P \subset S$ ein nulldimensionales Primideal (also zuglich ein maximales Ideal in S), so ist eine minimale reduzierte Gröbnerbasis von P bzgl. einer lexikographischen Termordnung triangular.

Beweis: Wir können uns auf die Untersuchung des Falls beschränken, daß $p(\mathbf{x}) := q(x_2,\ldots,x_n)\cdot x_1^k + \ \ldots$ in einer minimalen reduzierten Gröbnerbasis enthalten ist. Dann ist insbesondere $q \notin P$ und folglich $(q)+P = (1)$. Es gibt also ein Polynom $a(\mathbf{x})$ mit der Eigenschaft $a\cdot q \equiv 1\ (mod\ P)$, damit ist für $deg(q) > 0$ aber auch $NF(a\cdot p, P) = x_1^k + \ \ldots\ \in P$, was der Minimalität der Gröbnerbasis widerspricht. $\square$

Damit ist jede Primkomponentenzerlegung von I zugleich eine Zerlegung in Komponenten, die sich durch triangulare Systeme darstellen lassen. Untersuchen wir nun, ob eine Zerlegung eines nulldimensionalen Systems B in triangulare Teilsysteme B_α mit der Eigenschaft $Z(B) = \cup Z(B_\alpha)$ auch mit geringerem Aufwand möglich ist. Eine solche Zerlegung nennen wir eine *Triangulierung* von B.

4.5 Berechnung einer Triangulierung durch charakteristische Mengen

Die folgende Idee geht auf Ritt und Wu zurück. Betrachten wir sie zuerst wieder an einem Beispiel. Sei

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

Interreduktion bzgl. der Variablenordnung $x > y > z$ liefert

$$\{f_1 = x + y + z^2 - 3,\ f_2 = y^2 - y + z \cdot (-z + 1),\ f_3 = 2 \cdot y \cdot (z^2 - 2) + z^4 - 5 \cdot z^2 + 6\}$$

Die letzten beiden Gleichungen enthalten als Hauptvariable beide y. Ist $z^2 - 2 \neq 0$, so kann man die zweite Gleichung durch ihren Pseudorest

$$f_4 := prem(f_2, f_3, y) = z^8 - 12 \cdot z^6 + 4 \cdot z^5 + 39 \cdot z^4 - 16 \cdot z^3 - 44 \cdot z^2 + 16 \cdot z + 12$$

bzgl. der dritten ersetzen. Ist $z^2 - 2 = 0$, so verschwindet das dritte Polynom. In beiden Fällen erhalten wir triangulare Systeme

$$\begin{array}{l}\{x + y + z^2 - 3,\\ 2 \cdot y \cdot (z^2 - 2) + z^4 - 5 \cdot z^2 + 6,\\ z^8 - 12 \cdot z^6 + 4 \cdot z^5 + 39 \cdot z^4 - 16 \cdot z^3 - 44 \cdot z^2 + 16 \cdot z + 12\}\end{array}$$

und

$$\{x + y + z^2 - 3,\ y^2 - y + z \cdot (-z + 1),\ z^2 - 2\},$$

wobei beim ersten System noch zu berücksichtigen ist, daß $z^2 \neq 2$ vorausgesetzt wurde. Damit fallen vier Lösungen der letzten Gleichung zur Bestimmung von z weg und das System kann ersetzt werden durch

$$\{x + y + z^2 - 3,\ 2 \cdot y + z^2 - 3,\ z^4 - 8 \cdot z^2 + 4 \cdot z + 3\}.$$

Jeder der beiden Zweige steuert also 4 Lösungen zur Lösungsmenge $Z(B)$ bei.

Wir sehen zunächst, daß die bei diesem Verfahren entstehenden Systeme für die Berechnung der einzelnen Lösungszweige zwar prinzipiell geeignet sind, aber nicht die starke Eigenschaft triangularer Systeme besitzen, was den Leitkoeffizienten betrifft.

Wir bezeichnen ein System von Polynomen (oder eine Teilmenge davon)

$$B := \{f_1(x_1, \ldots, x_n),\ f_2(x_2, \ldots, x_n),\ \ldots,\ f_{n-1}(x_{n-1}, x_n),\ f_n(x_n)\}$$

als *System in Dreiecksform.* $in(f, x_i)$ bezeichne weiter den Leitkoeffizienten des Polynoms $f \in R := k[x_1, \ldots, x_n]$ betrachtet als Polynom in x_i mit Koeffizienten in den restlichen Variablen. Ist insbesondere $l_i := in(f_i, x_i)$ für $f_i \in B$, so kann man durch fortgesetzte Pseudodivision zu jedem Polynom $f \in R$ eine Normalform bzgl. B definieren.

Für nicht konstante Polynome $f, g \in R$ definieren wir deshalb die *Klasse* $mvar(f)$ als diejenige Variable x_i, für die $f \in k[x_i, \ldots, x_n]$ und $deg(f, x_i) > 0$ gilt. Dann berechnet

```
prem(f,g) ==
      x:=mvar(g);
      while (d := deg(f,x) - deg(g,x)) ≥ 0 do
            f := lc(g,x) · f - lc(f,x) · g · x^d
      return f;
```

den *Pseudorest* von f bei Division durch g und für obiges System B in Dreiecksform

```
PNF(f,B) ==
      for i:=1 to n do f := prem(f, f_i)
      return f;
```

eine *Pseudo-Normalform*, in der das Ergebnis f' entweder verschwindet oder $deg(f', x_i) < deg(f_i, x_i)$ für alle i gilt. Ist insbesondere $PNF(f, B) = 0$, so verschwindet f auf der relativen Nullstellenmenge

$$Z(B, l) = Z(B) \setminus Z(\{l\}), \quad l := l_1 \cdot \ldots \cdot l_n.$$

Schließlich heißt f *reduziert* bzgl. B, wenn es mit seiner Pseudo-Normalform übereinstimmt.

Def.: Ein System $B = (f_1, \ldots, f_r)$ (mglw. mit $r < n$) in Dreiecksform heißt *schwach triangular*, wenn f_i bzgl. $(f_{i+1}, \ldots, f_n)$ reduziert ist. $(d_1, \ldots, d_n)$ mit

$$d_i = \begin{cases} deg(f, x_i) & \text{wenn } mvar(f) = x_i,\ f \in B \\ \infty & \text{sonst} \end{cases}$$

ist der zugehörige *Gradvektor*.

Wir nennen eine schwach triangulare Menge eine *charakteristische Menge von I*, wenn ihr Gradvektor bzgl. der invers lexikographischen Ordnung unter allen möglichen Gradvektoren minimal ist. Dabei ist die invers lexikographischen Ordnung definiert durch

$$(d_1, \ldots, d_n) < (d'_1, \ldots, d_n :) \ :<=> \ \exists\, i\ (d_i < d'_i \text{ und } \forall j > i\ d_j = d'_j)$$

Satz: Sei $G = (f_1, \ldots, f_n) \subset I$ eine schwach triangulare Menge, $J \subset I$ das von G erzeugte Ideal und $l = l_1 \cdot \ldots \cdot l_n$ das Produkt der Leitkoeffizienten.

1) G ist genau dann eine charakteristische Menge des Ideal I, wenn

$$h \in I \ => \ PNF(h, G) = 0$$

gilt.

In diesem Fall gilt

2) $J \subseteq I \subseteq J :< l >$.

3) $Z(G) \supset Z(I) \supset Z(G, l)$.

4) Ist I ein Primideal, dann gilt $I = J :< l >,\ Z(I) = Z(G, l)$ und somit

$$f \in I \quad <=> \quad PNF(f, G) = 0.$$

Beweis: 1) Sei G eine char. Menge, $h \in I$ und $h' = PNF(h, G) \neq 0$. Dann ist $h' \in I$ und für $x_i = mvar(h')$ gilt $deg(h', x_i) < d_i$. $B' := \{h'\} \cup \{f \in G\ :\ mvar(f) > i\}$ hätte dann einen kleineren Gradvektor als G.

Ist umgekehrt $G' = (f'_1, \ldots, f'_r) \subset I$ schwach triangular mit einem Gradvektor $(d'_1, \ldots, d'_n)$, der echt kleiner als der von G ist, also etwa $d'_i < d_i$ und $\forall\ j > i\ (d'_j = d_j)$, so ist offensichtlich $PNF(f', G) \neq 0$ für $f' \in G'$ mit $mvar(f) = x_i$.

2) folgt aus der Tatsache, daß

$$PNF(f, G) \equiv l_1^{a_1} \ldots l_n^{a_n} \cdot f\ (mod\ G)$$

gilt, 3) ist eine Umformulierung von 2).

4) Wegen der Reduziertheit von G ist $PNF(l_i, G) = l_i \neq 0$, also $\prod l_i \notin I$. Ist I ein Primideal und $PNF(f, G) = 0$, so folgt damit bereits $f \in I$. $\square$

Es im allgemeinen schwierig, solche charakteristischen Mengen zu konstruieren. Ist $F := \{f_1, \ldots, f_r\}$ eine Basis des Ideals I, so wollen wir deshalb wenigstens eine schwach triangulare Menge konstruieren, die noch einige gute Eigenschaften charakteristischer Mengen hat. Deshalb folgende weitere Definition:

Wir nennen $G \subset I$ eine *erweitert charakteristische Menge* des Ideals Ibzgl. der Basis F, wenn entweder G ein Polynom vom Grad 0 enthält (in diesem Fall ist also I trivial) oder eine schwach triangulare Menge ist mit $PNF(f, G) = 0$ für alle $f \in F$.

Satz: Ist $G = (f_1, \ldots, f_n) \subset I$ eine erweitert charakteristische Menge von $I = I(F)$ bzgl. F und $l = l_1 \cdot \ldots \cdot l_n$ das Produkt der Leitkoeffizienten von G, so gilt

$$I(G) \subseteq I \subseteq I(G) :< l >$$

und somit auch

$$Z(G) \supset Z(I) \supset Z(G, l).$$

Beweis: Wie oben zeigt man, daß $l^n\, f_i \in I(G)$ für $n \gg 0$ und damit auch $l^n\, I \subset I(G)$ gilt. $\square$

Um einen Algorithmus zu beschreiben, der eine solche erweitert charakteristische Menge aus einer vorgegebenen Idealbasis F konstruiert, führen wir noch die folgende Ordnung auf den nichtkonstanten Polynomen ein:

$$f < g \;\; :<=> \begin{cases} mvar(f) > mvar(g) \\ \text{oder} \\ x := mvar(f) = mvar(g) \text{ und } deg(f, x) < deg(g, x) \end{cases}$$

Der folgende Algorithmus von Ritt und Wu berechnet aus einer Idealbasis F eine erweitert charakteristische Menge G:

```
ExtCharSet(F)
Input: Idealbasis F von I
Output: erweitert charakteristische Menge G
begin R:=∅;
repeat
      G:=∅; F:=F ∪ R; F':=F;
      while F' ≠ ∅ do
            Wähle das kleinste f ∈ F'
            G:=G ∪ {f};
            Entferne aus F' alle Elemente, die bzgl. f nicht reduziert sind.
                  (* G ist eine schwach triangulare Menge *)
      R:={r := PNF(f,G) | r ≠ 0,  f ∈ F \ G};
until R = ∅;
return G
end.
```

Beispiel:

$$F := \{f_1 = x + y + z^2 - 3,\; f_2 = y^2 - y - z^2 + z,\; f_3 = 2 \cdot y \cdot (z^2 - 2) + z^4 - 5 \cdot z^2 + 6\}$$

Hier ist im ersten Durchlauf $G_1 = \{f_1, f_3\}, R = \{f_4\}$ mit $f_4 := PNF(f_2, G_1) = z^8 - 12 \cdot z^6 + 4 \cdot z^5 + 39 \cdot z^4 - 16 \cdot z^3 - 44 \cdot z^2 + 16 \cdot z + 12$ und danach $F = \{f_1, f_2, f_3, f_4\}$. Im zweiten Durchlauf erhalten wir $G_2 = \{f_1, f_3, f_4\}$ und $R = \emptyset$. G_2 ist also die gesuchte erweitert charakteristische Menge. Wir hatten bereits oben gesehen, daß in der Tat

$$Z(G_2) \supset Z(F) \supset Z(G, z^2 - 2)$$

gilt. Beide Inklusionen sind in diesem Fall strikt. $Z(G_2)$ ist nicht einmal mehr null-dimensional.

Satz: Obiger Algorithmus terminiert stets und erfüllt die geforderte Spezifikation.

Aufgabe: Beweisen Sie diesen Satz.

Wie wir im Beispiel gesehen haben, taugen solche charakteristischen Mengen jedoch nicht, um Nullstellenmengen vollständig zu beschreiben. Wir müssen im Laufe des Reduktionsprozesses offensichtlich eine Verzweigung zulassen, die auch den Fall berücksichtigt, daß ein aktueller Leitkoeffizient in einem Punkt der Nullstellenmenge verschwinden kann. Andererseits können wir nicht mit absoluten Nullstellenmengen $Z(G)$ arbeiten, weil die im Normalfall zu groß werden. Wir suchen deshalb im weiteren eine Zerlegung

$$Z(F) = \bigcup Z(T_i, q_i)$$

in Dreiecksmengen T_i, so daß $q_i \neq 0$ das Nichtverschwinden aller Leitkoeffizienten in T_i nach sich zieht. Bezeichnen wir für ein System F von Polynomen und $f \in F$

$mvar(F) := max(mvar(f) \mid f \in F)$,
$F^{top} := \{f \in F \mid mvar(f) = mvar(F)\}$,
$in(f) := in(f, mvar(f))$ und
$in(F) := lcm(in(t) \mid t \in F)$,

so bedeutet letzteres gerade $Z(in(T_i)) \cap Z(T_i, q_i) = \emptyset$. Solche Dreiecksmengen heißen in [7] bereits triangulare Systeme.

Der folgende Algorithmus konstruiert eine solche Zerlegung:

```
Triang(F,q)
Input: Polynomsystem F mit Nebenbedingung q
Output: Liste von Dreiecksmengen (T_i,q_i), so daß Z(F,q) = ⋃ Z(T_i,q_i) gilt.
begin
      if inconsistent(F) then return ∅;
            (* etwa, wenn F ein Polynom vom Grad 0 enthält *)
      if F^top = {f} then return
            append(
                  for each (T_i,q_i) in Triang(rest(F),q) collect ({f} ∪ T_i, lcm(in(f),q_i)),
                  Triang({in(f),red(f)} ∪ rest(F),q))
      else
            Wähle f ∈ F^top von minimalem Grad.
            return append(
                  Triang({f} ∪ {prem(g,f) ≠ 0 | g ∈ F^top \ {f}} ∪ (F \ F^top), lcm(q,in(f))),
                  Triang({in(f),red(f)} ∪ (F \ {f}),q));
end.
```

Beispiel. Für das obige System F erhalten wir die folgende Aufrufhierarchie: Am Anfang ist $F^{top} = \{f_1\}$, so daß $Triang(F, 1)$ zuerst $Triang((f_2, f_3), 1)$ aufruft. Hier ist $F^{top} = \{f, f_3\}$, also wird mit $f = f_3$ einerseits $Triang((f_3, f_4), z^2 - 2)$ und andererseits $Triang((f_2, f_5 := z^4 - 5 \cdot z^2 + 6, z^2 - 2), 1)$ aufgerufen. Das erstere System ist bereits in Dreiecksform. Für das zweitere erhalten wir nach Abspalten von f_2 mit $f = z^2 - 2$ wegen $prem(f_5, f) = 0$ das System $((f_2, z^2 - 2), 1)$ in Dreieckform.

Satz: Triang(F,q) terminiert nach endlich vielen Schritten mit einer Liste (T_i, q_i) von Systemen T_i in Dreiecksform, so daß $Z(q_i) \supset Z(in(T_i))$ und $Z(F, q)$ die disjunkte Vereinigung der relativen Nullstellenmengen $Z(T_i, q_i)$ ist.

Aufgabe: Beweisen Sie die Termination dieses Algorithmus.

Der zweite Teil der Behauptung ist offensichtlich: Wenn sie für jeden der beiden Zweige, die Tr rekursiv aufrufen, erfüllt ist, dann gilt sie auch für (F, q). Andererseits erfolgt die Verzweigung gerade nach dem Prinzip, ob auf dem zu konstruierenden Teil der Nullstellenmenge $in(f) = 0$ oder $in(f) \neq 0$ ist und die entsprechende Information wird entweder in T_i oder in q_i aufgenommen.

Beachte, daß $Z(T, q)$ leer sein kann. Dies geschieht etwa, wenn $prem(q, T) = 0$ ist, da dann $Z(q) \supset Z(T, in(T)) \supset Z(T, q)$ gilt. Deshalb nennt Wang in [7] ein Paar (T, q) mit $prem(q, T) \neq 0$ ein *feines triangulares System*. Aber selbst solche Systeme können eine leere relative Nullstellenmenge definieren. Dies kann zusätzlich beim Aufruf von `inconsistent` geprüft werden.

Beispiel: $F = (x_1^2 - 2, x_2^2 - 2x_1x_2 + 2, (x_1 - x_2)x_3 + 1)$ zerlegt sich unter Tr bzgl. $x_1 < x_2 < x_3$ in $(F, x_1 - x_2)$ und den leeren Zweig, also gilt $Z(F) = Z(F, x_1 - x_2)$. Aber aus den beiden ersten Gleichungen folgt $x_1 = x_2$, also $Z(F) = \emptyset$.

Aufgabe: Finden Sie die Zerlegung von $F = (x^{31} - x^6 - x - y, x^8 - z, x^10 - t)$ bzgl. $x > y > z > t$.

Im nulldimensionalen Fall kann man nach dem D5-Ansatz aus einem Dreieckssystem eine Liste von triangularen Systemen in unserem Sinne gewinnen. Wir wollen diesen Ansatz im weiteren nicht ausarbeiten, sondern am Beispiel $T = ((f_1, f_2, f_3), z^2 - 2)$ mit

$$\begin{aligned}
f_1 &:= x + y + z^2 - 3, \\
f_2 &:= 2 \cdot y \cdot (z^2 - 2) + z^4 - 5 \cdot z^2 + 6, \\
f_3 &:= z^8 - 12 \cdot z^6 + 4 \cdot z^5 + 39 \cdot z^4 - 16 \cdot z^3 - 44 \cdot z^2 + 16 \cdot z + 12\}
\end{aligned}$$

erläutern. Wegen $f_3 = (z^2 - 2)^2 f_4$ mit $f_4 = z^4 - 8z^2 + 4z + 3$ können wir das letzte Polynom vereinfachen. f_4 und $z^2 - 2$ sind teilerfremd, also gibt es eine Kombination

$$49 = (4z^3 + 9z^2 - 24z - 38)(z^2 - 2) - (4z + 9)f_4.$$

Multiplizieren wir also f_2 mit dem auf $Z(T)$ invertierbaren Polynom $a = 4z^3 + 9z^2 - 24z - 38$ und reduzieren anschließend bzgl. f_4, erhalten wir das zum Ausgangssystem äquivalente (echt) triangulare System

$$((x + y + z^2 - 3, 2y + z^2 - 3, z^4 - 8z^2 + 4z + 3), z^2 - 2).$$

Im allgemeinen Fall zweier Polynome $(f(y, z), g(z))$ berechnen wir $a(z) = gcd(in(f), g)$ und verzweigen nach $a = 0$ und $a \neq 0$. Im ersten Fall ist $(red(f), a)$ zu triangulieren, im zweiten $((f, g/a), a)$ zu vereinfachen. Hier ist aber $gcd(in(f), g/a) = 1$ und wir können wie oben verfahren.

Literatur

[1] S.-C. Chou: Mechanical geometry theorem proving. Reidel, Dortrecht 1988.

[2] S.-C. Chou: Automated reasoning in geometries using the characteristic set method and Gröbner basis method. In: Proc. ISSAC-90, ACM Press 1990.

[3] S.-C. Chou: Proving elementary geometry theorems using Wu's algorithm. *Contemp. Math.* **19** (1984), 243 - 286.

[4] Coxeter: Neue Treffen mit der Geometrie.

[5] E. Donath: Die merkwürdigen Punkte und Linien des ebene Dreiecks.

[6] M. Kalkbrener: A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.* **15** (1993), 143 - 167.

[7] D. Wang: An elimination method for polynomial systems. *J. Symb. Comp.* **16** (1993), 83 - 114.

[8] F. Winkler: Gröbner bases in geometry theorem proving and simplest degeneracy conditions. *Math. Pann.* **1** (1990), 15 - 32.

[9] W.-T. Wu: Mechanical Theorem Proving in Geometries. Texts and Monographs in Symbolic Computation 1, Springer Wien, 1994.

[10] W.-T. Wu: Some recent advances in mechanical theorem proving of geometry. *Contemp. Math.* **19** (1984), 235 - 241.

[11] W.-T. Wu: On the decosion problem and the mechanization of theorem-proving in elementary geometry. *Contemp. Math.* **19** (1984), 213 - 234.