Skript zum Kurs
Geometrie mit dem Computer
Wintersemester 2000/2001

Hans-Gert Gräbe, Univ. Leipzig

19. Januar 2001

0 Einführung

Die (synthetische) Geometrie ist eine sehr alte mathematische Disziplin und stand lange Zeit wohl für Mathematik schlechthin, ehe ihr dieser Platz durch eine stürmische Entwicklung der Mathematik in den letzten 200 Jahren von anderen Disziplinen streitig gemacht wurde. Natürlich hat sich in dieser Zeit auch die Geometrie weiter entwickelt. Teildisziplinen wie Differentialgeometrie oder Algebraische Geometrie untersuchen komplizierte geometrische Gebilde und haben zu wichtigen Einsichten über die Struktur von Raum (und Zeit) geführt. Die elementare Geometrie ist darüber, vollkommen zu unrecht, in die zweite Reihe gerückt. Das findet insbesondere seinen Ausdruck im Curriculum der Schule, in dem (elementar)geometrische Fragestellungen nur noch in geringem Umfang auftauchen.

Andererseits faszinieren solche Aufgaben immer wieder durch die Einfachheit, mit der relevante Probleme formuliert werden können, sowie den Scharfsinn und die Tiefgründigkeit der Argumentation, die zu deren Beantwortung herangezogen werden müssen. Sie sind damit für Hobbymathematiker, interessierte Schüler eingeschlossen, immer wieder eine Fundgrube von Problemen und Ideen, an denen man die eigene Argumentationskraft trainieren und verbessern kann. Die Vielfalt der Argumentationsmuster, die dabei zum Einsatz kommen, lassen eine Mechanisierung derartiger Beweisansätze als schier unmöglich erscheinen.

Besonders **Fragen der Konstruierbarkeit mit Zirkel und Lineal** haben Mathematiker verschiedener Epochen immer wieder fasziniert. So gehören die beiden großen Fragestellungen aus der antiken Mathematik nach der Verdopplung eines Würfels und der Dreiteilung eines beliebigen Winkels mit diesen Instrumenten zu den wohl auch außerhalb der Mathematik bekanntesten geometrischen Problemen. Trotz der Einfachheit der Fragestellung ließ sich deren Unlösbarkeit erst exakt nachweisen, als ein entsprechender **algebraischer Apparat**, in diesem Fall die Körpertheorie, entwickelt wurde. Eine solche *Methode der "Symbolisierung" geometrischer Sachverhalte* in der Sprache der Algebra erlaubte es C.F. Gauß im Jahre 1796, die Konstruierbarkeit eines 17-Ecks nachzuweisen. Die entsprechenden Argumente sind heute in den meisten Standardwerken zur (höheren) Algebra als Anwendungsbeispiele dieser Theorie enthalten.

Ein exaktes Studium der mit der Konstruierbarkeit verbundenen Fragestellungen kommt um **eine ordentliche Fundierung, eine Axiomatisierung der Geometrie** nicht herum. Auch hier lassen sich die entsprechenden Ansätze bis in die Antike hinein, etwa zu den Büchern des Euklid, verfolgen. Doch auch hier wurden entscheidende Fortschritte erst in der Neuzeit erreicht, die insbesondere mit den Namen D. Hilbert und F. Klein sowie der Klassifizierung der Transformationsgruppen verschiedener Geometrien verbunden sind. Unter diesem Blickwinkel stellte es sich heraus, daß man Geometrie in verschiedener Allgemeinheit betreiben kann, wobei jeweils eigene Fragestellungen, Grundlagen und Methoden zur Verfügung stehen.

Die aus der Schule bekannte **Euklidsche** oder **Bewegungsgeometrie** setzt dabei das umfangreichste Instrumentarium voraus. Neben Punkten, Geraden, Parallelen, Streckenlängen und Winkelgrößen gibt es auch noch Strahlen und Halbebenen, wozu auf jeder Geraden g (auf konsistente Weise) eine Ordnungsrelation zur Verfügung stehen muß, die es erlaubt, für drei Punkte $A, B, C \in g$ zu entscheiden, ob C zwischen A und B liegt. Geometrische Aussagen, die von Strahlen, Halbebenen und dieser *Zwischenrelation* Gebrauch machen, werden der **Ordnungsgeometrie** zugeordnet.

Da algebraische Verfahren, die wir zum Mechanisieren ausschließlich heranziehen werden, mit solchen Ordnungsrelationen nicht gut zusammenspielen, wollen wir derartige geometrische Aussagen im Weiteren ausklammern.

Damit wird der Kreis der betrachteten geometrischen Aufgaben aber nur etwas eingeschränkt, da viele Konfigurationen, in denen Strecken vorkommen, diese Ordnungsrelation in Wirklichkeit nicht ausnutzen. So kann man etwa den Mittelpunkt einer Strecke AB bestimmen, ohne zu wissen, wo auf der Geraden $g(AB)$ links oder rechts ist, indem man z.B. einfach ein Parallelogramm mit AB als einer seiner beiden Diagonalen konstruiert. Die Mitte der Strecke ist dann genau der Diagonalenschnittpunkt.

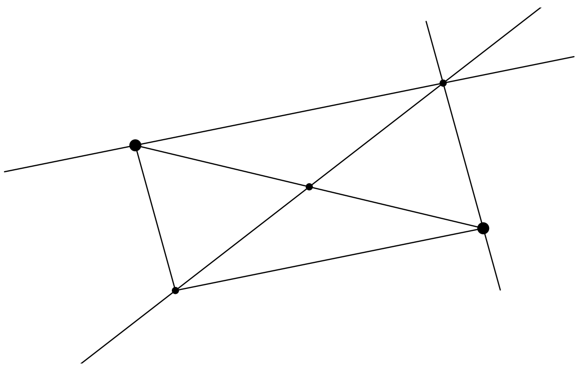

Bild 1.1: Affine Geometrie: Konstruktion des Mittelpunkts einer Strecke

Wir haben dafür nicht einmal die Möglichkeit der Euklidschen Geometrie benötigt, Strecken (und Winkel) vorgegebener Größe in einem vorgegebenen Punkt anzutragen, sondern einzig die Möglichkeit, zu vorgegebenen Geraden Parallelen konstruieren zu können. Eine Geometrie, die nur mit Punkten, Geraden und Parallelen auskommt, bezeichnet man als **affine Geometrie**. Im Mittelpunkt dieser Geometrie stehen der Strahlensatz und Eigenschaften des Parallelogramms.

Letzteres kann man z.B. verwenden, um eine vorgegebene Strecke *auf derselben Trägergeraden* in einem vorgegebenen Punkt abzutragen.

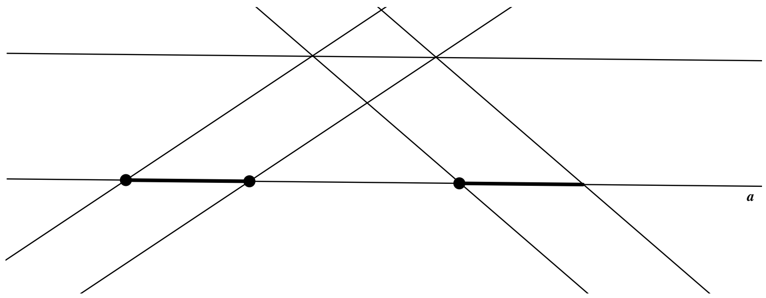

Bild 1.2: Affine Geometrie: Abtragen einer Strecke auf derselben Trägergeraden

Der Strahlensatz kann verwendet werden, um Strecken in vorgegebenen (rationalen) Verhältnissen zu teilen, womit die affine Geometrie auch den Begriff des Teilverhältnisses bereithält.

Noch allgemeinere Sätze der **projektiven Geometrie** erhält man, wenn man auch auf die Verwendung von Parallelen verzichtet. Derartige Sätze sind invariant unter projektiven Transformationen, d.h. solchen, die man in der Malerei bei der Übertragung einer weiten Landschaft auf die Staffelei antrifft, wenn sich die ehemals parallelen Geraden im Bild auf der *Horizontlinie* schneiden. Eine solche projektive Transformation überträgt eine geometrische Konfiguration von einer Ebene ε (im Raum) auf eine andere Ebene ε' nach folgendem Verfahren:

> Wähle ein Projektionszentrum Z außerhalb der beiden Ebenen aus. Den Bildpunkt $A' \in \varepsilon'$ zu einem Original $A \in \varepsilon$ findet man als den Schnittpunkt von $g(AZ)$ mit ε'.

Offensichtlich gehen bei dieser Konstruktion Geraden in Geraden über. In der Tat, die Geraden $g(AZ)$ für $A \in g$ spannen eine Ebene auf, so daß die Bildpunkte auf der Schnittgeraden dieser Ebene mit ε' liegen. Allerdings besitzt nicht jeder Punkt A der Urbildebene ε einen Bildpunkt, denn die Gerade $g(AZ)$ kann ja parallel zu ε' verlaufen. Die entsprechenden Punkte A mit dieser Eigenschaft liegen genau auf der Schnittgeraden von ε mit der Parallelen zu ε' durch Z. Diese Gerade bezeichnet man als die *Ausnahmegerade* auf ε. Ihre Punkte werden in die "unendlich ferne" Gerade von ε' abgebildet. Insbesondere sind die Bilder zweier Geraden, die sich in ε auf dieser Ausnahmegeraden schneiden, parallel zueinander. Genauso gibt es auf ε' eine Ausnahmegerade. Aussagen der projektiven Geometrie enthalten also typischerweise Formulierungen der Art "... die Geraden schneiden sich oder sind parallel zueinander ...".

Wie kann man nun eine solche Vielfalt von Ansätzen unter einen Hut bringen? Unsere hauptsächlichen Arbeitsmittel werden die Einführung von Koordinaten und Methoden der analytischen Geometrie sein. Es stellt sich dabei heraus, daß es ein solcher Ansatz gestattet, konstruktive, also algorithmische Ansätze auf der Seite der Geometrie mit Hilfe eines informatik-theoretischen Hilfsmittels, des Unterprogramms, in einem symbolischen Kontext in vielen Fällen so auszuwerten, daß sich daraus ein im mathematischen Sinne exakter Beweis ergibt.

Das Vorhandensein eines Koordinatensystems werden wir dabei, wie in der Schule auch, als gegeben voraussetzen. Da hierfür allein die Festlegung einer Einheitsstrecke und deren Übertragbarkeit an alle Orte und Richtungen der Ebene gewährleistet sein muß, stellt das, wenigstens für Problemstellungen innerhalb der Euklidschen Geometrie, keine Einschränkung dar.

Es stellt sich allerdings heraus, daß man das Vorhandensein eines Koordinatensystems aus noch viel allgemeineren Annahmen heraus ableiten kann. Diese Frage steht im Zentrum der axiomatischen Einführung der Geometrie und wird deshalb in den entsprechenden Lehrbüchern umfassend abgehandelt. Insbesondere in der Monographie [4] von W.-T. Wu sind dazu interessante Ausführungen enthalten, in denen auch Koordinatensysteme über nichtkommutativen Zahlbereichen eine Rolle spielen. Wir werden darauf nicht näher eingehen.

1 Einige Sätze aus der ebenen Geometrie

In diesem Kapitel wollen wir zunächst einige einfache und weniger einfache Sätze aus der ebenen Geometrie kennenlernen bzw. uns wieder ins Gedächtnis zurückrufen.

Dies soll zum einen ausreichendes Material für die weiteren Betrachtungen zur Verfügung stellen, an dem sich zu entwickelnde algorithmische Ansätze werden demonstrieren lassen, und zum anderen die Vielfalt geometrischer Argumente noch einmal demonstrieren, die im Rahmen einer Mechanisierung unter einen gemeinsamen Hut zu bringen sind.

Außerdem sollen wichtige Begriffe, die beim Beweisen geometrischer Sachverhalte eine Rolle spielen, beispielhaft demonstriert werden.

1.1 Sätze über die Ecktransversalen im Dreieck

Satz vom Schnittpunkt der Mittelsenkrechten

Verwendet den Begriff der *Ortslinie*: Eine Mittelsenkrechte besteht aus genau den Punkten, die von zwei gegebenen Punkten A, B den gleichen Abstand haben. Aus dem Beweis ergibt sich dann außerdem, daß der Schnittpunkt O von allen drei Eckpunkten gleichweit entfernt ist, also der Umkreismittelpunkt sein muß.

Eine Ortslinie verbindet eine geometrische (Mittelsenkrechte als Gerade) mit einer logischen (P mit $|AP| = |BP|$) Eigenschaft. Ihre Beweiskraft entwickeln Ortslinien aus dem Zusammenspiel beider Seiten.

Satz vom Schnittpunkt der Winkelhalbierenden

Auch hier spielen Ortslinien eine Rolle: Eine Winkelhalbierende besteht aus genau den Punkten, die von zwei gegebenen Geraden den gleichen Abstand haben. Aus dem Beweis ergibt sich dann außerdem, daß der Schnittpunkt W von allen drei Dreiecksseiten gleichweit entfernt ist, also der Inkreismittelpunkt sein muß.

Allerdings ist das ungenau, denn der genannte geometrische Ort besteht aus den Punkten auf dem Geraden-*Paar*, das die Halbierenden von Innen- und Außenwinkel bilden. Innenwinkel und Außenwinkel sind allerdings Begriffe der Ordnungsgeometrie und deshalb von unserem Standpunkt aus nicht zu unterscheiden. Die drei Winkelhalbierendenpaare haben neben dem Inkreismittelpunkt noch die drei Mittelpunkte der Ankreise gemeinsam.

Man beachte die Ähnlichkeit zum Begriff des *Parallelenpaars* als dem geometrischen Ort aller Punkte, die von einer gegebenen Gerade einen vorgegebenen Abstand haben.

Zwei Geraden schneiden sich (normalerweise) immer in genau einem Punkt. Wenn drei Geraden durch einen gemeinsamen Punkt gehen, so liegt schon eine besondere Situation vor. Solche Geraden nennt man *konkurrent*.

Umgekehrt geht durch zwei Punkte (normalerweise) immer genau eine Gerade. Wenn drei Punkte auf einer gemeinsamen Geraden liegen, so liegt ebenfalls eine besondere Situation vor. Solche Punkte nennt man *kollinear*.

Satz vom Schnittpunkt der Seitenhalbierenden

Beweis über Strahlensatz und seine Umkehrungen. Im Gegensatz zu den bisherigen Aussagen ist das ein Satz der affinen Geometrie.

Satz vom Höhenschnittpunkt

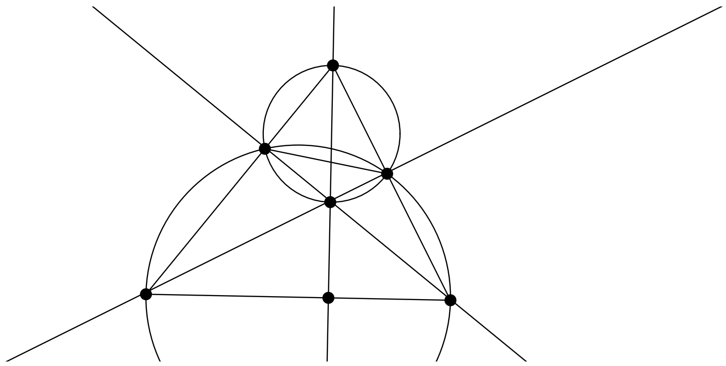

Bild 1.3: Beweis des Satzes vom Höhenschnittpunkt

Beweis über Mehrfachanwendung von Thaleskreis und Peripheriewinkelsatz.

Anwendung des Sehnensatzes liefert die zusätzliche Eigenschaft, daß der Höhenschnittpunkt die Höhen so teilt, daß die Produkte aus den beiden Höhenabschnitten jeweils gleichgroß sind.

1.2 Der Satz von Ceva

All diese Sätze kann man aus einem allgemeinen Prinzip über Teilverhältnisse von Transversalen am Dreieck herleiten.

Satz 1 (Satz des Ceva) *Drei Ecktransversalen des Dreiecks ΔABC mögen die gegenüberliegenden Seiten in den Punkten D, E, F schneiden. Diese drei Ecktransversalen gehen genau dann durch einen Punkt, wenn*

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

gilt.

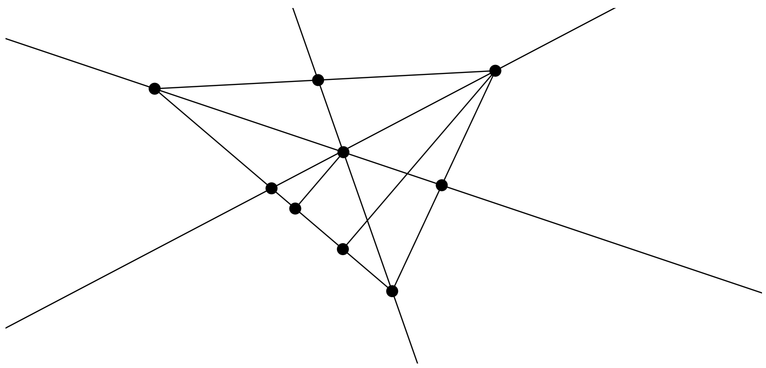

Bild 1.4: Der Satz des Ceva

Beweis über den Vergleich von Flächeninhalten: $c_1 : c_2 = F(APC) : F(BPC)$ usw.

Als Folgerung erhält man neue Beweise der Sätze vom Schnittpunkt der Seitenhalbierenden und vom Höhenschnittpunkt.

Aufgabe 1:

a) Zeigen Sie, daß man aus dem Satz des Ceva auch den Satz vom Höhenschnittpunkt herleiten kann, indem Sie die Längen der Seitenabschnitte durch geeignete trigonometrische Formeln ausdrücken.

b) Zeigen Sie, daß die Transversalen zu den Berührungspunkten des Inkreises sich in einem Punkt schneiden. (Hinweis: Berechnen Sie die Länge der einzelnen Tangentenabschnitte.)

Weitere Folgerung:

Die Transversalen zu den drei Berührungspunkten der Ankreise schneiden sich in einem Punkt. (Dieser Punkt heißt auch Nagelscher Punkt*)*

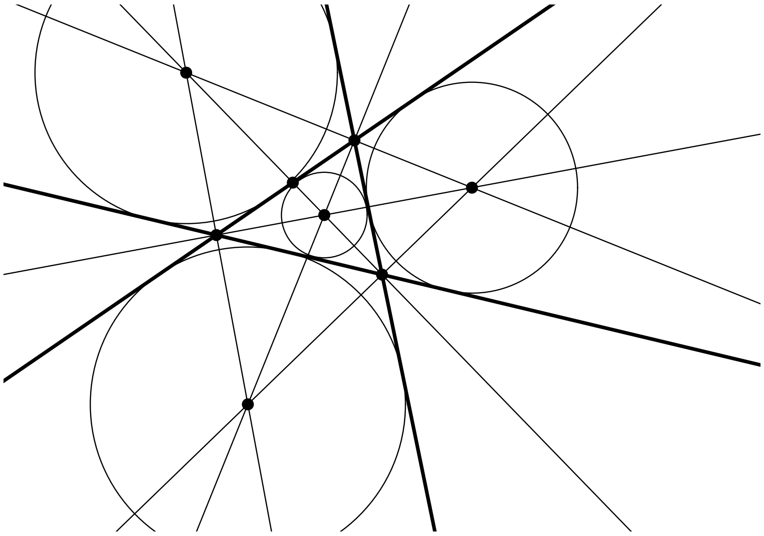

Bild 1.5: In- und Ankreise am Dreieck

Betrachte dazu verschiedene Beziehungen zwischen den Tangentenabschnitten zu den Berührungspunkten der drei Ankreise:

$$\begin{array}{rrcl} & x+y+z & = & r+s+t \\ & x+y+t & = & z+r+s \\ \hline \Rightarrow & z & = & t \end{array}$$

Analog gilt $x = r,\ y = s$.

1.3 Weitere Sätze am Dreieck

Satz 2 (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.*

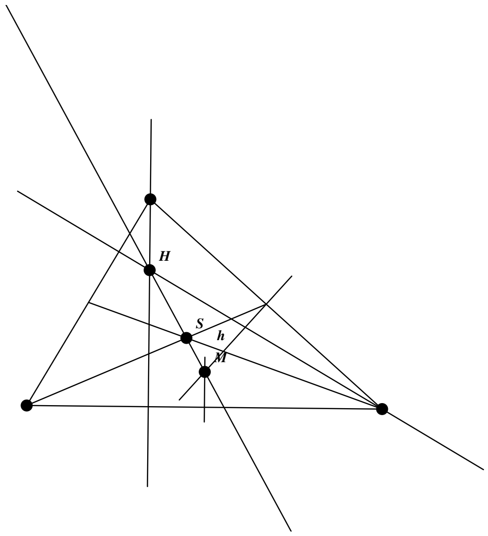

Bild 1.6: Die Eulersche Gerade

Im Beweis werden Dreiecke in Ähnlichkeitslage verwendet.

Zwei Dreiecke ABC und $A'B'C'$ heißen in Ähnlichkeitslage, wenn einander entsprechende Seiten jeweils zueinander parallel sind.

Dann kann man schlußfolgern, daß das eine Dreieck aus dem anderen durch eine Zentralstreckung hervorgeht. Diese Aussage ist Gegenstand des folgenden Satzes.

Satz 3 (Der affine 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 $BC \| B'C'$.*

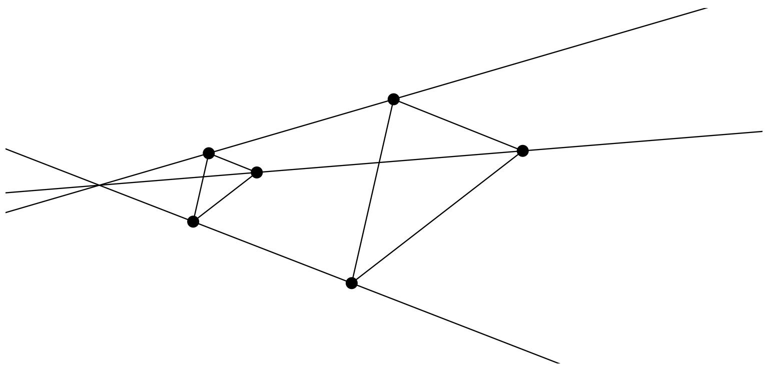

Bild 1.7: Der (affine) Satz von Desargue

Aufgabe 2:

Leiten Sie diesen Satz aus dem Strahlensatz her.

Der Satz von Desargue spielt in der Fundierung der Geometrie als "schwache Version des Strahlensatzes" eine wichtige Rolle. Er ist schwächer als der Strahlensatz und führt damit zu einer umfassenderen als der affinen Geometrie. Details finden sich im Buch [4].

Satz 4 (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*

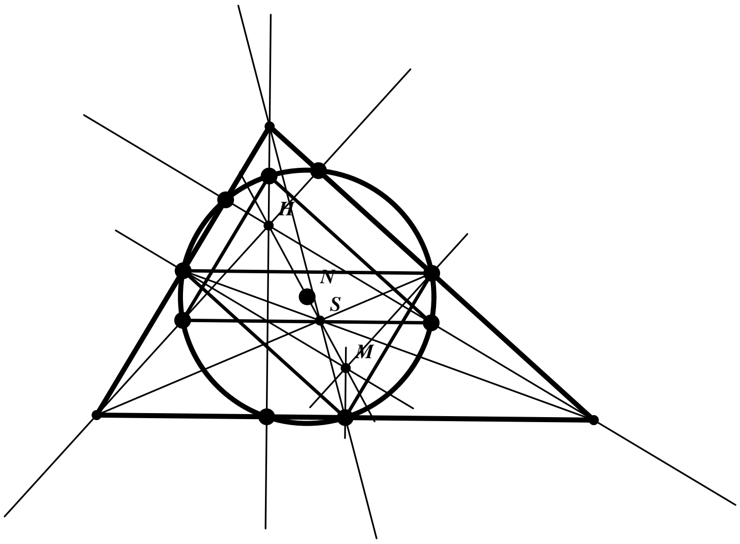

Bild 1.8: Der Feuerbachsche Kreis

Beweis : Die beiden Dreiecke, die durch die Seitenmitten bzw. die Mitten der oberen Höhenabschnitte aufgespannt werden, sind in Ähnlichkeitslage mit dem Faktor (-1), also zueinander kongruent. Sie gehen durch Drehung um N um 180^o ineinander über, wobei H als Höhenschnittpunkt in M als Höhenschnittpunkt des Seitenmittendreiecks übergeht. N ist außerdem nach Strahlensatz der Umkreismittelpunkt eines der beiden Dreiecke. Also geht der Feuerbachkreis durch die genannten 6 Punkte. Schließlich entsprechen sich Seitenmitte und gegenüberliegende Mitte des oberen Höhenabschnitts. Die Verbindungsgerade geht also durch das Streckungszentrum N und ist ein Durchmesser des Feuerbachkreises. Aus dem Satz des Thales folgt schließlich, dass auch der Höhenfußpunkt auf dem Feuerbachkreis liegt. $\square$

Der Feuerbachkreis hat eine weitere, mit elementargeometrischen Mitteln nur schwer zu beweisende Eigenschaft: Er berührt den Inkreis des Dreiecks $\Delta\, ABC$ und dessen drei Ankreise.

1.4 Sätze am Dreieck aus der neueren Forschung

Wir erwähnen hier nur zwei Sätze, die im Zusammenhang mit dem mechanisierten Theorembeweisen in der Geometrie immer wieder als Beispiele herangezogen werden.

Satz 5 (Der Miquelsche Punkt) *Nimmt man auf jeder Seite eines Dreiecks ΔABC 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.*

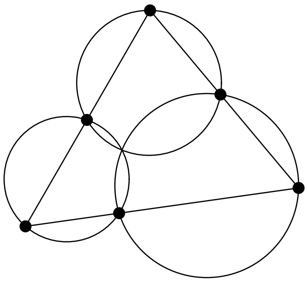

Bild 1.9: Der Miquelsche Punkt

Der Beweis folgt fast unmittelbar aus dem Satz über das Sehnenviereck und dessen Umkehrung.

Satz 6 (Die Simsonsche Gerade) *Fällt man von einem Punkt P außerhalb eines Dreiecks ΔABC 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 ΔABC liegt.*

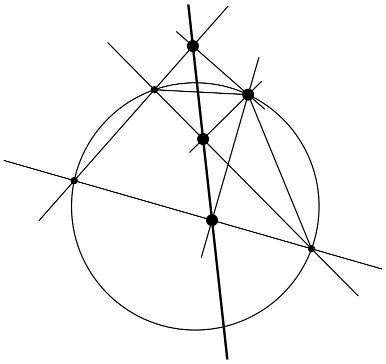

Bild 1.10: Die Simsonsche Gerade

Beweis : Seien die drei Fußpunkte mit A_1, B_1, C_1 bezeichnet (d.h. A_1 ist der Fußpunkt des Lots von P auf $g(BC)$ usw.). Der Thaleskreis über PC liefert $\angle B_1A_1P = \angle B_1CP$. Der Thaleskreis über PA liefert $\angle B_1C_1P = \angle B_1AP$. Im Sehnenviereck $ABCP$ ist $\angle APC = 180^o - \beta$. Wegen zweier rechter Winkel ist aber auch $\angle A_1PC_1 = 180^o - \beta$. Folglich ist $\angle A_1B_1C_1 = \angle AB_1C = 180^o$, A_1, B_1, C_1 also kollinear. □

Zu beiden Sätzen gäbe es noch eine Menge zu sagen. So kann man etwa zu jedem Punkt P im Inneren des Dreiecks ΔABC Punkte A_1, B_1, C_1 so auf den Dreiecksseiten finden, daß P der zugehörige Miquelsche Punkt ist. Ein solches Dreieck bekommt man (Thalessatz!) insbesondere dann, wenn man von P aus die Lote auf die drei Dreiecksseiten fällt. Dieses Dreieck wird auch als das zum Punkt P gehörende *Fußpunktdreieck* bezeichet.

Aufgabe 3:

a) [2, 1.91] Zeigen Sie, daß die Seiten des Fußpunktdreiecks von P die Längen

$$\frac{a\,x}{2\,r}, \frac{b\,y}{2\,r}, \frac{c\,z}{2\,r}$$

haben, wobei $a = |BC|$, $b = |AC|$, $c = |AB|$ die Längen der Seiten des Dreiecks $\Delta\, ABC$, r dessen Umkreisradius und $x = |AP|$, $y = |BP|$, $z = |CP|$ die Abstände von den Eckpunkten zu P sind.

b) Zeigen Sie, daß für den Flächeninhalt des Fußpunktdreiecks $A_1B_1C_1$ bzgl. P

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

gilt, wobei M der Umkreismittelpunkt ist.

Das eben betrachtete Fußpunktdreieck entartet zu einer Geraden, wenn P auf dem Umkreis des Dreiecks $\Delta\, ABC$ liegt und ergibt dann genau die Simsonsche Gerade. Von Satz über die Simsonsche Gerade gilt übrigens auch die Umkehrung:

Satz 7 (Simsonsche Gerade II) *Sind die Lotfußpunkte A_1, B_1, C_1 von einem Punkt P auf die Seiten des Dreiecks $\Delta\, ABC$ oder deren Verlängerungen kollinear, so liegt P auf dem Umkreis des Dreiecks.*

AUFGABE 4:

a) Leiten Sie aus der Flächeninhaltsformel für das Fußpunktdreieck (vorige Aufgabe) einen zweiten Beweis für den Satz über die Simsonsche Gerade her.

b) Beweisen Sie die Umkehrung des Satzes von der Simsonschen Geraden.

Weitere interessante Sätze, die an dieser Stelle vielleicht noch zu nennen wären (alle aus [2]): Satz des Ptolemäus, Satz vom Schmetterling und der Satz von Morley.

1.5 Sätze der projektiven Geometrie

Wir wollen dieses Kapitel mit einigen Sätzen aus der projektiven Geometrie beschließen, die ob der verwendeten Mittel (meist nur genügend verzwickte Geradenkonfigurationen) einen ganz speziellen Reiz besitzen.

Satz 8 (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. Die entstehende Gerade wollen wir als* Pappus-Gerade *bezeichnen.*

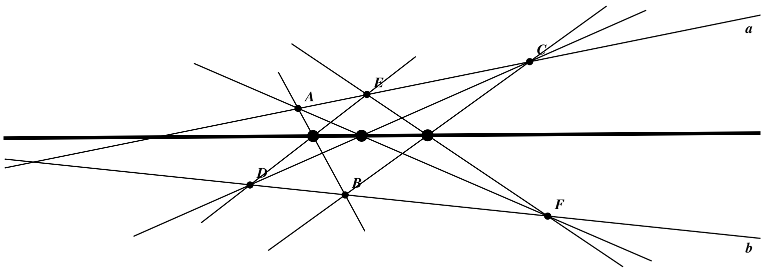

Bild 1.11: Pappus-Gerade

Beweis : Wir beweisen diesen Satz zuerst in einer speziellen Situation, in der zwei der drei Verbindungegeraden zueinander parallel sind:

$$AB\|DE, BC\|EF \Rightarrow CD\|AF$$

Der Beweis ergibt sich hier unmittelbar aus dem Strahlensatz und seinen Umkehrungen.

Für den allgemeinen Beweis verwenden wir eine projektive Transformation, bei der die Gerade $g(AB \cap DE, BC \cap EF)$ die Ausnahmegerade ist, d.h. in der Bildebene in die Ferngerade übergeht. Damit sind für das Bild unserer Geradenkonfiguration die Voraussetzungen des bewiesenen Spezialfalls erfüllt und die Bilder von $g(CD)$ und $g(AF)$ sind zueinander parallel. Die Urbilder schneiden sich damit auf der Ausnahmegeraden, so daß die drei Schnittpunkte kollinear sind. □

Übrigens ist auch der Satz von Desargue eigentlich ein projektiver Satz.

Satz 9 (Allgemeiner Satz von Desargue) *Sind die Schnittpunkte $AB \cap A'B'$, $AC \cap A'C'$ und $BC \cap B'C'$ kollinear, so gehen die drei Geraden AA', BB' und CC' durch einen gemeinsamen Punkt.*

Beweis : Wir betrachten eine projektive Transformation, die die Gerade durch die drei Schnittpunkte auf die Ferngerade abbildet. Dann haben wir gerade die Situation des affinen Satzes von Desargue vorliegen. □

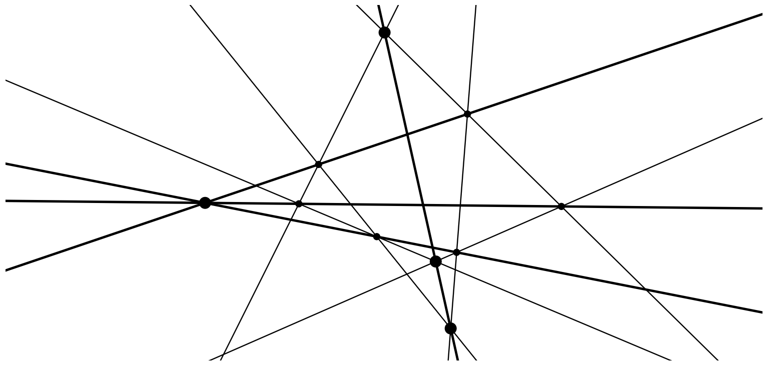

Bild 1.12: Allgemeiner Satz von Desargue

Eine interessante Fragestellung, die wir zum selben Thema hier nur aufwerfen wollen, entsteht aus dem Vergleich verschiedener Pappus-Geraden. Sind A_1, A_2, A_3 und B_1, B_2, B_3 jeweils kollinear, so führen die verschiedenen Permutationen der Punkte B_1, B_2, B_3 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). Es stellt sich heraus, daß drei dieser Geraden durch einen gemeinsamen Punkt gehen.

Der Satz von Pappus ist ein Spezialfall eines noch allgemeineren Satzes der projektiven Geometrie. Wir betrachten dazu eine Konfiguration aus sechs Punkten der Ebene A, B, C, D, E, F, für die $X = AB \cap DE, Y = BC \cap EF$ und $Z = CD \cap AF$ kollinear sind. In einer solchen Konfiguration sind die ersten fünf Punkte frei wählbar, wobei auch die Lage von X bestimmt wird. Die Richtung der Geraden $g = g(EF)$ bestimmt Y eindeutig und somit auch $Z = CD \cap XY$. F ergibt sich dann als $F = AZ \cap g$. Eine solche Punktekonfiguration bezeichnet man als ein *Pascalsches Sechseck*.

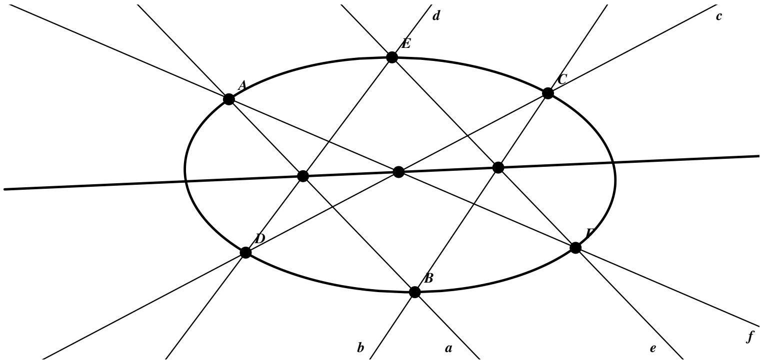

Bild 1.13: Pascalsches Sechseck

Führt man Koordinaten ein, so stellt sich heraus, daß sich solche Punktekonfigurationen analytisch recht einfach charakterisieren lassen. Es gilt der folgende

Satz 10 (Satz von Pascal) *Sechs Punkte spannen genau dann ein Pascalsches Sechseck auf, wenn sie auf einer Kurve zweiten Grades liegen.*

Auf einen vollständigen Beweis dieses Satzes muß hier verzichtet werden, da hierfür noch Kurven zweiten Grades einzuführen wären. Man kann aber wie im Beweis des Satzes von Pappus einen wesentlichen Teil durch eine projektive Transformation aus einer spezielleren Situation herleiten, die Gegenstand der folgenden Aufgabe ist. AUFGABE 5:

> Beweisen Sie den folgenden Spezialfall des Satzes von Pascal:
> Liegen die Punkte A, B, C, D, E, F auf einem Kreis und gilt $AB \| CD$ und $BC \| EF$, so ist auch $CD \| EF$.

Eine wichtige Folgerung aus dem Satz von Pascal ist die aus der ursprünglichen Definition nicht ersichtliche Tatsache, daß jede Permutation von Punkten, die ein Pascalsches Sechseck aufspannen, wieder ein solches bilden. Das liefert Aussagen der ebenen Geometrie, zu deren Formulierung keine Kurven zweiter Ordnung benötigt werden. Solche Sätze heißen in [4] *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.

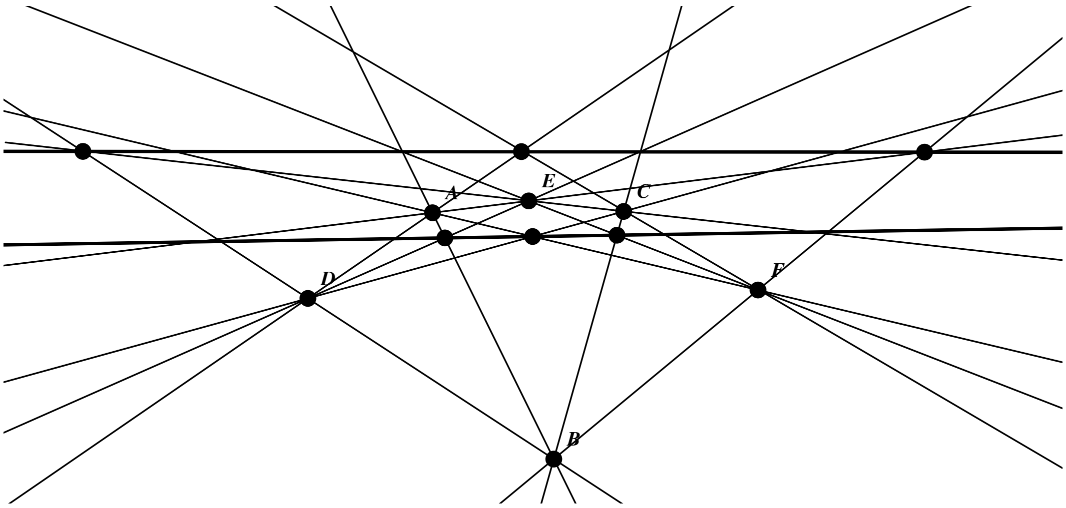

Bild 1.14: Satz vom Pascal-Typ

2 Die Koordinatenmethode und geometrische Sätze vom konstruktiven Typ

2.1 Grundlegende geomtrische Zusammenhänge in koordinatengeometrischer Interpretation

Wir wollen nun Methoden der analytischen Geometrie anwenden, um geometrische Aussagen zu beweisen. Dazu fixieren wir ein kathesisches Koordinatensystem, so dass sich Punkte durch zwei Parameter $P = (p_1, p_2)$, seine Koordinaten bzgl. dieses Koordinatensystems, darstellen lassen.

Auf ähnliche Weise ergeben sich Darstellungen auch für abgeleitete Objekte wie Geraden oder Kreise. Ein Tripel $g = (g_1, g_2, g_3)$ steht etwa für die Gerade aus den Punkten $\{ (x_1, x_2) \ : \ g_1x_1 + g_2x_2 + g_3 = 0 \}$. Ein solches Tripel bezeichnet man als *homogene Koordinaten* der Geraden g. Zueinander proportionale Tripel beschreiben dieselbe Gerade g und für (echte) Geraden dürfen g_1 und g_2 nicht gleichzeitig verschwinden.

Die wichtigsten geometrischen Eigenschaften von Punkten und Geraden spiegeln sich dann in den folgenden Formeln wider:

- A, B, C sind *kollinear*, d.h. liegen auf einer gemeinsamen Geraden g genau dann, wenn das homogene lineare Gleichungssystem

  $$\begin{aligned} g_1a_1 + g_2a_2 + g_3 &= 0 \\ g_1b_1 + g_2b_2 + g_3 &= 0 \\ g_1c_1 + g_2c_2 + g_3 &= 0 \end{aligned}$$

  eine (nichttriviale) Lösung in (g_1, g_2, g_3) besitzt, d.h. wenn

  $$det \begin{pmatrix} a_1 & a_2 & 1 \\ b_1 & b_2 & 1 \\ c_1 & c_2 & 1 \end{pmatrix} = 0$$

  gilt.

- Analog gehen drei Geraden g, h, k durch einen gemeinsamen Punkt genau dann, wenn das lineare Gleichungssystem

  $$\begin{aligned} g_1x_1 + g_2x_2 + g_3 &= 0 \\ h_1x_1 + h_2x_2 + h_3 &= 0 \\ k_1x_1 + k_2x_2 + k_3 &= 0 \end{aligned}$$

  eine Lösung in (x_1, x_2) besitzt. Das ist genau dann der Fall, wenn die zugehörige Koeffizientenmatrix denselben Rang wie die erweiterte Koeffizientenmatrix hat. Da dieser Rang höchstens 2 sein kann, muss also

  $$det \begin{pmatrix} g_1 & g_2 & g_3 \\ h_1 & h_2 & h_3 \\ k_1 & k_2 & k_3 \end{pmatrix} = 0$$

  gelten. Ist der Rang der Koeffizientenmatrix gleich 2, so hat das System dann eine (eindeutig bestimmte) Lösung. Ist ihr Rang dagegen gleich 1, d.h. sind ihre drei Zeilen (g_1, g_2), (h_1, h_2) und (k_1, k_2) zueinander proportional, so sind die drei Geraden g, h, k zueinander parallel, schneiden sich also "im Unendlichen" oder fallen zusammen.

  Geraden, die durch einen gemeinsamen Punkt gehen oder zueinander parallel sind, bezeichnet man als *konkurrente Geraden*.

- Für die Parameter einer Geraden durch zwei Punkte A, B erhalten wir aus der Zwei-Punkte-Gleichung

  $$(g_1, g_2, g_3) = (b_2 - a_2,\, a_1 - b_1,\, a_2b_1 - a_1b_2)$$

- Zwei Geraden g, h sind parallel genau dann, wenn $g_1 h_2 - h_1 g_2 = 0$ gilt, d.h. ihre Normalenvektoren (g_1, g_2) und (h_1, h_2) zueinander parallel sind.
- Die Parameter der Parallelen h zu g durch einen Punkt P ergeben sich durch Adjustieren des Absolutglieds von g als

$$(h_1, h_2, h_3) = (g_1, g_2, -(g_1 p_1 + g_2 p_2)).$$

- Die Koordinaten des Schnittpunkts P zweier Geraden g, h berechnet sich als Lösung des entsprechenden Gleichungssystems nach der Cramerschen Regel zu

$$(p_1, p_2) = \left(\frac{g_2 h_3 - g_3 h_2}{d}, \frac{g_3 h_1 - g_1 h_3}{d} \right) \quad \text{mit} \quad d = g_1 h_2 - h_1 g_2$$

- Ein Punkt X auf der Geraden $g(AB)$ hat bei bekanntem Teilverhältnis $u = \frac{l(AX)}{l(AB)}$ die Koordinaten

$$(x_1, x_2) = ((1-u)\, a_1 + u\, b_1,\ (1-u)\, a_2 + u\, b_2)$$

Auch Begriffe aus der Euklidschen Geometrie lassen sich symbolisch durch entsprechende Koordinaten ausdrücken:

- So ergibt sich der Abstand zwischen den Punkten A, B aus der Formel

$$d(A, B) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}.$$

Da es sich dabei nicht um einen polynomialen Ausdruck handelt, wollen wir statt dessen mit dem *Abstandsquadrat* $sqrdist(A, B) = d(A, B)^2$ arbeiten.

- Zwei Geraden g, h sind orthogonal genau dann, wenn ihre Normalenvektoren (g_1, g_2) und (h_1, h_2) senkrecht aufeinander stehen, d.h. für das entsprechende Skalarprodukt

$$g_1 h_1 + g_2 h_2 = 0$$

gilt.

- Schließlich lässt sich das Lot h von P auf die Gerade g ausdrücken als

$$(h_1, h_2, h_3) = (g_2, -g_1, g_1 p_2 - g_2 p_1).$$

2.2 Zur Algorithmisierung geometrischer Konstruktionen. Analytische Geometrie mit dem Computer

Wir können auf der Basis der soeben hergeleiteten oder noch einmal zusammengestellten Beziehungen nun in einer klassischen imperativen Programmiersprache (die an dieser Stelle nicht über die Fähigkeit zur Symbolverarbeitung verfügt) Programme schreiben, die in der Lage sind, Beziehungen in durch konkrete Koordinatenwerte vorgegebenen geometrischen Konfigurationen zu überprüfen oder gesuchte Größen auszurechnen und z.B. über eine entsprechende Schnittstelle auch graphisch darzustellen.

Die elementaren geometrischen Objekte Punkt und Gerade stellen wir dazu als Datentypen `Point` und `Line` dar, etwa als

```
class Point {
public:
  Scalar x,y;

  Point(Scalar u, Scalar v) {x=u; y=v;}
  void print();
};

class Line  {
public:
  Scalar a,b,c;

  Line(Scalar u, Scalar v, Scalar w) {a=u; b=v; c=w;}
  void print();
};
```

hinter denen sich der entsprechende Punkt $P(x, y)$ bzw. die Gerade

$$g(a, b, c) := \{(x, y) \,:\, ax + by + c = 0\}$$

verbergen. `Scalar` ist dabei ein Körper, aus dem die Werte der Koordinaten kommen, also in einer klassischen Programmiersprache etwa der interne Typ `float` oder etwas Selbstgestricktes wie `Rational` oder `Complex`. Wir wollen annehmen, dass für diesen Datentyp die arithmetischen Operationen $+ \; - \; * \; /$ sowie ein boolesches Prädikat `int iszero(Scalar a)` definiert sind.

Geometrische Grundkonstruktionen können wir in diesem Kontext als Funktionen auffassen, die aus gegebenen Objekten neue konstruieren.

1) Die Gerade durch zwei Punkte P und Q

```
Line pp_line(Point p, Point q) {
  return Line(q.y-p.y, p.x-q.x, p.y*q.x-p.x*q.y);
}
```

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, wobei die zu definierende Funktion mit einer Fehlermeldung abbricht, wenn kein bzw. kein eindeutig bestimmter Schnittpunkt existiert.

```
Point intersection_point(Line g, Line h) {
  Scalar d = g.a*h.b-g.b*h.a;
  if (iszero(d)) perror("Geraden parallel");
  return Point((g.b*h.c - g.c*h.b)/d,(g.c*h.a - g.a*h.c)/d);
}
```

Auch hier sind g und h formale Parameter, diesmal vom Typ `Line`.

3) Für das Lot l von einem Punkt P auf eine Gerade g erhalten wir analog

```
Line perpendicular(Point p, Line g) {
  return Line(g.b, -g.a, g.a*p.y - g.b*p.x);
}
```

und für die Parallele zu einer Geraden g durch einen Punkt P

```
Line par_line(Point p, Line g) {
  return Line(g.a, g.b, -(g.a*p.x + g.b*p.y));
}
```

Das *Abstandsquadrat* ergibt sich schließlich als

```
Scalar sqrdist(Point p, Point q) {
  return ((p.x-q.x)*(p.x-q.x) + (p.y-q.y)*(p.y-q.y));
}
```

4) 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 Skalare 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 durch zwei Punkte gegebenen Geraden kann man etwa durch eine zufällige Wahl des entsprechenden Teilverhältnisses festlegen:

```
Point varpoint(Point P, Point Q, Scalar u) {
  return Point((1-u)*p.x+u*q.x,(1-u)*p.y+u*q.y);
}
```

erzeugen. Insbesondere liefert

```
Point midpoint(Point P,Point Q) { return varpoint(P,Q,1/2); }
```

den Mittelpunkt der Strecke PQ (wir hatten vorausgesetzt, dass / zur Signatur des Datentyps `Scalar` gehört).

5) 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

```
Point pedalpoint(Point P, Line a) {
  return intersection_point(perpendicular(P,a),a);
}
```

AUFGABE 6:

Geben Sie entsprechende Funktionen an

- `Line midpoint_perpendicular(Point A, Point B)` für die Mittelsenkrechte auf der Seite AB,
- `Line altitude(Point A, Point B, Point C)` für die Höhe durch A im Dreieck ABC,
- `Line median(Point A, Point B, Point C)` für die Seitenhalbierende, die durch A im Dreieck ABC verläuft.

6) Schließlich kann man testen, ob für gewisse Konfigurationen geometrische Bedingungen erfüllt sind. So kann man etwa testen, ob zwei gegebene Geraden g und h parallel oder orthogonal sind, indem man prüft, ob $g_1h_2 - g_2h_1$ bzw. $g_1h_1 + g_2h_2$ verschwindet, oder ob ein Punkt P auf einer Geraden g liegt. Entsprechende Funktionen haben folgende Spezifikation:

```
int is_parallel(Line g, Line h) {
  return iszero(g.a*h.b-h.a*g.b);
}
```

bzw.

```
int is_orthogonal(Line g, Line h) {
  return iszero(g.a*h.a+g.b*h.b);
}

int is_point_on_line(Point P, Line g) {
  return iszero(g.a*P.x+g.b*P.y+g.c);
}
```

Auch kompliziertere Bedingungen, die wir im letzten Paragraph hergeleitet hatten, kann man auf diese Weise prüfen, so z.B., ob drei gegebene Punkte P, Q, R *kollinear* oder drei gegebene Geraden a, b, c d.h. *konkurrent* sind. Die entsprechenden Funktionen haben die Signatur `is_collinear(A,B,C:Point):int` bzw. `is_concurrent(a,b,c:Line):int`.

Aufgabe 7:

> Führen Sie die Implementierung entsprechender Funktionen wie oben begonnen in einer klassischen Programmiersprache zu Ende.

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

```
int Test(Point A, Point B, Point C) {
  return is_concurrent(mp(A,B), mp(B,C), mp(C,A));
}
```

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:

```
int Test(Point A, Point B, Point C) {
  Point M = intersection_point(midpoint_perpendicular(A,B),
            midpoint_perpendicular(B,C));
  return is_point_on_line(M, midpoint_perpendicular(C,A));
}
```

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 iszero(sqrdist(M,A) - sqrdist(M,B))
      and iszero(sqrdist(M,B) - sqrdist(M,C));
```

zu ersetzen.

Aufgabe 8:

Geben Sie analoge Testfunktionen für die Sätze vom Schnittpunkt der Höhen bzw. 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:

```
int Test(Point A, Point B, Point C) {
  Point M = intersection_point(midpoint_perpendicular(A,B),
            midpoint_perpendicular(B,C));
  Point H = intersection_point(altitude(A,B,C), altitude(B,C,A));
  Point S = intersection_point(median(A,B,C), median(B,C,A));
  return is_collinear(M,H,S);
}
```

Aufgabe 9:

> Modifizieren Sie diese Testfunktion so, dass sie den Satz vom Feuerbachschen Kreis testet.
>
> Testen Sie den Satz von Desargue.

2.3 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 10:

> Implementieren Sie obige Palette von Funktionen in einem der gängigen Computeralgebrasysteme Maple, Mathematica, Reduce oder Macsyma. (Eine Reduce-Lösung siehe `geo2.r`).

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. Dieser rationale Ausdruck stellt eine *universelle Formel* in dem Sinne dar, dass jede konkrete Belegung der Variablen mit Werten aus dem Grundbereich, also etwa den reellen Zahlen, zu den Parametern der abgeleiteten geometrischen Größe führt. 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 `intersection_point(midpoint_perpendicular(B,C), midpoint_perpendicular(C,A))` in der Formel

$$\left(\frac{m_2n_3 - m_3n_2}{m_1n_2 - m_2n_1}, \frac{m_3n_1 - m_1n_3}{m_1n_2 - m_2n_1}\right),$$

nach der sich die Koordinaten des Schnittpunkts der Geraden m, n berechnen, die Komponenten von m, n durch die entsprechenden rationalen Ausdrücke

$$\texttt{midpoint\_perpendicular}(B,C) = \{b_1 - c_1,\ b_2 - c_2,\ \frac{-b_1^2 - b_2^2 + c_1^2 + c_2^2}{2}\}$$

bzw.

$$\texttt{midpoint\_perpendicular}(C,A) = \{-a_1 + c_1,\ -a_2 + c_2,\ \frac{a_1^2 + a_2^2 - c_1^2 - c_2^2}{2}\}$$

zu ersetzen sind. Diese Ausdrücke sind ihrerseits während des Aufrufs

```
midpoint_perpendicular(B,C) == perpendicular(midPoint(B,C),pp_line(B,C))
```

in einem Substitutions- und Simplifikationsprozess (der Tiefe 2) nach demselben Prinzip entstanden. Wir erhalten in diesem Fall als Formel für den Umkreismittelpunkt

$$M := \left(\frac{\begin{array}{l} {a_1}^2 b_2 - {a_1}^2 c_2 + {a_2}^2 b_2 - {a_2}^2 c_2 - \\ a_2 {b_1}^2 - a_2 {b_2}^2 + a_2 {c_1}^2 + a_2 {c_2}^2 + \\ {b_1}^2 c_2 + {b_2}^2 c_2 - b_2 {c_1}^2 - b_2 {c_2}^2 \end{array}}{\begin{array}{l} 2\, a_1 b_2 - 2\, a_1 c_2 - 2\, a_2 b_1 + 2\, a_2 c_1 + \\ 2\, b_1 c_2 - 2\, b_2 c_1 \end{array}} , \frac{\begin{array}{l} -{a_1}^2 b_1 + {a_1}^2 c_1 + a_1 {b_1}^2 + a_1 {b_2}^2 - \\ a_1 {c_1}^2 - a_1 {c_2}^2 - {a_2}^2 b_1 + {a_2}^2 c_1 - \\ {b_1}^2 c_1 + b_1 {c_1}^2 + b_1 {c_2}^2 - {b_2}^2 c_1 \end{array}}{\begin{array}{l} 2\, a_1 b_2 - 2\, a_1 c_2 - 2\, a_2 b_1 + 2\, a_2 c_1 + \\ 2\, b_1 c_2 - 2\, b_2 c_1 \end{array}} \right)$$

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. Die zurückgegebene rationale Funktion stellt somit eine *Funktionstransformation* gegenüber dem vorherigen geschachtelten Funktionsaufruf dar, mit dessen Hilfe sich die genannten Parameter *direkt* berechnen lassen. Der Definitionsbereich der simplifizierten rationalen Funktion kann allerdings größer sein als der der Ausgangsfunktion.

Wir können diese Rechnungen nun für die Aufgaben aus dem vorigen Abschnitt mit symbolischen Eingabewerten ausführen (siehe `geo.2`)

In all diesen Beispielen simplifizierte der zusammengesetzte rationale Ausdruck, manchmal mit einiger Mühe, zu Null. Wir können in diesem Fall also schlussfolgern, dass diese Bedingung für alle zulässigen Parameterspezifikationen, d.h. solche, wo in den auftretenden Nennern nicht durch 0 geteilt wird, erfüllt ist. Auf diesem Wege erhalten wir bereits allgemeingültige Beweise für eine Reihe der oben betrachteten Geometrie-Theoreme.

`geo.2a` enthält weitere Beispiele.

Für geometrische Sachverhalte, die sich analytisch in die beschriebene Form bringen lassen, gibt es 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 `intersection_point` und `choose_pl`, wo die entsprechenden Nenner nicht verschwinden dürfen. Eine Modifikation der Funktionen erlaubt es, die (Zähler der) entsprechenden Nichtdegenerationsbedingungen in einer global definierten Liste aufzusammeln.

2.4 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 geometrischen 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* $f \in R,\ f \neq 0$, 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 geometrischer 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 11 *(Über das mechanisierte Beweisen geometrischer Sätze vom konstruktiven Typ):*
Eine geometrische Behauptung g vom konstruktiven Typ in einer 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. $\phi_K(g) \neq 0$. $\square$

Die Aussage des Satzes, dass eine rationale Funktion, die “fast” überall verschwindet, zu $0 \in K$ simplifiziert, ist nicht sehr überraschend. Die Hürden dieses Konzepts sind in Punkt 3) enthalten, wo die Definition eines elementaren Konstruktionsschrittes nur durch Eigenschaften, die garantiert werden müssen, eingeschränkt wird. Hier sind bei jeder Erweiterung unseres bisher entwickelten Instrumentariums Beweise zu erbringen.

3 Geometrische Sätze vom Gleichungstyp

Der bisher betrachtete Mechanisierungsansatz für Geometrietheoreme ging davon aus, dass man einen gegebenen Satz der Geometrie in eine konstruktive Form überführen kann. Das ist aber eine für geometrische Aussagen eher untypische Situation. Die meisten geometrischen Sätze gehen von einer bestimmten (konstruktiv gegebenen) geometrischen Konfiguration aus und behaupten dann:

> *Wenn* gewisse geometrische Voraussetzungen erfüllt sind, *dann* ergeben sich daraus gewisse Konsequenzen.

So behauptet etwa der *Satz des Ceva*:

Gegeben sei ein Dreieck ABC und Punkte

$$D = \texttt{varpoint}(B,C,u),\; E = \texttt{varpoint}(C,A,v),\; F = \texttt{varpoint}(A,B,w)$$

auf den Dreiecksseiten. Wenn AD, BE und CF konkurrent sind, so gilt

$$u\,v\,w = (1-u)\,(1-v)\,(1-w)$$

(und umgekehrt).

Eine wortwörtliche Übertragung der Formulierung in die im vorigen Abschnitt entwickelte Sprache lautet:

```
A:=Point(a1,a2); B:=Point(b1,b2); C:=Point(c1,c2);
D:=varpoint(B,C,u);
E_:=varpoint(C,A,v);
F:=varpoint(A,B,w);

pre:=is_concurrent(pp_line(A,D),pp_line(B,E_),pp_line(C,F));
con:=u*v*w-(1-u)*(1-v)*(1-w);
```

In der gegebenen Konfiguration, die generisch durch die 6 Koordinaten von A, B, C und die baryzentrischen Parameter u, v, w von D, E, F beschrieben wird, ist also zu zeigen, dass jede Nullstelle des Polynoms *pre* (der Voraussetzung = presumtio) auch eine Nullstelle des Polynoms *con* (der Schlussfolgerung = conclusio) ist. In diesem Fall lässt sich *pre* in die drei Faktoren

$$\begin{aligned}
f_1 &= -a_1\,b_2 + a_1\,c_2 + a_2\,b_1 - a_2\,c_1 - b_1\,c_2 + b_2\,c_1,\\
f_2 &= a_1\,b_2 - a_1\,c_2 - a_2\,b_1 + a_2\,c_1 + b_1\,c_2 - b_2\,c_1,\\
f_3 &= 2\,u\,v\,w - u\,v - u\,w + u - v\,w + v + w - 1
\end{aligned}$$

zerlegen, von denen nur der dritte mit *con* übereinstimmt, so dass es auch Spezifikationen gibt, in denen *pre* verschwindet, *con* jedoch nicht.

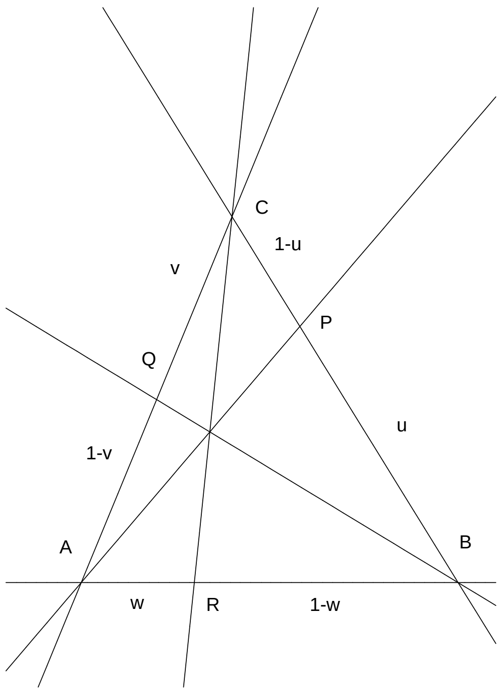

Bild 3.1: Der Satz des Ceva

Analysiert man die beiden anderen Faktoren genauer, so erkennt man, dass sie genau der Bedingung `is_collinear(A,B,C)` entsprechen. Eine Spezifikation, in der dieses Polynom verschwindet, wäre also eine *degenerierte Lage*, so dass wir sehen, dass die beiden Polynome *pre* und *con* "im Wesentlichen" übereinstimmen. Der Satz des Ceva gilt also für alle (nicht degenerierten) Dreiecke.

Ähnlich können wir auch die Aussage des Satzes von Desargue formulieren. Hier sind 6 Punkte $A, \ldots, F$ gegeben. Die Voraussetzung besteht aus drei geometrischen Bedingungen, dass in den Dreiecken ABC und DEF einander entsprechende Geraden zueinander parallel sind. Die Behauptung lautet, dass dann die Geraden AD, BE und CF konkurrent sind:

```
A:=Point(a1,a2); B:=Point(b1,b2); C:=Point(c1,c2);
D:=Point(d1,d2); E_:=Point(e1,e2); F:=Point(f1,f2);

pre:={ is_parallel(pp_line(A,B),pp_line(D,E_)),
        is_parallel(pp_line(B,C),pp_line(E_,F)),
        is_parallel(pp_line(A,C),pp_line(D,F))};

con:=is_concurrent(pp_line(A,D),pp_line(B,E_),pp_line(C,F));
```

Die Voraussetzung entspricht hier also einer Menge von drei Polynomen

$$\begin{array}{l}\{a_1\,d_2 - a_1\,e_2 - a_2\,d_1 + a_2\,e_1 - b_1\,d_2 + b_1\,e_2 + b_2\,d_1 - b_2\,e_1,\\ b_1\,e_2 - b_1\,f_2 - b_2\,e_1 + b_2\,f_1 - c_1\,e_2 + c_1\,f_2 + c_2\,e_1 - c_2\,f_1,\\ a_1\,d_2 - a_1\,f_2 - a_2\,d_1 + a_2\,f_1 - c_1\,d_2 + c_1\,f_2 + c_2\,d_1 - c_2\,f_1\},\end{array}$$

die Behauptung dem deutlich komplizierteren Polynom

$$\begin{array}{l}-a_1\,b_1\,c_2\,d_2 + a_1\,b_1\,c_2\,e_2 + a_1\,b_1\,d_2\,f_2 - a_1\,b_1\,e_2\,f_2 + a_1\,b_2\,c_1\,d_2 - a_1\,b_2\,c_1\,f_2 - a_1\,b_2\,c_2\,e_1 +\\ a_1\,b_2\,c_2\,f_1 - a_1\,b_2\,d_2\,f_1 + a_1\,b_2\,e_1\,f_2 - a_1\,c_1\,d_2\,e_2 + a_1\,c_1\,e_2\,f_2 + a_1\,c_2\,d_2\,e_1 - a_1\,c_2\,e_2\,f_1 -\\ a_1\,d_2\,e_1\,f_2 + a_1\,d_2\,e_2\,f_1 - a_2\,b_1\,c_1\,e_2 + a_2\,b_1\,c_1\,f_2 + a_2\,b_1\,c_2\,d_1 - a_2\,b_1\,c_2\,f_1 - a_2\,b_1\,d_1\,f_2 +\\ a_2\,b_1\,e_2\,f_1 - a_2\,b_2\,c_1\,d_1 + a_2\,b_2\,c_1\,e_1 + a_2\,b_2\,d_1\,f_1 - a_2\,b_2\,e_1\,f_1 + a_2\,c_1\,d_1\,e_2 - a_2\,c_1\,e_1\,f_2 -\\ a_2\,c_2\,d_1\,e_1 + a_2\,c_2\,e_1\,f_1 + a_2\,d_1\,e_1\,f_2 - a_2\,d_1\,e_2\,f_1 + b_1\,c_1\,d_2\,e_2 - b_1\,c_1\,d_2\,f_2 - b_1\,c_2\,d_1\,e_2 +\\ b_1\,c_2\,d_2\,f_1 + b_1\,d_1\,e_2\,f_2 - b_1\,d_2\,e_2\,f_1 + b_2\,c_1\,d_1\,f_2 - b_2\,c_1\,d_2\,e_1 + b_2\,c_2\,d_1\,e_1 - b_2\,c_2\,d_1\,f_1 -\\ b_2\,d_1\,e_1\,f_2 + b_2\,d_2\,e_1\,f_1 - c_1\,d_1\,e_2\,f_2 + c_1\,d_2\,e_1\,f_2 + c_2\,d_1\,e_2\,f_1 - c_2\,d_2\,e_1\,f_1\end{array}$$

Dass jede gemeinsame Nullstelle der Polynome *pre* eine Nullstelle von *con* ist, ist hier nicht mehr so einfach zu erkennen. Wählen wir ein spezielles Koordinatensystem

```
A:=Point(0,0); B:=Point(0,1); C:=Point(1,0);
```

so erhalten wir als Voraussetzung

$$pre = \{d_1 - e_1, -e_1 - e_2 + f_1 + f_2, -d_2 + f_2\}$$

und als Behauptung

$$con = -d_1\,e_1\,f_2 - d_1\,e_2\,f_2 + d_1\,f_2 + d_2\,e_1\,f_1 + d_2\,e_1\,f_2 - d_2\,e_1.$$

Für eine gemeinsame Nullstelle der Voraussetzungen gilt insbesondere $d_1 = e_1$ und $d_2 = f_2$. In die Behauptung eingesetzt erhalten wir

```
sub(d1=e1,d2=f2,con);
```

$$-{e_1}^2\,f_2 - e_1\,e_2\,f_2 + e_1\,f_1\,f_2 + e_1\,{f_2}^2 = e_1\,f_2(-e_1 - e_2 + f_1 + f_2)$$

woran wir erkennen, dass jede gemeinsame Nullstelle von *pre* auch eine Nullstelle von *con* ist.
Aufgabe 11:

Formulieren und untersuchen Sie auf dieselbe Weise den Satz des Pappus.

Wir sehen also, dass die algebraische Formulierung geometrischer Sätze normalerweise auf eine Situation führt, wo die Voraussetzungen einer Menge $pre = \{f_1, \ldots, f_m\} \subset R$ von Polynomen und die Behauptung in einem Polynom $con = g \in R$ codiert werden können, so dass für jede Spezifikation ϕ, die eine gemeinsame Nullstelle von *pre* beschreibt (und evtl. noch einer Nichtdegenerationsbedingung $\phi_R(g) \neq 0$ mit oft vorher nicht bekanntem g genügt), auch $\phi_R(h) = 0$ gilt.

3.1 Nichtlineare geometrische Bedingungen

Mit diesem Ansatz können wir nun auch nichtlineare geometrische Bedingungen erfassen. Diese Bedingungen treten auf, wenn sich schneidende geometrische Linien mehrere Schnittpunkte haben (Schnitt zweier Kreise, Schnitt von Kreis und Gerade) oder wenn es mehrere Geraden mit einer gegebenen Eigenschaft gibt (Parallelenpaar zu einer gegebenen Geraden in gegebenem Abstand, Winkelhalbierendenpaar eines gegebenen Winkels). Diese können ihrem Wesen nach nicht konstruktiver Natur sein, da dort in jedem Schritt ein *eindeutig bestimmtes* geometrisches Objekt konstruiert wurde.

Betrachten wir zunächst, wie sich die eben aufgelisteten geometrischen Bedingungen durch die Koordinaten der an ihnen beteiligten geometrischen Objekte beschreiben lassen.

Punkte auf einem Kreis

Ähnlich wie eine Gerade kann man einen Kreis durch die Koordinaten seines Mittelpunkts und seinen Radius beschreiben. Wir wollen im folgenden, wenn wir einen Kreis als geometrisches Objekt explizit angeben werden, statt des Radius dessen Quadrat, den *Sq-Radius*, verwenden, um nicht bereits an dieser Stelle Wurzelausdrücke zu erzeugen.

Als Objekt der analytischen Geometrie wird ein solcher Kreis durch seine Gleichung

$$(x - x_0)^2 + (y - y_0)^2 - r^2 = (x^2 + y^2) + c_2\, x + c_3\, y + c_4$$

mit $c_2 = -2\, x_0,\ c_3 = -2\, y_0,\ c_4 = x_0^2 + y_0^2 - r^2$ gegeben, die durch die drei Parameter $c = (c_2, c_3, c_4)$ eindeutig charakterisiert werden kann. Umgekehrt lassen sich aus den Kreisparametern (c_2, c_3, c_4) auch Zentrum (x_0, y_0) und Sqradius r^2 unmittelbar polynomial zurückgewinnen.

Aufgabe 12:

> Geben Sie entsprechende Funktionen `circle_center(c:Circle):Point` und `circle_sqradius(c:Circle):Scalar` an. Definieren Sie weiter eine Funktion `circle1(M:Point, A:Point):Circle` für den Kreis mit Zentrum M und Punkt A auf der Peripherie.

Bestimmen wir nun den Kreis, der durch drei vorgegebene Punkte A, B, C verläuft. Formeln für die Koordinaten des Mittelpunkts $M = (m_1, m_2)$ dieses Kreises können wir aus den Gleichungen

```
A:=Point(a1,a2); B:=Point(b1,b2); C:=Point(c1,c2); M:=Point(m1,m2);
polys:={sqrdist(M,A)-sqrdist(M,B), sqrdist(M,A)-sqrdist(M,C)};
```

bestimmen, wenn wir für A, B, C entsprechende *allgemeine* Punkte (AGO's) einsetzen. Das entsprechende Gleichungssystem

$$2 \cdot m_1 \cdot (-a_1 + b_1) + 2 \cdot m_2 \cdot (-a_2 + b_2) + a_1^2 + a_2^2 - b_1^2 - b_2^2 = 0,$$
$$2 \cdot m_1 \cdot (-a_1 + c_1) + 2 \cdot m_2 \cdot (-a_2 + c_2) + a_1^2 + a_2^2 - c_1^2 - c_2^2 = 0$$

ist linear in (m_1, m_2) und besitzt eine eindeutige Lösung genau dann, wenn die zugehörige Determinante, die wieder einmal genau mit der Kollinearitätsbedingung `is_collinear(A,B,C)` übereinstimmt, verschieden von 0 ist.

```
solve(polys,{m1,m2});
```

ergibt dann die gesuchten Mittelpunktskoordinaten, die wir nun fest als Prozedur zur weiteren Verwendung einbrennen können. Alternativ hätten wir den Mittelpunkt natürlich auch wie bisher berechnen können:

```
M:=intersection_point(midpoint_perpendicular(B,C), midpoint_perpendicular(C,A));
```

Für den Kreis durch drei vorgegebene Punkte A, B, C erhalten wir

$$\left(\frac{-a_1^2 b_2 + a_1^2 c_2 - a_2^2 b_2 + a_2^2 c_2 + a_2 b_1^2 + a_2 b_2^2 - a_2 c_1^2 - a_2 c_2^2 - b_1^2 c_2 - b_2^2 c_2 + b_2 c_1^2 + b_2 c_2^2}{D}, \right.$$

$$\frac{a_1^2 b_1 - a_1^2 c_1 - a_1 b_1^2 - a_1 b_2^2 + a_1 c_1^2 + a_1 c_2^2 + a_2^2 b_1 - a_2^2 c_1 + b_1^2 c_1 - b_1 c_1^2 - b_1 c_2^2 + b_2^2 c_1}{D},$$

$$\left. \frac{-a_1^2 b_1 c_2 + a_1^2 b_2 c_1 + a_1 b_1^2 c_2 + a_1 b_2^2 c_2 - a_1 b_2 c_1^2 - a_1 b_2 c_2^2 - a_2^2 b_1 c_2 + a_2^2 b_2 c_1 - a_2 b_1^2 c_1 + a_2 b_1 c_1^2 + a_2 b_1 c_2^2 - a_2 b_2^2 c_1}{D} \right)$$

mit $D = a_1 b_2 - a_1 c_2 - a_2 b_1 + a_2 c_1 + b_1 c_2 - b_2 c_1$. Die Parameter dieses Kreises sind rationale Funktionen der Parameter der Punkte A, B, C, wobei im Nenner wiederum das Polynom $D =$`is_collinear(A,B,C)` auftritt. Um solche Nenner zu vermeiden, wollen wir ähnlich wie für Geraden, auch für Kreise homogene Koordinaten verwenden, d.h. einen Kreis durch ein Tupel $c = (c_1, c_2, c_3, c_4)$ charakterisieren, das für die Punktmenge

$$\{(x, y)\ :\ c_1(x^2 + y^2) + c_2\, x + c_3\, y + c_4 = 0\}$$

steht.

Wir wollen als nächstes charakterisieren, wann 4 Punkte A, B, C, D auf einer gemeinsamen Kreislinie liegen. Mit den oben berechneten Koordinaten des Umkreismittelpunkts M von ABC ergibt sich die gesuchte Bedingung aus

```
D:=Point(d1,d2);
con:=sqrdist(M,A)-sqrdist(M,D);
```

als Zähler $p =$ `num(con)` der (gekürzten) rationalen Funktion *con*. Dieses Zählerpolynom p ist ein Polynom vierten Grades, das die entsprechende Bedingung beschreibt. Wir können auch dieses Polynom extrahieren und als Prozedur zur weiteren Verwendung in unsere Programmsammlung aufnehmen.

Satz 12 *Vier Punkte $A = (a_1, a_2), B = (b_1, b_2), C = (c_1, c_2), D = (d_1, d_2)$ liegen genau dann auf einem gemeinsamen Kreis, wenn*

$$a_1{}^2\,b_1\,c_2 - a_1{}^2\,b_1\,d_2 - a_1{}^2\,b_2\,c_1 + a_1{}^2\,b_2\,d_1 + a_1{}^2\,c_1\,d_2 - a_1{}^2\,c_2\,d_1 - a_1\,b_1{}^2\,c_2 + a_1\,b_1{}^2\,d_2 -$$
$$a_1\,b_2{}^2\,c_2 + a_1\,b_2{}^2\,d_2 + a_1\,b_2\,c_1{}^2 + a_1\,b_2\,c_2{}^2 - a_1\,b_2\,d_1{}^2 - a_1\,b_2\,d_2{}^2 - a_1\,c_1{}^2\,d_2 - a_1\,c_2{}^2\,d_2 +$$
$$a_1\,c_2\,d_1{}^2 + a_1\,c_2\,d_2{}^2 + a_2{}^2\,b_1\,c_2 - a_2{}^2\,b_1\,d_2 - a_2{}^2\,b_2\,c_1 + a_2{}^2\,b_2\,d_1 + a_2{}^2\,c_1\,d_2 - a_2{}^2\,c_2\,d_1 +$$
$$a_2\,b_1{}^2\,c_1 - a_2\,b_1{}^2\,d_1 - a_2\,b_1\,c_1{}^2 - a_2\,b_1\,c_2{}^2 + a_2\,b_1\,d_1{}^2 + a_2\,b_1\,d_2{}^2 + a_2\,b_2{}^2\,c_1 - a_2\,b_2{}^2\,d_1 +$$
$$a_2\,c_1{}^2\,d_1 - a_2\,c_1\,d_1{}^2 - a_2\,c_1\,d_2{}^2 + a_2\,c_2{}^2\,d_1 - b_1{}^2\,c_1\,d_2 + b_1{}^2\,c_2\,d_1 + b_1\,c_1{}^2\,d_2 + b_1\,c_2{}^2\,d_2 -$$
$$b_1\,c_2\,d_1{}^2 - b_1\,c_2\,d_2{}^2 - b_2{}^2\,c_1\,d_2 + b_2{}^2\,c_2\,d_1 - b_2\,c_1{}^2\,d_1 + b_2\,c_1\,d_1{}^2 + b_2\,c_1\,d_2{}^2 - b_2\,c_2{}^2\,d_1$$

gilt.

Diese Bedingung kann man auch als Determinante schreiben: Vier Punkte $A = (a_1, a_2), B = (b_1, b_2), C = (c_1, c_2), D = (d_1, d_2)$ liegen genau dann auf einem gemeinsamen Kreis, wenn es eine nichttriviale Lösung $x = (x_1, x_2, x_3, x_4)$ des Gleichungssystems

$$\begin{aligned} x_1(a_1^2 + a_2^2) + x_2\,a_1 + x_3\,a_2 + x_4 = 0 \\ x_1(b_1^2 + b_2^2) + x_2\,b_1 + x_3\,b_2 + x_4 = 0 \\ x_1(c_1^2 + c_2^2) + x_2\,c_1 + x_3\,c_2 + x_4 = 0 \\ x_1(d_1^2 + d_2^2) + x_2\,d_1 + x_3\,d_2 + x_4 = 0 \end{aligned}$$

gibt, d.h. wenn

$$\begin{vmatrix} (a_1^2 + a_2^2) & a_1 & a_2 & 1 \\ (b_1^2 + b_2^2) & b_1 & b_2 & 1 \\ (c_1^2 + c_2^2) & c_1 & c_2 & 1 \\ (d_1^2 + d_2^2) & d_1 & d_2 & 1 \end{vmatrix} = 0$$

gilt.

Damit können wir bereits den **Satz von der Simsonschen Geraden** beweisen. Seien A, B, C, D vier Punkte wie eben betrachtet und

```
R:=pedalpoint(D,pp_line(B,C));
S:=pedalpoint(D,pp_line(A,C));
T:=pedalpoint(D,pp_line(A,B));
```

die Fußpunkte der Lote aus D auf die drei Seiten des Dreiecks ABC oder deren Verlängerungen. Der Satz von der Simsonschen Geraden behauptet, dass für einen Punkt D auf dem Umkreis von ABC die Lotfußpunkte R, S, T kollinear sind. Die Voraussetzung wird genau durch das oben hergeleitete Polynom p 4. Grades charakterisiert. Die Behauptung

```
con:=is_collinear(R,S,T);
```

ist eine rationale Funktion, deren Zähler ein Polynom 8. Grades mit 576 Summanden enthält und dessen Nenner aus dem Produkt

$$sqrdist(A, B) * sqrdist(B, C) * sqrdist(A, C)$$

besteht. Das Zählerpolynom lässt sich seinerseits in das Produkt

$$collinear(A, B, C)^2 * p$$

zerlegen, woraus der geforderte Beweis nunmehr leicht abzuleiten ist. Aus dem Beweis folgt, dass nicht nur der Satz selbst richtig ist, sondern auch dessen Umkehrung gilt: Sind die Lotfußpunkte R, S, T kollinear, so liegt D auf dem Umkreis des Dreiecks ABC.

Auf ähnliche Weise kann man auch den folgenden Satz herleiten.

Satz 13 (Satz des Ptolemäus) *Das Viereck $ABCD$ ist genau dann ein Sehnenviereck, wenn für die Seitenlängen a, b, c, d und die Diagonalenlängen e, f die Beziehung*

$$a\,c + b\,d = e\,f$$

gilt.

Dieser Satz macht in seiner Formulierung zum einen von der speziellen Lage der Punkte auf der Kreislinie Gebrauch (ansonsten kann man die Vierecksseiten nicht von den Diagonalen unterscheiden) und verwendet zum anderen mit den Seitenlängen Größen, die sich nicht polynomial durch die Koordinaten der Eckpunkte ausdrücken lassen. Eine zur Ausgangsbedingung äquivalente Aussage, die besser in unser Konzept passt, erhält man, wenn man die Behauptung wie folgt umformt:

$$(a\,c)^2 + (b\,d)^2 - (e\,f)^2 = 2\,a\,b\,c\,d$$
$$((a\,c)^2 + (b\,d)^2 - (e\,f)^2)^2 - (2\,a\,b\,c\,d)^2 = 0$$

Ausmultiplizieren liefert die Gleichung

$$a^4\,c^4 - 2\,a^2\,b^2\,c^2\,d^2 - 2\,a^2\,c^2\,e^2\,f^2 + b^4\,d^4 - 2\,b^2\,d^2\,e^2\,f^2 + e^4\,f^4 = 0,$$

in der nur noch Quadrate von Seitenlängen vorkommen und die zudem nunmehr symmetrisch in den drei Paaren gegenüberliegender Strecken ist. Ersetzen wir diese Quadrate durch die entsprechenden Abstandsquadrate `sqrdist(A,B)`, `sqrdist(B,C)`, `sqrdist(C,D)`, `sqrdist(D,A)`, `sqrdist(A,C)` und `sqrdist(B,D)`, so erhalten wir ein Polynom 8. Grades mit 962 Summanden, das genau das Quadrat des Polynoms p ist.

Betrachten wir schließlich noch den **Satz vom Miquelschen Punkt**. Die zugehörige allgemeine geometrische Konfiguration (Dreieck ABC mit Punkten R, S, T auf den Dreiecksseiten) lässt sich wie folgt angeben:

```
A:=Point(a1,a2); B:=Point(b1,b2); C:=Point(c1,c2);
R:=varpoint(B,C,u1);
S:=varpoint(A,C,u2);
T:=varpoint(A,B,u3);
```

Zum Beweis des Satzes bestimmen wir (zur Vereinfachung wieder mit einem speziell positionierten Koordinatensystem) die Koordinaten des Schnittpunkts $P = (x_1, x_2)$ zweier der Kreise und zeigen, dass dieser Punkt auch auf dem dritten Kreis liegt:

```
A:=Point(0,0); B:=Point(0,b2); C:=Point(c1,c2);
R:=varpoint(B,C,u1);
S:=varpoint(A,C,u2);
T:=varpoint(A,B,u3);

P:=Point(x1,x2);
polys:={is_p4_circle(A,S,T,P), is_p4_circle(B,R,T,P)};

sol:=solve(polys,{x1,x2});
```

Wir erhalten zwei Lösungen, deren Koordinaten jeweils rationale Funktionen in den Parametern sind. Eine der beiden Lösungen ist der Punkt T, von dem wir bereits wissen, dass er zu beiden Kreisen gehört. Der zweite Punkt ist der gesuchte Schnittpunkt P (seine rationalen Koordinaten haben 38 bzw. 17 Zählerterme und 42 Nennerterme). Er liegt auf dem dritten Kreis, wie die folgende Rechnung zeigt.

```
P0:=sub(first sol,P);
is_p4_circle(C,R,S,P0);
```

Es ist nicht verwunderlich, dass die Schnittpunktkoordinaten von P rationale Funktionen in den Parametern sind, wenn einer der beiden Schnittpunkte bekannt ist, da die Schnittpunktbedingung auf eine Gleichung zweiten Grades hinausläuft.

Aufgabe 13:

Finden Sie allgemein Formeln für folgende Funktionen:

- `other_cl_point(c:Circle,l:Line,P:Point):Point`, die zu gegebenem Kreis c und gegebener Gerade l den zweiten Schnittpunkt von c und l findet, wenn P der andere Schnittpunkt ist.
- `other_cc_point(c1:Circle,c2:Circle,P:Point):Point`, die zu zwei gegebenen Kreisen c_1 und c_2 den zweiten Schnittpunkt von c_1 und c_2 findet, wenn P der andere Schnittpunkt ist.

Im Gegensatz zu obigem Beispiel lassen sich im Allgemeinen die Schnittpunktkoordinaten zweier Kreise oder von Kreis und Gerade nicht rational durch die Ausgangskoordinaten ausdrücken. So erhalten wir etwa für die Schnittpunkte zweier Kreise mit den Radien r_1 und r_2 und dem Mittelpunktsabstand $2u$ als Bedingung an die Koordinaten des Schnittpunkts $P = (x_1, x_2)$ das Gleichungssystem

```
P:=Point(x1,x2);
polys:={
    is_point_on_circle(P,circle1(Point(-u,0),Point(-u-r1,0))),
    is_point_on_circle(P,circle1(Point(u,0),Point(u+r2,0)))};
```

$$\{-{r_1}^2 + u^2 + 2\,u\,x_1 + {x_1}^2 + {x_2}^2, -{r_2}^2 + u^2 - 2\,u\,x_1 + {x_1}^2 + {x_2}^2\},$$

zu dessen Lösung

```
solve(polys,{x1,x2});
```

$$x = \frac{{r_1}^2 - {r_2}^2}{4\,u},\ y = \pm\frac{\sqrt{-{r_1}^4 + 2\,{r_1}^2\,{r_2}^2 + 8\,{r_1}^2\,u^2 - {r_2}^4 + 8\,{r_2}^2\,u^2 - 16\,u^4}}{4\,u}$$

bereits Wurzelausdrücke erforderlich sind.

Winkel und Winkelhalbierende

Nichtlineare Bedinungen erhalten wir ebenfalls im Zusammenhang mit Winkelhalbierenden, da es zu zwei gegebenen Geraden g, h stets zwei (zueinander senkrechte) Winkelhalbierende gibt.

Um eine Bedingung herzuleiten, die beschreibt, wann ein Punkt P auf einer der beiden Winkelhalbierenden liegt, betrachten wir die beiden Anstiege der Geraden $g = (g_1, g_2, g_3)$ und $h = (h_1, h_2, h_3)$. Der Tangens des entsprechenden Winkels lässt sich durch das Verhältnis $\frac{g_2}{g_1}$ bzw. $\frac{h_2}{h_1}$ ausdrücken. Für den Tangens des Winkels zwischen diesen beiden Geraden erhalten wir dann

$$\tan(\angle(g,h)) = \tan(\alpha_2 - \alpha_1) = \frac{\tan(\alpha_2) - \tan(\alpha_1)}{1 + \tan(\alpha_1)\tan(\alpha_2)} = \frac{g_1\,h_2 - g_2\,h_1}{g_1\,h_1 + g_2\,h_2}$$

Dieser Ausdruck ist nicht definiert, wenn der Nenner verschwindet, also die beiden Geraden g und h senkrecht aufeinander stehen.

P ergibt sich damit aus der Bedingung

```
u:=angle(pp_line(A,B),pp_line(P,B));
v:=angle(pp_line(P,B),pp_line(C,B));

u - v;
```

von der wiederum nur der Zähler `poly:=num(u-v)` von Interesse ist, ähnlich der Unterscheidung zwischen geometrisch und algebraisch parallelen Geraden. Die entsprechende Bedingung ist ein Polynom vom Grad 2 in x und y, das für allgemeine Punkte A, B, C 56 Terme enthält.

Dieser Ausdruck beschreibt zwei zueinander senkrechte Geraden v und w, deren Parameter sich vielleicht durch Faktorisieren aus diesem Polynom

$$poly = (v_1 x + v_2 y + v_3)(w_1 x + w_2 y + w_3)$$

gewinnen lassen. Eine einfache Faktorisierung des Polynoms führt allerdings nicht zum gewünschten Ergebnis. Zur genaueren Analyse extrahieren wir durch Koeffizientenvergleich ein Gleichungssystem für die Geradenparameter und untersuchen dessen Lösungen. Wir erkennen, dass bei der Beschreibung dieser Lösungen, ähnlich wie für die Koordinaten der Schnittpunkte zweier Kreise, Wurzelausdrücke auftreten, sich die beiden Winkelhalbierenden über dem Grundkörper also nicht gut genug voneinander unterscheiden lassen. Wir können also die Winkelhalbierenden nicht direkt als Geraden beschreiben, sondern verfügen nur über eine Prozedur

```
algebraic procedure is_point_on_bisector(P,A,B,C);
  begin scalar u,v;
  u:=angle(pp_line(A,B),pp_line(P,B));
  v:=angle(pp_line(P,B),pp_line(C,B));
  return (num(u)*den(v)-den(u)*num(v));
  end;
```

mit der geprüft werden kann, ob ein gegebener Punkt P auf einer der beiden Winkelhalbierenden liegt.

Aufgabe 14:

> Vier Punkte A, B, C, D liegen nach der Umkehrung des Peripheriewinkelsatzes auf einem Kreis, wenn B und D auf demselben Bogen AC liegen und $\angle ABC = \angle ADC$ gilt.
>
> Zeigen Sie, dass diese Bedingung genau auf das oben hergeleitete Polynom vierten Grades führt.
>
> Diskutieren Sie den Fall, dass B und D auf unterschiedlichen Bögen AC liegen. (Hinweis: Beachten Sie, dass $\tan(-\alpha) = -\tan(\alpha)$ gilt, also mit *orientierten* Winkeln zu rechnen ist.)

Um den **Satz vom Schnittpunkt der Winkelhalbierenden** zu beweisen, können wir wieder zunächst die Koordinaten des Schnittpunkts $P = (x_1, x_2)$ von zwei der drei Winkelhalbierenden bestimmen und dann prüfen, ob P auch auf der dritten Winkelhalbierenden liegt. Zur Vereinfachung der Rechnung fixieren wir ein spezielles Koodinatensystem, in dem die Eckpunkte des Dreiecks die folgenden Koordinaten haben:

```
A:=Point(0,0); B:=Point(0,1); C:=Point(c1,c2); P:=Point(x1,x2);

polys:={is_point_on_bisector(P,B,A,C), is_point_on_bisector(P,C,B,A)};
```

Zur Bestimmung der Koordinaten von P erhalten wir das Gleichungssystem

$$\begin{aligned}&c_1\, {x_1}^2 - c_1\, {x_2}^2 + 2\, c_2\, x_1\, x_2, \\ &c_1\, {x_1}^2 - c_1\, {x_2}^2 + 2\, c_1\, x_2 - c_1 + 2\, c_2\, x_1\, x_2 - 2\, c_2\, x_1 - 2\, x_1\, x_2 + 2\, x_1\end{aligned}$$

aus zwei Gleichungen zweiten Grades, für das Reduce als Lösung

```
sol:=solve(polys,{x1,x2});
```

$$\{x_1 = \mathrm{root\_of}(4\,c_1{}^3\,x_1{}^2 - c_1{}^3 - 8\,c_1{}^2\,x_1{}^3 + 4\,c_1{}^2\,x_1 + 4\,c_1\,c_2{}^2\,x_1{}^2 - 4\,c_1\,c_2\,x_1{}^2 + 4\,c_1\,x_1{}^4$$
$$-4\,c_1\,x_1{}^2 - 8\,c_2{}^2\,x_1{}^3 + 8\,c_2\,x_1{}^3, x_1),$$

$$x_2 = \frac{c_1{}^2\,c_2 + 2\,c_1{}^2\,x_1{}^2 - c_1{}^2 + 2\,c_1\,c_2{}^2\,x_1 - 2\,c_1\,c_2\,x_1 - 2\,c_1\,x_1{}^3 + 2\,c_1\,x_1 + 4\,c_2{}^2\,x_1{}^2 - 4\,c_2\,x_1{}^2}{2\,c_1{}^2\,c_2 - c_1{}^2}\}$$

liefert. x_1 ist eine der vier Wurzeln einer Gleichung 4. Grades, die nicht mehr (effizient) explizit berechnet werden können. x_2 ergibt sich jeweils aus dem zugehörigen Wert von x_1 eindeutig (als rationaler Ausdruck in x_1 und den anderen Parametern) aus der zweiten Gleichung.

Ein ähnliches Ergebnis war auch zu erwarten, denn die zwei *Paare* von Winkelhalbierenden durch A bzw. B haben insgesamt genau 4 Punkte gemeinsam, die Mittelpunkte des Inkreises und der drei Ankreise des Dreiecks ABC. Es ergibt sich nun die Frage, ob jeder der vier Punkte auf einer der beiden Winkelhalbierenden durch C liegt, ob also jede der vier Lösungen auch Nullstelle der Gleichung

```
is_point_on_bisector(P,A,C,B);
```

$$2\,c_1{}^3\,x_2 - c_1{}^3 - 2\,c_1{}^2\,c_2\,x_1 - 2\,c_1{}^2\,x_1\,x_2 + 2\,c_1{}^2\,x_1 + 2\,c_1\,c_2{}^2\,x_2 - c_1\,c_2{}^2 + 2\,c_1\,c_2\,x_1{}^2 -$$
$$2\,c_1\,c_2\,x_2{}^2 - c_1\,x_1{}^2 + c_1\,x_2{}^2 - 2\,c_2{}^3\,x_1 + 2\,c_2{}^2\,x_1\,x_2 + 2\,c_2{}^2\,x_1 - 2\,c_2\,x_1\,x_2$$

ist. Derartige Fragen wollen wir im nächsten Abschnitt genauer formulieren und studieren.

Hier sei noch angemerkt, dass man Winkelhalbierende mit einem anderen Konzept auch als geometrische Objekte vom konstruktiven Typ einführen kann.

AUFGABE 15:

> Zeigen Sie auf folgende Weise, dass sich die Winkelhalbierenden 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.

3.2 Geometrische Sätze vom Gleichungstyp

Alle unsere Geometrietheoreme hatten die folgende Gestalt: Gegeben ist

> eine allgemeine geometrische Konfiguration AGK mit Variablen $\mathbf{x} = (x_1, \ldots, x_n)$,
>
> eine Menge von Polynomen $F = \{f_1, \ldots, f_m\} \subset R := k[x_1, \ldots, x_n]$, die algebraische Abhängigkeiten zwischen den verschiedenen Elementen der gegebenen AGK beschreiben und die wir als *allgemeine geometrische Voraussetzung* (AGV) bezeichnen wollen,
>
> eine (oft nicht explizit gegebene) Nichtdegenerationsbedingung $h(\mathbf{x}) \in R$ sowie
>
> ein Polynom $g(\mathbf{x}) \in R$, das die geometrische Folgerung algebraisch kodiert.

Als *Geometriesatz vom Gleichungstyp* bezeichnen wir dann eine Aussage der folgenden Gestalt:

> Jede gemeinsame Nullstelle $\mathbf{x}_0$ der Polynome aus F, die eine nicht degenerierte (d.h. $h(\mathbf{x}_0) \neq 0$) *spezielle* geometrische Konfiguration beschreibt, in der die durch F gegebenen (zusätzlichen) geometrischen Voraussetzungen erfüllt sind, ist auch eine Nullstelle von g, d.h. erfüllt die geometrische Folgerung.

Wir schreiben für einen solchen Satz auch kurz $(F/h \Rightarrow g)$.

Im folgenden bezeichnen wir mit

$$Z(F) := \{\, \mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{C}^n \ : \ \forall\, f \in F\; f(\mathbf{a}) = 0 \,\}$$

die Menge der gemeinsamen komplexen Nullstellen des Polynomsystems F. Für ein einzelnes Polynom $f \in R$ schreiben wir statt $Z(\{f\})$ auch kurz $Z(f)$. In dieser Notation lässt sich ein Geometrietheorem von Gleichungstyp formulieren als

$$\mathbf{a} \in Z(F) \text{ und } \mathbf{a} \notin Z(h) \ \Rightarrow\ \mathbf{a} \in Z(g) \text{ oder anders: } Z(F) \setminus Z(h) \subseteq Z(g)$$

Wir wollen zunächst die folgenden zwei dazu äquivalenten Formulierungen festhalten:

$$\mathbf{a} \in Z(F) \ \Rightarrow\ \mathbf{a} \in Z(g \cdot h)$$

d.h. eine gemeinsame Nullstelle von F entspricht entweder einer degenerierten geometrischen Situation oder die Behauptung gilt, und

$$\mathbf{a} \in Z(F) \text{ und } \mathbf{a} \notin Z(g) \ \Rightarrow\ \mathbf{a} \in Z(h)$$

d.h. eine gemeinsame Nullstelle von F, in der die Behauptung nicht gilt, entspricht einer degenerierten geometrischen Situation. Man beachte besonders die Symmetrie, mit der g und h in die Formulierungen eingehen.

Da die Nichtdegenerationsbedingungen oft nicht explizit gegeben sind, können wir außer nach Beweisen für konkrete geometrische Sätze auch die Frage nach der "schwächsten" Nichtdegenerationsbedingung stellen, unter der eine gegebene geometrische Aussage noch gilt. Dazu definieren wir die Menge

$$I(F/g) := \{h \in R \ : \ Z(F) \setminus Z(h) \subseteq Z(g)\} = \{h \in R \ : \ Z(F) \subseteq Z(g \cdot h)\}$$

die alle diese Nebenbedingungen auflistet. Es stellt sich im Weiteren heraus, dass diese Menge in Wirklichkeit ein Ideal ist, d.h. eine zusätzliche mathematische Struktur trägt, die es gestattet, sie explizit zu bestimmen.

Betrachten wir zum Abschluss dieses Punktes zwei Möglichkeiten, einen interessanten geometrischen Satz als Satz vom Gleichungstyp zu formulieren. Es handelt sich um das folgende

> **Schmetterlingstheorem** [2, S. 31]:
> Auf einer Kreislinie mit dem Mittelpunkt O seien vier Punkte A, B, C, D gegeben. P sei der Schnittpunkt von AC und BD. Die Senkrechte auf der Verbindungslinie OP schneide die Seiten AB und CD (die "Schmetterlingsflügel") in den Punkten F und G. Dann gilt $PF = PG$.

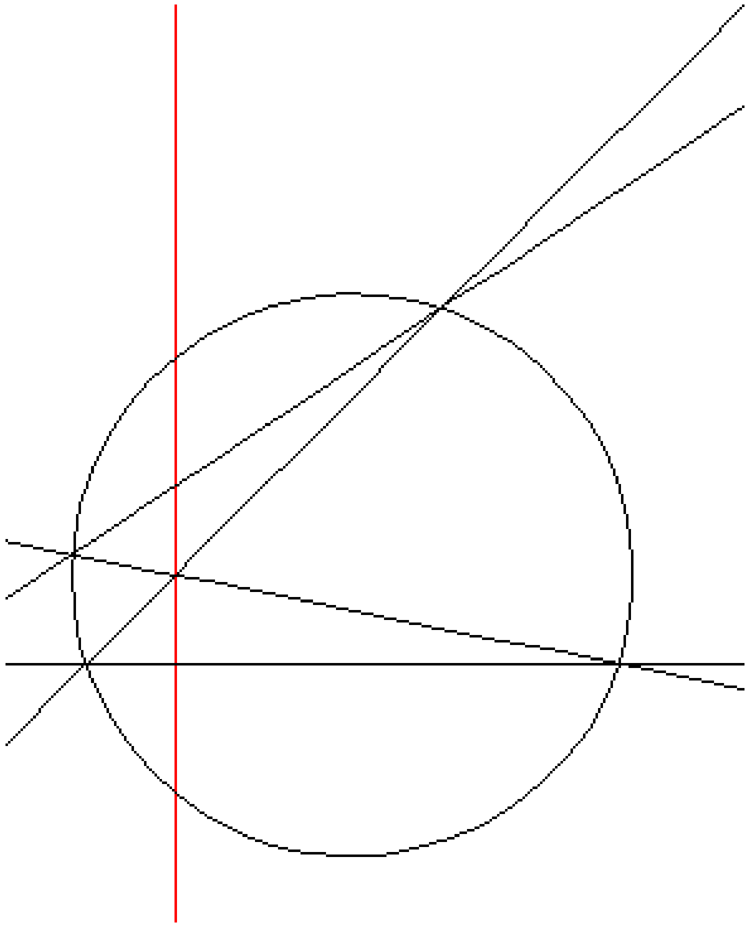

Bild 3.2: Das Schmetterlingstheorem

Wir wollen bei der Herleitung einer algebraischen Form dieses Satzes zugleich zwischen (in einem später zu präzisierenden Sinne) "unabhängigen" Variablen u_i, deren Wert frei wählbar ist, und "abhängigen" Variablen x_i, deren Wert sich eindeutig oder endlich vieldeutig aus den algebraischen Bedingungen und bereits fixierten Werten ergibt, unterscheiden.

Für die erste Version sei O der Koordinatenursprung und $A = (u_1, 0)$ auf der x-Achse gelegen. Die x-Koordinate stimmt damit zugleich mit dem Radius des Kreises überein. B, C und D seien drei weitere Punkte auf dem Kreis. Je eine Koordinate kann frei gewählt werden, die andere ergibt sich aus der Kreisgleichung. Die Punkte seien also $B = (u_2, x_1)$, $C = (u_3, x_2)$ und $D = (u_4, x_3)$. $P = (x_4, x_5)$ ergibt sich dann eindeutig als Schnittpunkt, ebenso wie die Senkrechte h und die Punkte $F = (x_6, x_7)$ und $G = (x_8, x_9)$. Insgesamt erhalten wir folgende algebraische Formulierung

```
O:=Point(0,0); A:=Point(u1,0); B:=Point(u2,x1); C:=Point(u3,x2);
D:=Point(u4,x3); P:=Point(x4,x5);
h:=lot(P,pp_line(O,P));
F:=Point(x6,x7); G:=Point(x8,x9);

polys:={sqrdist(O,B)-u1^2, sqrdist(O,C)-u1^2, sqrdist(O,D)-u1^2,
        is_point_on_line(P,pp_line(A,C)),
        is_point_on_line(P,pp_line(B,D)), is_point_on_line(F,h),
        is_point_on_line(F,pp_line(A,D)), is_point_on_line(G,h),
        is_point_on_line(G,pp_line(B,C))};
```

```
con:=sqrdist(P,F)-sqrdist(P,G);
```

$$
\begin{aligned}
polys = \{ \quad & x_1{}^2 - u_1{}^2 + u_2{}^2, \\
& x_2{}^2 - u_1{}^2 + u_3{}^2, \\
& -u_1{}^2 + u_4{}^2 + x_3{}^2, \\
& -x_2\, u_1 + x_2\, x_4 + u_1\, x_5 - u_3\, x_5, \\
& x_1\, u_4 - x_1\, x_4 - u_2\, x_3 + u_2\, x_5 - u_4\, x_5 + x_3\, x_4, \\
& x_4{}^2 - x_4\, x_6 + x_5{}^2 - x_5\, x_7, \\
& -u_1\, x_3 + u_1\, x_7 - u_4\, x_7 + x_3\, x_6, \\
& x_4{}^2 - x_4\, x_8 + x_5{}^2 - x_5\, x_9, \\
& x_1\, u_3 - x_1\, x_8 - x_2\, u_2 + x_2\, x_8 + u_2\, x_9 - u_3\, x_9\} \\
con = \quad & -2\, x_4\, x_6 + 2\, x_4\, x_8 - 2\, x_5\, x_7 + 2\, x_5\, x_9 + x_6{}^2 + x_7{}^2 - x_8{}^2 - x_9{}^2
\end{aligned}
$$

Die Anzahl der abhängigen Variablen x_i entspricht dabei genau der Anzahl der Gleichungen in der Menge *poly*, allerdings ist nicht so ganz klar, wie man daraus die x_i bestimmen könnte.

In der zweiten Algebraisierung sei P der Koordinatenursprung und die Koordinatenachsen so gelegen, dass O, F und G auf ihnen liegen. O kann dabei in y-Richtung an einer beliebigen Stelle liegen. Ebenso ist A frei wählbar, woraus sich der Radius des Kreises ergibt und B halbbestimmt ist. C und D sind nun vollständig als Schnittpunkte des Kreises mit den Geraden AP bzw. BP determiniert, ebenso die (noch fehlenden) x-Koordinaten der Punkte F und G. Zusammen erhalten wir 7 abhängige Parameter statt 9 wie in der ersten Version (und entsprechend weniger Bestimmungsgleichungen)

```
A:=Point(u1,u2); B:=Point(u3,x1); C:=Point(x2,x3); D:=Point(x4,x5);
P:=Point(0,0); O:=Point(0,u4); F:=Point(x6,0); G:=Point(x7,0);

polys:={sqrdist(O,B)-sqrdist(O,A), sqrdist(O,C)-sqrdist(O,A),
        sqrdist(O,D)-sqrdist(O,A),
is_point_on_line(P,pp_line(A,C)),
        is_point_on_line(P,pp_line(B,D)),
        is_point_on_line(F,pp_line(A,D)),
        is_point_on_line(G,pp_line(B,C))};

con:=sqrdist(P,F)-sqrdist(P,G);
```

$$
\begin{aligned}
polys = \{ \quad & x_1{}^2 - 2\, x_1\, u_4 - u_1{}^2 - u_2{}^2 + 2\, u_2\, u_4 + u_3{}^2, \\
& x_2{}^2 - u_1{}^2 - u_2{}^2 + 2\, u_2\, u_4 - 2\, u_4\, x_3 + x_3{}^2, \\
& -u_1{}^2 - u_2{}^2 + 2\, u_2\, u_4 - 2\, u_4\, x_5 + x_4{}^2 + x_5{}^2, \\
& x_2\, u_2 - u_1\, x_3, \\
& x_1\, x_4 - u_3\, x_5, \\
& -u_1\, x_5 + u_2\, x_4 - u_2\, x_6 + x_5\, x_6, \\
& x_1\, x_2 - x_1\, x_7 - u_3\, x_3 + x_3\, x_7\} \\
con = \quad & x_6{}^2 - x_7{}^2
\end{aligned}
$$

Aufgabe 16:

> Man kann diese Aufgabe auch konstruktiv formulieren, wenn man eine Parametrisierung der Punkte auf der Kreislinie verwendet. Definieren Sie eine entsprechende Funktion `choose_point_on_circle` und finden Sie einen konstruktiven Beweis des Schmetterlingstheorems.

3.3 Ideale und Nullstellengebilde. Der Korrespondenzsatz

Genau wie in der linearen Algebra nicht einzelne Vektoren, sondern die von ihnen erzeugten Unterräume als die unter den wichtigsten Vektor-Operationen invarianten Objekte eine zentrale Rolle spielen, betrachtet man in der nichtlinearen Algebra nicht einzelne Mengen $F \subset R$ von Polynomen, sondern zusammen mit ihnen auch alle daraus polynomial ableitbaren Objekte.

Definition: Als von den Polynomen $f \in F$ erzeugtes Ideal $I(F)$ bezeichnet man die Menge aller polynomialen Linearkombinationen

$$I(F) = \{\sum_{f \in F} r_f\, f \ : \ r_f \in R\}$$

von Elementen aus F.

Da R ein Ring ist, kann man alle angegebenen Operationen ausführen. Es entsteht eine Menge, die abgeschlossen ist bzgl. Addition, Subtraktion und Vervielfachung mit Elementen $r \in R$. Diese Eigenschaft charakterisiert Ideale zugleich. Zur Bestimmung der Nullstellenmenge ist es unerheblich, ob man von der Menge F oder aber vom Ideal $I(F)$ ausgeht.

Auf der Menge $\mathcal{I}(R)$ der Ideale eines Ringes R sind folgende Operationen möglich:

Summe zweier Ideale $I_1, I_2 \in \mathcal{I}(R)$:

$$I_1 + I_2 = \{a + b \in R \ : \ a \in I_1,\ b \in I_2\}$$

Summe zweier Ideale $I_1, I_2 \in \mathcal{I}(R)$:

$$I_1 \cdot I_2 = \{\sum_k a_k \cdot b_k \in R \ : \ a_k \in I_1,\ b_k \in I_2\}$$

Durchschnitt $I_1 \cap I_2$ zweier Ideale $I_1, I_2 \in \mathcal{I}(R)$.

Aufgabe 17:

> Zeigen Sie, dass jede dieser Konstruktionen wieder ein Ideal ergibt. Warum reicht es beim Idealprodukt nicht aus, die Menge aller Produkte zu bilden ?

Es besteht generell ein enger Zusammenhang zwischen Idealen und Nullstellengebilden. Zunächst kann, wie bereits in der linearen Algebra, nicht jede beliebige Menge als Nullstellengebilde eines Ideals auftreten.

Aufgabe 18:

> Zeigen Sie, dass in einem eindimensionalen Raum $\mathbf{A}^1$ nur der Raum selbst sowie jede endliche Teilmenge als Nullstellengebilde auftreten kann.
>
> Zeigen Sie weiter, dass höherdimensionale Nullstellengebilde stets die Eigenschaft besitzen, dass sie von einer Geraden, die nicht ganz in dem Nullstellengebilde enthalten ist, nur in endlich vielen Punkten getroffen werden kann.

Eine Menge, die sich als Nullstellengebilde $V(I)$ eines Ideals darstellen lässt, bezeichnen wir als *affine Varietät.*

Im Gegensatz zur linearen Algebra können *verschiedene* Ideale dieselbe affine Varietät definieren. Das hängt damit zusammen, dass Ideale eigentlich Nullstellenmengen mit deren Vielfachheiten verkörpern. So besteht etwa aus Sicht der Nullstellen kein Unterschied zwischen den Mengen

$F_1 = \{x+1, y-1\}$ und $F_2 = \{(x+1)^2, (y-1)^3\}$, aus Sicht der Ideale schon. Sei deshalb $rad(I)$ das größte Ideal für welches $V(I) = V(rad(I)) \subset \mathbf{A}^n_{\overline{k}}$ über einem algebraisch abgeschlossenen Grundkörper $\overline{k}$ gilt. Dieses Ideal bezeichnet man auch als das *Radikal* von I. Ideale, die mit ihrem Radikal übereinstimmen, bezeichnen wir auch als *Radikalideale*.

Sicher gilt $f \in rad(I)$ für jedes Polynom $f \in R$, von dem eine gewisse Potenz f^k in I liegt. Es stellt sich heraus (Hilberts Nullstellensatz), dass dies das Radikal bereits charakterisiert, d.h. es gilt

$$rad(I) = \{f \in R \;:\; \exists\, k > 0 \;\; f^k \in I\}.$$

Aufgabe 19:

> Zeigen Sie, dass die Menge $\{f \in R \;:\; \exists\, k > 0 \;\; f^k \in I\}$ ein Ideal ist.

Ist $Z \subset \mathbf{A}^n$ eine Teilmenge des affinen Raums, so bezeichnen wir mit

$$I(Z) = \{f \in R \;:\; \forall\, z \in Z \;\; f(z) = 0\}$$

das Radikal-Ideal der Polynome, die auf Z verschwinden.

In der Vorlesung "Gröbnerbasen und deren Anwendungen" hatten wir den folgenden Korrespondenzsatz bewiesen:

Satz 14 *(Korrespondenzsatz) Sei*

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

V und I sind zueinander inverse, inklusionsumkehrende Korrespondenzen zwischen den affinen Varietäten im $\mathbf{A}^n$ und den Radikalidealen in R, die Durchschnitte der Nullstellenmengen in Idealsummen und Vereinigungen der Nullstellenmengen in Idealdurchschnitte überführen, d.h.

1. *die Bilder unter V sind genau die affinen Varietäten im $\mathbf{A}^n$,*
2. *die Bilder unter I sind genau die Radikalideale in R,*
3. *für jede Teilmenge $W \in \mathbf{A}^n$ ist $V(I(W))$ die kleinste affine Varietät, die W umfasst (deren* affiner Abschluss*),*
4. *für jedes Ideal $J \subset R$ gilt $I(V(J)) = rad(J)$,*
5. *$I_1 \subseteq I_2 \Rightarrow V(I_1) \supseteq V(I_2)$,*
6. *$V_1 \subseteq V_2 \Rightarrow I(V_1) \supseteq I(V_2)$.*
7. *$V(I_1 + I_2) = V(I_1) \bigcap V(I_2)$ und*
8. *$V(I_1 \cdot I_2) = V(I_1 \bigcap I_2) = V(I_1) \bigcup V(I_2)$.*

Ohne Beweis. Siehe Vorlesung "Gröbnerbasen und deren Anwendungen".

3.4 Der Zerlegungssatz

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

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

gilt.

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

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

wäre das eine Zerlegung in kleinere Varietäten. Das Verschwindungsideal $I = I(V)$ ist also ein Primideal.

Satz 15 *In einem Polynomring lässt sich jedes Radikalideal als Durchschnitt endlich vieler Primideale darstellen.*

Jede affine Varietät V ist die Vereinigung von endlich vielen irreduziblen Varietäten $V = \cup V_i$.

Ohne Beweis. Siehe Vorlesung "Gröbnerbasen und deren Anwendungen".

Die Teilvarietäten V_i bezeichnet man auch als die *irreduziblen Komponenten* von V.

Beispiel: Satz vom Miquelschen Punkt

Das weiter oben betrachtete System

```
A:=Point(0,0); B:=Point(0,b2); C:=Point(c1,c2);
R:=varpoint(B,C,u1);
S:=varpoint(A,C,u2);
T:=varpoint(A,B,u3);

P:=Point(x1,x2);
polys:={is_p4_circle(A,S,T,P), is_p4_circle(B,R,T,P)};
```

erzeugt ein Ideal $I = I(polys)$, dessen Nullstellengebilde in zwei Komponenten zerfällt. Eine davon ist $V(x_1, x_2 + (b_2u_3 - b_2))$, also der Schnittpunkt $T = (0, -b_2u_3 + b_2)$ der beiden Kreise. Die zweite Komponente, ebenfalls Nullstelle von Gleichungen, die linear in x_1, x_2 sind, besteht gerade aus dem zu untersuchenden Punkt P. Der Satz ist also nur auf einer der beiden Komponenten richtig, die zweite liegt vollkommen im Degenerationslocus.

Diese Situation ist typisch für die meisten Geometriesätze vom Gleichungstyp. Wird etwa die Varietät V durch *eine* Gleichung f gegeben und ist $f = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ die Zerlegung dieses Polynoms in Primfaktoren, so lässt sich die Varietät $V(f)$ zerlegen als

$$V(f) = \bigcup_{i=1}^{k} V(p_i)$$

Die Aufgabenstellung des Satzes von Ceva, die eingangs dieses Kapitels formuliert wurde, führt damit auf eine affine Varietät aus zwei Komponenten, die den Nullstellenmengen der Polynome $2\,u\,v\,w - u\,v - u\,w + u - v\,w + v + w - 1$ und `is_collinear(A,B,C)` entsprechen.

Betrachten wir zum Abschluss noch den Einfluss von Nichtdegenerationsbedingungen. Offensichtlich ist $V(F) \setminus V(h)$ nur in seltenen Fällen wieder eine algebraische Menge. Da die Schlussfolgerung eines Geometrietheorems jedoch ein Polynom $g \in R$ ist, können wir diese Menge durch die kleinste algebraische Menge ersetzen, die $V(F) \setminus V(h)$ enthält, die also vom Ideal $I(V(F) \setminus V(h))$ beschrieben wird. Das ist offensichtlich genau die Menge

$$I(F/h) = \{f \in R \ : \ V(F) \subseteq V(f \cdot h)\} = \{f \in R \ : \ f \cdot h \in rad(I(F))\}.$$

Aufgabe 20:

Zeigen Sie, dass $I(F/h)$ ein Ideal ist.

Ist $J = I(F)$ ein Radikalideal, d.h. $J = rad(J)$, so ist das gerade das Ideal

$$I(J/h) = J \, : \, h = \{f \in R \ : \ f \cdot h \in J\},$$

welches man als den *Idealquotienten* von J nach h bezeichnet. Für ein allgemeines Ideal erhalten wir nach dem Charakterisierungssatz für Radikale

$$I(J/h) = \{f \in R \ : \ \exists\, n > 0 \ (f \cdot h)^n \in J\}.$$

Da man diese Objekte auf der Seite der algebraischen Menge nicht auseinanderhalten kann, mag es nicht verwundern, dass ein drittes Ideal

$$I(J/h) = J \, : \, h^\infty = \{f \in R \ : \ \exists\, n > 0 \ f \cdot h^n \in J\},$$

der *stabile Idealquotient* von J nach h, in geometrischen Argumenten die zentrale Rolle spielt. Stellen wir uns Ideale als Nullstellengebilde mit Vielfachheiten vor, so können wir den stabilen Idealquotienten als solchen verstehen, in dem auch Faktoren h mit höherer Vielfachheit herausdividiert worden sind.

Für die Gültigkeit eines Geometrietheorems vom Gleichungstyp genügt es damit zu zeigen, dass die Schlussfolgerung g zum Ideal $I(F) \, : \, h^\infty$ gehört, was im Fall eines Radikalideals $I(F)$ sogar gleichwertig zur Ausgangsfrage ist.

Wir hatten gesehen, dass die Schlussfolgerung g aus einem Geometrietheorem und dessen Nichtdegenerationsbedingung h vertauscht werden können. So kann man umgekehrt auch aus der Schlussfolgerung g (oft nicht vorab bekannte) Nichtdegenerationsbedingungen gewinnen. Die Menge aller Nichtdegenerationsbedingungen $I(F/g)$ bildet ein Ideal, das man auf dieselbe Weise wie eben diskutiert berechnen kann:

Satz 16 *Die Menge $I(F/g)$ aller Nichtdegenerationsbedingungen h eines geometrischen Satzes $(F = 0 \Rightarrow \ g = 0)$ stimmt mit dem Radikal des stabilen Idealquotienten $J = I(F) : g^\infty$ überein.*

Anders: $V(J)$ ist der Degenerationslocus des Geometrieproblems, d.h. die kleinste affine Varietät, für die $V(F) \setminus V(J) \subset V(g)$ gilt.

Beweis :

$$f \in rad(J) \ \Leftrightarrow \ \exists\, m, n \ : \ (g^n f)^m \in I(F) \ \Leftrightarrow \ \exists\, k \ : \ (gf)^k \in I(F) \ \Leftrightarrow \ V(F) \subseteq V(fg)$$

□

$V(J)$ ist somit die kleinste affine Varietät, so dass für jede Spezifikation $\phi : \ x_i \mapsto c_i$ mit $\phi(\mathbf{x}) \notin V(J)$ und $\phi(f) = 0 \ \forall \ f \in F$ die Schlussfolgerung $\phi(g) = 0$ gilt.

Der Degenerationslocus muss dabei nicht unbedingt eine Hyperfläche $(h = 0)$ sein, sondern kann kleinere Dimension haben. Wegen $V(h) \supset V(J)$ für $h \in J$ kann *jedes* Element aus J als Nichtdegenerationsbedingung verwendet werden. Insbesondere gibt es keine “minimale” Nichtdegenerationsbedingung, wenn das Ideal J kein Hauptideal ist.

3.5 Idealtest, Normalformen und Gröbnerbasen

DEFINITION: Zwei Polynome $f, g \in R$ heißen *kongruent* modulo dem Ideal I, wenn $f - g \in I$ gilt. Wir schreiben in diesem Fall $f \equiv g \ (mod\ I)$.

Mit Kongruenzen kann man genauso rechnen, wie wir das von Restklassen ganzer Zahlen gewohnt sind. Insbesondere gilt $f \in I$, wenn wir $f \equiv 0 \ (mod\ I)$ nachweisen können.

Ist $I = I(F)$ mit der Basis $F = \{f_1, \dots, f_m\}$, so versucht man in praktischen Anwendungen, die aus den Basispolynomen deduzierten Beziehungen $f_i \equiv 0 \ (mod\ I)$ in *Ersetzungsregeln* umzuwandeln. Dazu wählt man einen Term m_i aus f_i aus und stellt das Polynom $f_i = m_i - f_i'$ in der Form $m_i \equiv f_i' \ (mod\ I)$ dar. Nun kann man überall, wo der Term m_i auftritt, diesen durch f_i' ersetzen. Dies ist ebenfalls für alle Termvielfachen $n\, m_i$ von m_i möglich, die dann durch $n\, f_i' \ (mod\ I)$ ersetzt werden. Ersetzungsregeln dieser Form bezeichnen wir als *algebraische Ersetzungsregeln*.

Um die Termination dieses Ersetzungsverfahrens zu sichern, wollen wir (in einem zu spezifizierenden Sinne) stets "größere" durch "kleinere" Terme ersetzen. Wir halten dazu auf dem Termmonoid $T = T(x_1, \dots, x_n)$ eine lineare Ordnung fest. Dann können wir in jedem Polynom

$$0 \neq f = \sum_{\alpha} c_\alpha \mathbf{x}^\alpha \in R$$

den größten Term $lt(f) \in T$, den *Leitterm*, und dessen Koeffizienten $lc(f)$, den *Leitkoeffizienten*, identifizieren und somit unser Polynom als

$$f = lc(f) \cdot lt(f) + red(f)$$

darstellen, wobei $red(f)$, das *Reduktum*, alle anderen Summanden von f, die sämtlich kleiner als $lt(f)$ in der gewählten Ordnung sind, enthält.

Wir können dann f als (exakte) Ersetzungsregel

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

umschreiben. Damit auch die daraus abgeleitete algebraische Ersetzungsregel, die aus allen exakten Regeln

$$n \cdot lt(f) \mapsto -lc(f)^{-1} n \cdot red(f), \ n \in T$$

besteht, dieselbe Form hat, muss die gewählte Ordnung auf T außerdem *monoton* sein, d.h.

$$m_1 < m_2 \ \Rightarrow n \cdot m_1 < n \cdot m_2 \quad \text{für } n, m_1, m_2 \in T$$

erfüllen.

Damit ist gewährleistet, dass das beschriebene algebraische Ersetzungsverfahren nicht im Kreis verlaufen kann. Um die Termination zu sichern, müssen wir zusätzlich fordern, dass es keine unendlichen streng absteigenden Ketten $m_1 > m_2 > \dots$ in T gibt. Ordnungen auf T mit diesen beiden Zusatzeigenschaften bezeichnen wir als *Termordnungen*. Beispiele für solche Termordnungen sind etwa lexikographische oder gradweise Ordnungen, die bei gleichem Grad lexikographisch verfeinert sind.

Es stellt sich heraus, dass die Kettenbedingung für monotone Ordnungen auf T äquivalent dazu ist, dass der Einsterm $1 \in T$ der kleinste Term ist. Diese Bedingung ist offensichtlich für die eben genannten Ordnungen erfüllt.

Beispiel:

$$F = \{f_1 = x^2 - 2\,x\,z + 5, f_2 = x\,y^2 + y\,z^3, f_3 = 3\,y^2 - 8\,z^3\}$$

Daraus leiten sich die Ersetzungsregeln

$$\begin{array}{ll} (1) & x^2 \mapsto 2\,x\,z - 5 \\ (2) & x\,y^2 \mapsto -y\,z^3 \\ (3) & y^2 \mapsto \frac{8}{3}\,z^3 \end{array}$$

ab. Auf den Term x^2y^2 können sie auf verschiedene Weise angewendet werden:

$$\begin{array}{rll} & x^2y^2 & \xrightarrow{(1)\cdot y^2} 2xy^2z - 5y^2 \xrightarrow{(2)\cdot 2z} -5y^2 - 2yz^4 \xrightarrow{(3)\cdot(-5)} -2yz^4 - \frac{40}{3}z^3 \\ & x^2y^2 & \xrightarrow{(2)\cdot x} -xyz^3 \\ \text{oder} & x^2y^2 & \xrightarrow{(3)\cdot x^2} \frac{8}{3}x^2z^3 \xrightarrow{(1)\cdot \frac{8}{3}z^3} \frac{16}{3}xz^4 - \frac{40}{3}z^3 \end{array}$$

Das Ergebnis dieses (unter den genannten Prämissen stets terminierenden) algebraischen Ersetzungsverfahrens, angewendet auf ein Polynom $f \in R$, bezeichnet man als die *Normalform* $g = NF(f, F)$ von f bzgl. der gegebenen Basis F.

Algorithmus NF(f,F)

Input: Polynom f und Polynomsystem F

Output: Normalform von f bzgl. des Systems F

```
Maple: reduce, Mathematica: PolynomialReduce, MuPAD: normalf,
Reduce: preduce, cali: mod
```

Da in jedem Schritt mglw. mehrere verschiedene Reduktionsalternativen bestehen, ist eine solche Normalform nicht eindeutig bestimmt. Allerdings gilt unabhängig vom Reduktionsweg für jedes Zwischen- und Endergebnis stets $f \equiv g\ (mod\ I)$. Wir können dieses Verfahren also insbesondere auf die Frage $f \in I$ anwenden und erhalten

Ist $NF(f, F) = 0$ *so gilt* $f \in I$.

Die Umkehrung gilt nicht unbedingt. Insbesondere gilt für obiges Beispiel

$$y^2 f_1 - x f_2 = -2\,x\,y^2\,z - x\,y\,z^3 + 5\,y^2 \in I(F),$$

aber

$$h = NF(-2\,x\,y^2\,z - x\,y\,z^3 + 5\,y^2, F) = -x\,y\,z^3 + 5\,y^2 + 2\,y\,z^4 \neq 0$$

Ein solche minimale monomiale Linearkombination zweier Polynome, so dass sich die Leitterme gerade wegheben, bezeichnet man als *S-Polynom* $S(f_1, f_2)$. Das Polynom h ist nicht zu 0 reduzierbar, weil sein Leitterme nicht durch einen der Leitterme von $f_i \in F$ teilbar ist. Bezeichnen wir mit $\Sigma(I) \subset T$ die Menge aller Leitterme des Ideals $I = I(F)$ und $\Sigma(F) \subset T$ die Menge aller monomialen Vielfachen der Leitterme der Polynome aus F, so gilt offensichtlich $\Sigma(F) \subset \Sigma(I)$.

Eine Idealbasis G, für die $\Sigma(G) = \Sigma(I)$ gilt, bezeichnet man als *Gröbnerbasis*. Eine solche Basis kann man aus F durch Hinzunahme endlich vieler S-Polynome gewinnen.

Algorithmus gbasis(F)

Input: Polynomsystem F

Output: (minimale reduzierte) Gröbnerbasis von F

```
Maple: gbasis, Mathematica: GroebnerBasis, MuPAD: gbasis,
Reduce: groebner, cali: gbasis
```

Für derartige Basen gilt

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

Für eine solche Gröbnerbasis ist außerdem das Ergebnis der Normalformberechnung unabhängig vom gewählten Reduktionsweg. Genauer gilt der folgende

Satz 17 *(Charakterisierungssatz für Gröbnerbasen) Die folgenden Bedingungen an eine Basis G eines Ideals $I \subset R$ sind äquivalent:*

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

Ohne Beweis. Siehe Vorlesung "Gröbnerbasen und deren Anwendungen".

Beispiel ([1, S. 267]): Gegeben sei ein Quadrat $ABCD$ und der Punkt P auf der Parallelen zu BD durch C mit $BP = BD$. Sei ferner Q der Schnittpunkt von CD und BP. Man zeige, dass dann $DP = DQ$ gilt.

Eine Lösung in einem speziellen Koordinatensystem (in dem die Gerade $g(CD)$ durch $y = 1$ bestimmt wird und damit auch die zweite Koordinate von Q feststeht) geht von drei Variablen aus:

```
A:=Point(0,0); B:=Point(1,0); C:=Point(1,1); D:=Point(0,1);
P:=Point(x1,x2); Q:=Point(x3,1);

polys:={ is_point_on_line(P,par_line(C,pp_line(B,D))),
      sqrdist(B,D)-sqrdist(B,P), is_point_on_line(Q,pp_line(B,P))};

con:=sqrdist(D,Q)-sqrdist(D,P);
```

Wir erhalten als Idealbasis

$$polys = \{x_1 + x_2 - 2, -x_1{}^2 + 2\,x_1 - x_2{}^2 + 1, -x_1 + x_2\,x_3 - x_2 + 1\}$$

und als Behauptung

$$con = -x_1{}^2 - x_2{}^2 + 2\,x_2 + x_3{}^2 - 1$$

Mit dem Reduce-Paket CALI erhalten wir

```
load cali;
vars:={x1,x2,x3};
setring(vars,{},lex);
setideal(polys,polys);
con mod polys;
```

$$-2\,{x_2}^2 + 6\,x_2 + {x_3}^2 - 5$$

da bzgl. der lexikographischen Termordnung im Ausgangssystem *polys* nur Vielfache von x_1 als Leitterme auftreten. Mit der zugehörigen Gröbnerbasis

```
gbasis polys;
```

$$\{{x_3}^2 + 2\,x_3 - 2, 2\,x_2 - x_3 - 2, 2\,x_1 + x_3 - 2\}$$

liefert die entsprechende Normalform

```
con mod gbasis polys;
```

Null und damit einen Beweis der Behauptung.

Allerdings ist es schwierig, die genauen Koordinaten der Punkte P und Q zu bestimmen, denn das Polynom ${x_3}^2 + 2\,x_3 - 2$ aus der Gröbnerbasis hat *zwei* Nullstellen für x_3 (aus denen sich dann jeweils x_1 und x_2 aus den beiden folgenden Gleichungen eindeutig ergibt). Hat diese zweite Lösung eine geometrische Bedeutung oder ist sie degeneriert? Ein genauerer Blick auf die geometrische Konfiguration zeigt, dass wir die zweite Lösung schlichtweg übersehen haben.

Enthält ein Ideal I ein Polynom $f = f_1 \cdot f_2$, das sich in zwei Faktoren zerlegen lässt, die beide nicht im Ideal I enthalten sind, so entspricht dem die Aufspaltung der Nullstellenmenge $Z = V(I)$ in die beiden Teile $V(I + I(f_1)) \cup V(I + I(f_2))$. Auch wenn jeder der beiden Teile noch aus mehreren Komponenten von Z bestehen kann, so kann eine solche partielle Zerlegung hilfreich sein, da wir das Geometrietheorem auf jeder einzelnen Komponente verifizieren können bzw. vielleicht eine Komponente (und den Grund dafür) entdecken, auf der das Theorem nicht gültig ist. Führt man solche Probefaktorisierungen auf den Basiselementen und auch während der Rechnungen des Gröbneralgorithmus aus, so erhält man im Ergebnis aus dem Ausgangssystem F eine Liste von Gröbnerbasen G_i, so dass $V(F) = \cup_i V(G_i)$ gilt. Diese Variante des Gröbneralgorithmus bezeichnet man als den *Gröbnerfaktorisierer*.

Algorithmus groebfactor(F)

Input: Polynomsystem F

Output: Menge von Gröbnerbasen G_i, so dass

$$V(F) = \bigcup_i V(G_i)$$

gilt.

```
Maple: gsolve, Mathematica: -, MuPAD: -,
Reduce: groebnerf, cali: groebfactor
```

Obwohl dies nicht garantiert werden kann, ist die dabei produzierte Zerlegung für eine lexikographische Termordnung in praktischen Anwendungen oft nahe an der Primideal-Zerlegung.

Betrachten wir das Beispiel des Schnittpunkts der Winkelhalbierenden:

```
A:=Point(0,0); B:=Point(1,0); C:=Point(c1,c2); P:=Point(x1,x2);

polys:={is_point_on_bisector(P,A,B,C), is_point_on_bisector(P,B,C,A)};
```

```
con:=is_point_on_bisector(P,C,A,B);

vars:={x1,x2,c1,c2};
setring(vars,{},lex);
res:=groebfactor polys;
for each x in res collect con mod x;
```

Koordinatensystem und Maßstab sind so gewählt, dass wir nur zwei unabhängige (Lage von C) und zwei abhängige (Lage des Schnittpunkts der Winkelhalbierenden durch A und durch B) Parameter einführen brauchen. Als Gleichungen ergeben sich

$$\mathit{polys} := \{x^2\, c_2 - 2\,x\,y\,c_1 + 2\,x\,y - 2\,x\,c_2 - y^2\,c_2 + 2\,y\,c_1 - 2\,y + c_2, 2\,x^2\,c_1\,c_2 - x^2\,c_2 - 2\,x\,y\,{c_1}^2 + 2\,x\,y\,c_1 + 2\,x\,y\,{c_2}^2 - 2\,x\,{c_1}^2\,c_2 - 2\,x\,{c_2}^3 - 2\,y^2\,c_1\,c_2 + y^2\,c_2 + 2\,y\,{c_1}^3 - 2\,y\,{c_1}^2 + 2\,y\,c_1\,{c_2}^2 - 2\,y\,{c_2}^2 + {c_1}^2\,c_2 + {c_2}^3\}$$

Die faktorisierte Gröbnerbasis besteht aus zwei Komponenten, wovon auf der einen $\mathit{con} \equiv 0$ gilt. Die andere enthält in der Gröbnerbasis u.a. das Polynom

$${c_1}^2 - 2\,c_1 + {c_2}^2 + 1,$$

entspricht also dem degenerierten Fall, in dem $(c_1 - 1)^2 + c_2^2 = 0$ gilt. Über den reellen Zahlen würde damit $B = C$ sein, so dass wir diese Komponente aus unseren Betrachtungen ausschließen können.

3.6 Unabhängige und abhängige Variablen

In obigen Beispielen haben wir bereits begonnen, auf einer heuristischen Basis zwischen unabhängigen und abhängigen Variablen zu unterscheiden. Dies wollen wir nun präzisieren. Im konstruktiven Fall war eine wesentliche Voraussetzung für die Gültigkeit des entsprechenden Mechanisierungssatzes die algebraische Unabhängigkeit der Variablen gewesen. Ist $I \subset R = k[x_1, \ldots, x_n] = R[\mathbf{x}]$ ein Relationenideal, so wollen wir eine Teilmenge $\mathbf{u} \subset \mathbf{x}$ als *unabhängig* modulo I bezeichnen, wenn

$$I \cap k[\mathbf{u}] = (0)$$

gilt, d.h. wenn es keine polynomiale Relation in I zwischen den ausgewählten Variablen gibt. Der Nachweis, dass eine vorgegebene Variablenmenge unabhängig ist, wird somit auf ein Eliminationsproblem reduziert, das mit der Berechnung entsprechender Gröbnerbasen beantwortet werden kann. Aus einer Gröbnerbasis kann man umgekehrt auch auf unabhängige Variablenmengen schließen.

Ist I ein Primideal, so haben alle maximalen unabhängigen Variablenmengen die gleiche Kardinalität. Diese Anzahl (der unabhängigen Parameter) bezeichnet man auch als die Dimension des Ideals I bzw. der Nullstellenmenge $V(I)$. Ist $\mathbf{u}$ eine solche maximale unabhängige Variablenmenge und x_i eine weitere Variable, so hängt x_i über I algebraisch von den Variablen $\mathbf{u}$, d.h. es existiert ein Polynom

$$f_i(x_i, \mathbf{u}) = \sum_j c_{ij}(\mathbf{u}) x_i^j \in I$$

x_i kann man dann zwar im Allgemeinen nicht rational durch die unabhängigen Parameter ausdrücken, jedoch ergibt sich für fast alle Parameterbelegungen (genauer: solche, für die $c_{ij}(\mathbf{u}) \neq 0$ gilt) eine Bestimmungsgleichung für x_i und damit nur endlich viele zulässige Parameterspezifikationen $(\mathbf{x}, \mathbf{u}_0)$ für eine vorgegebene Spezifikation $\mathbf{u} = \mathbf{u}_0$.

3.7 Geometrietheoreme vom linearen Typ

Sätze, die auch eine Formulierung als Satz vom konstruktiven Typ besitzen, führen meist auf Ideale, in denen die Polynome f_i alle vom Grad 1 in x_i sind, d.h. wo sich die abhängigen Variablen rational durch die unabhängigen ausdrücken lassen. Betrachten wir als Beispiel den **Satz von Desargue**:

```
A:=Point(u1,u2); B:=Point(u3,u4); C:=Point(u5,u6);

P:=Point(u7,u8); Q:=Point(u9,x1); R:=Point(x2,x3);

pre:={  is_parallel(pp_line(A,C),pp_line(P,R)),
        is_parallel(pp_line(B,C),pp_line(Q,R)),
        is_parallel(pp_line(A,B),pp_line(P,Q))};

con:=   is_concurrent(pp_line(A,P),pp_line(B,Q),pp_line(C,R));
```

Die drei Gleichungen zur Bestimmung der abhängigen Parameter sind linear in x_1, x_2, x_3. Als Lösung ergeben sich rationale Funktionen in $\mathbf{u}$, die, in die Behauptung *con* eingesetzt, diese zu Null vereinfachen.

```
solve(pre,{x1,x2,x3});
sub(ws,con);
```

Bei der Auswahl der unabhängigen und abhängigen Parameter sind wir dem kostruktiven Ansatz gefolgt. Statt dessen könnte man auch versuchen, drei andere der Parameter als abhängig zu deklarieren, etwa

```
P:=Point(u7,x1); Q:=Point(u8,x2); R:=Point(u9,x3);
pre1:={  is_parallel(pp_line(A,C),pp_line(P,R)),
        is_parallel(pp_line(B,C),pp_line(Q,R)),
        is_parallel(pp_line(A,B),pp_line(P,Q))};
```

Auch hier erhalten wir drei Gleichungen, die linear in den abhängigen Variablen sind. Allerdings ist die entsprechende Lösungsmenge leer:

```
solve(pre1,{x1,x2,x3});
```

Geht man etwas vorsichtiger zu Werke, löst zunächst die beiden ersten Gleichungen nach x_1 und x_2 auf und setzt diese Werte dann in die dritte Gleichung ein, um diese schließlich nach x_3 aufzulösen, so erkennt man, dass dort x_3 bereits nicht mehr enthalten ist, sondern eine Gleichung vierten Grades in $\mathbf{u}$ entstanden ist, die Parameter also nicht algebraisch unabhängig sind wie angenommen.

Untersuchen wir nun allgemein, was man über Geometrietheoreme vom Gleichungstyp aussagen kann, in denen die abhängigen Parameter $\mathbf{x}$ linear von den unabhängigen Parametern $\mathbf{u}$ abhängen. Solche Geometrietheoreme wollen wir als *Sätze vom linearen Typ* bezeichnen.

Das entsprechende Gleichungssystem hat die Gestalt

$$\sum_{j=1}^{m} c_{ij}(\mathbf{u}) x_j + c_{i0}(\mathbf{u}) = 0,\ i = 1, \ldots, m$$

Seine Lösbarkeit hängt ganz wesentlich von der Determinante

$$D(\mathbf{u}) := det|c_{ij}(\mathbf{u})|_{i,j=1,\ldots,m}$$

ab. Genauer hat das Gleichungssystem für jede Belegung der Parameter $\mathbf{u}$, für die $D(\mathbf{u}) \neq 0$ gilt, eine eindeutige Lösung, die man in der Form $x_i = D_i(\mathbf{u})/D(\mathbf{u}) \in k(\mathbf{u})$ ausdrücken kann.

Wie im Fall der Sätze vom konstruktiven Typ können wir diese rationalen Funktionen in die Behauptung einsetzen und schauen, ob sich die einzelnen Terme gegenseitig wegheben. Wir erhalten ähnliche Alternativen:

1) Führt die Simplifikation auf das Nullpolynom, so ist für alle zulässigen Spezifikationen der unabhängigen Variablen (d.h. solche, für die $D(\mathbf{u}) \neq 0$ gilt) der Satz richtig.

2) Ergibt die Simplifikation eine nicht verschwindende rationale Funktion $\frac{P(\mathbf{u})}{Q(\mathbf{u})} \neq 0$, so ist der Satz für fast alle Spezifikationen falsch und höchstens unter der zusätzlichen Voraussetzung $P(\mathbf{u}) = 0$ richtig. Er gilt also dann nur, wenn zwischen den als unabhängig angenommenen Variablen eine Abhängigkeit besteht.

3) Ist schließlich bereits $D(\mathbf{u})$ identisch Null, so gibt es eine $k(\mathbf{u})$-lineare Kombination der Zeilen der Koeffizientenmatrix zum Nullvektor

$$\sum_i \alpha_i(\mathbf{u}) c_{ij} = 0,\ j = 1, \ldots, m$$

Dann ist entweder $\sum_i \alpha_i(\mathbf{u}) c_{i0} \neq 0$ eine nichttriviale algebraische Relation zwischen den unabhängigen Variablen oder aber auch die erweiterte Koeffizientenmatrix hat über $k(\mathbf{u})$ einen Rang kleiner als m, d.h. eine der abhängigen Variablen x_i kann frei gewählt werden. In beiden Fällen sind die Voraussetzungen nicht eingehalten.

Satz 18 *(Über das mechanisierte Beweisen geometrischer Sätze vom linearen Typ):*
Sei $(F(\mathbf{x}, \mathbf{u}) \Rightarrow g(\mathbf{x}, \mathbf{u}))$ ein Satz vom linearen Typ. Ist $D(\mathbf{u})$ nicht identisch Null, so ist $\mathbf{u}$ eine maximale Menge unabhängiger Variablen und der Satz gilt unter der Nichtdegenerationsbedingung $D(\mathbf{u}) \neq 0$ genau dann, wenn $g(x(\mathbf{u}), \mathbf{u})$, die rationale Funktion in $k(\mathbf{u})$, die durch Substitution der eindeutig bestimmten Lösung $x = x(\mathbf{u}) \in k(\mathbf{u})^m$ von F in $g(\mathbf{x}, \mathbf{u})$ entsteht, identisch Null ist.

AUFGABE 21:

> Beweisen Sie auf diesem Weg den Satz des Apollonius: In einem rechtwinkligen Dreieck liegen die drei Seitenmitten und der Höhenfußpunkt auf die Hypotenuse auf einem gemeinsamen Kreis.

AUFGABE 22:

> Beweisen Sie auf diese Weise den Satz von Pappus.

3.8 Generisch gültige Geometrietheoreme

Im Fall der Geometrietheoreme vom konstruktiven und vom linearen Typ haben wir lineare Algebra über dem Körper $k(\mathbf{u})$ der rationalen Funktionen in den unabhängigen Parametern getrieben. Wir wollen deshalb nun auch für den allgemeinen Fall im Ring $S' = k(\mathbf{u})[\mathbf{x}]$ der Polynome in $\mathbf{x}$ mit rationalen Funktionen in $\mathbf{u}$ als Koeffizienten rechnen statt wie bisher im Ring $S = k[\mathbf{u}, \mathbf{x}]$.

Betrachten wir zunächst einige Beispiele.

Beispiel 1 : Satz vom Miquelschen Punkt

```
A:=Point(0,0);
B:=Point(1,0);
C:=Point(u1,u2);
R:=varpoint(B,C,u3);
```

```
S:=varpoint(A,C,u4);
T:=varpoint(A,B,u5);
P:=Point(x1,x2);

polys:={ is_p4_circle(A,S,T,P), is_p4_circle(B,R,T,P)};

con:= is_p4_circle(C,R,S,P);
```

Wir wollen die Gröbnerbasis von $I = I(polys)$ im Ring $S' = k(\mathbf{u})[x_1, x_2]$ mit dem Reduce-Paket CALI berechnen:

```
load cali;
setring({x1,x2},{},lex);
setideal(polys,polys);
gb:=gbasis polys;
```

Diese Gröbnerbasis hat eine recht einfache Struktur

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

so dass das zugehörige Gleichungssystem zwei Lösungen $(x_1, x_2) \in \mathbf{A}^2_{k(\mathbf{u})}$ mit $x_{2.1} = 0$ und $x_{2.2} = -\frac{p_2(\mathbf{u})}{p_1(\mathbf{u})}$ besitzt. Die erste Lösung entspricht dem Schnittpunkt F der beiden Kreise, die zweite (die von Reduce als erste ausgegeben wird) dem Punkt P und erfüllt die Gleichung *con*:

```
sol:=solve(gb,{x1,x2});
sub(first sol,con);
```

Beispiel 2 : Satz vom Schnittpunkt der Winkelhalbierenden

```
A:=Point(0,0); B:=Point(0,1); C:=Point(u1,u2); P:=Point(x1,x2);

polys:={is_point_on_bisector(P,B,A,C), is_point_on_bisector(P,C,B,A)};

con:= is_point_on_bisector(P,A,C,B);

setring({x1,x2},{},lex);
setideal(polys,polys);
gb:=gbasis polys;
con mod gb;
```

Als Gröbnerbasis erhalten wir hier

$$\begin{aligned}&\{(4u_2)\,x_2^4 - (8u_1^2 - 8u_1 + 8u_2^2)\,x_2^3 + (4u_1^2u_2 - 4u_1u_2 + 4u_2^3 - 4u_2)\,x_2^2 + (4u_2^2)\,x_2 - u_2^3,\\ &(2u_1u_2^2 - u_2^2)\,x_1 + (2u_2)\,x_2^3 - (4u_1^2 - 4u_1 + 2u_2^2)\,x_2^2 - (2u_1^2u_2 - 2u_1u_2 + 2u_2)\,x_2 - (u_1u_2^2 - u_2^2)\}\end{aligned}$$

In $k(\mathbf{u})[x_1, x_2]$ ist das davon erzeugte Ideal nulldimensional und hat genau 4 Nullstellen in $\mathbf{A}^2_K$, dem zweidimensionalen affinen Raum über $K = \overline{k(\mathbf{u})}$, dem algebraischen Abschluss von $k(\mathbf{u})$. Diese entsprechen den vier ("generischen") Schnittpunkten der möglichen Auswahlen der Halbierenden von Innen- und Außenwinkel von $\angle\,ABC$ und $\angle\,BCA$. Jeder von ihnen liegt auf der ("generischen") Halbierenden entweder des Innen- oder des Außenwinkels von $\angle\,CAB$, da $NF(con, gb) = 0$ und folglich $con \in I(polys) \subset k(\mathbf{u})[x_1, x_2]$ gilt. Es bleibt zu untersuchen, was das mit der ursprünglichen geometrischen Fragestellung zu tun hat.

Beispiel 3 : Die Simsonsche Gerade

```
M:=Point(0,0);
A:=Point(0,u1); B:=Point(u2,x1); C:=Point(u3,x2); P:=Point(u4,x3);
R:=varpoint(A,B,x4); S:=varpoint(B,C,x5); T:=varpoint(A,C,x6);

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

con:= is_collinear(R,S,T);

xvars:={x4,x5,x6,x1,x2,x3};
setring(xvars,{},lex);
setideal(polys,polys);
gb:=gbasis polys;
con mod gb;
```

Auch in diesem Fall ist das Ideal $I(polys) \subset k(\mathbf{u})[\mathbf{x}]$ nulldimensional. Aus der Gröbnerbasis

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

lesen wir ab, dass dieses System 8 “generische” Lösungen besitzt und *con* auf allen diesen Punkten verschwindet, d.h. der Satz von der Simsonschen Geraden “generisch” (d.h. in $\mathbf{A}_K^2$) gilt.

In allen bisher betrachteten Beispielen besteht die Gröbnerbasis aus Gleichungen vom Grad 1 und 2 in den abhängigen Variablen und erlaubt es, die abhängigen Variablen durch die unabhängigen auszudrücken, auch wenn es im Gegensatz zum linearen Fall mehrere, aber stets endlich viele Lösungen für $\mathbf{x}$ in Abhängigkeit von den Parametern $\mathbf{u}$ gibt. In manchen Fällen, wie etwa beim Miquelschen Punkt, kann man die einzelnen Lösungen explizit in $k(\mathbf{u})$ ausdrücken, in anderen Fällen dagegen hätte man die einzelnen Zweige der Lösungsmenge durch mehr (Schnittpunkt der Winkelhalbierenden) oder weniger (Simsonsche Gerade) komplizierte Wurzelausdrücke in den unabhängigen Variablen angeben müssen. Die betrachteten Gleichungssysteme haben also stets endlich viele Lösungen (in den abhängigen Variablen), deren Koordinaten aber, in Übereinstimmung mit der allgemeinen Theorie, im algebraischen Abschluss des Koeffizientenkörpers $k(\mathbf{u})$ liegen.

Um zu testen, ob ein gegebenes Polynom *con* auf *allen* diesen Nullstellen verschwindet, haben wir aber nicht in dieser Erweiterung gerechnet, sondern $NF(con, G) = 0$ in $S' = k(\mathbf{u})[\mathbf{x}]$ für eine Gröbnerbasis $G = \mathtt{gbasis}_{S'}(F)$ der geometrischen Bedingungen F geprüft. Wir wollen nun diskutieren, was dieses Ergebnis mit unserer ursprünglichen geometrischen Fragestellung zu tun hat.

Sei dazu $F \subset S = k[\mathbf{u}, \mathbf{x}]$ ein System von Polynomen, $I = I(F)$ und $I' = I_{S'}(F)$ das Ideal, das von diesen Polynomen in S' erzeugt wird. $\mathbf{u}$ sei eine bzgl. I maximale Menge von unabhängigen Variablen, womit F über $k(\mathbf{u})$ nur endlich viele Lösungen, sogenannte *allgemeine Nullstellen*, besitzt. Ein Polynom $g \in S'$ verschwindet auf all diesen Nullstellen genau dann, wenn $g \in rad_{S'}(I')$ gilt. Ist $NF(g, G) = 0$ für eine Gröbnerbasis G von I', so gilt sogar $g \in I'$. Allgemeiner gilt

$$g \in rad_{S'}(I') \;\Leftrightarrow\; \exists n > 0 \;:\; NF(g^n, G) = 0.$$

$g = g(\mathbf{x}, \mathbf{u}) \in I'$ bedeutet aber nichts anderes als die Existenz von rationalen Funktionen $r_f =$

$z_f(\mathbf{x},\mathbf{u})/n_f(\mathbf{u}) \in S',\ f \in F$, so dass

$$g(\mathbf{x},\mathbf{u}) = \sum_{f\in F} \frac{z_f(\mathbf{x},\mathbf{u})}{n_f(\mathbf{u})}\ f(\mathbf{x},\mathbf{u})$$

gilt. Ist $n(\mathbf{u})$ ein gemeinsamer Hauptnenner, so verschwindet also g auf den "allgemeinen" Nullstellen von F in dem Sinne, dass es auf allen (gewöhnlichen) Nullstellen $(\mathbf{x}_0,\mathbf{u}_0)$ verschwindet, für die $n(\mathbf{u}_0) \neq 0$ gilt.

Satz 19 *(Über die Gültigkeit geometrischer Sätze vom Gleichungstyp "im Allgemeinen"):*
Sei $(F(\mathbf{x},\mathbf{u}) \Rightarrow g(\mathbf{x},\mathbf{u}))$ ein Satz vom Gleichungstyp und $\mathbf{u}$ eine für diesen Satz maximale unabhängige Teilmenge der Variablen.

Gilt $g \in I' = I_{S'}(F)$ als Polynome in $S' = k(\mathbf{u})[\mathbf{x}]$, etwa weil $NF(g,\mathtt{gbasis}_{S'}(F)) = 0$, so gibt es eine Nichtdegenerationsbedingung $h(\mathbf{u})$, so dass g auf allen gemeinsamen Nullstellen $(\mathbf{x}_0,\mathbf{u}_0)$ von F mit $h(\mathbf{u}_0) \neq 0$ verschwindet, also der Satz $(F = 0,\ h \neq 0\ \Rightarrow\ g)$ gilt.

Eine Darstellung

$$h(\mathbf{u})g(\mathbf{x},\mathbf{u}) = \sum_{f\in F} z_f(\mathbf{x},\mathbf{u})\, f(\mathbf{x},\mathbf{u})$$

kann man mit einiger Mühe aus der Normalformberechnung $NF(g,G) = 0$ extrahieren, wenn man sich in der Gröbnerbasisberechnung $G = \mathtt{gbasis}_{S'}(F)$ noch die Darstellung der $g_i \in G$ als polynomiale Kombination der $f_j \in F$ gemerkt hat. Allerdings folgt allein aus der *Existenz* von $h \in k[\mathbf{u}]$, dass die Menge derjenigen Spezifikationen der unabhängigen Parameter, für die $h(\mathbf{u}_0) = 0$ gilt, eine Hyperfläche im Parameterraum definiert, so dass eine "zufällige" Wahl dieser Parameter "normalerweise" zulässig ist. Deshalb auch "Gültigkeit im Allgemeinen".

Es ist auch plausibel, dass wenigstens für ein Radikalideal I' aus dem Nichtverschwinden von $NF(g,\mathtt{gbasis}_{S'}(F))$ folgt, dass g auf wenigstens einer der "allgemeinen" Nullstellen von F nicht verschwindet und folglich nicht allgemeingültig ist. Um dies besser zu verstehen, müssen wir den Zusammenhang zwischen Nullstellen von F in $S := k[\mathbf{x},\mathbf{u}]$ und $S' = k(\mathbf{u})[\mathbf{x}]$ genauer studieren.

Dazu betrachten wir ein Geometrietheorem vom Gleichungstyp, dessen Voraussetzungen F ein Ideal $I = I(F) \subset S$ erzeugen. $\mathbf{u}$ sei wieder eine maximale Teilmenge der Variablen, die unabhängig bzgl. I sind.

Der Polynomring S' enthält S als Unterring. Das von F in S' erzeugte Ideal $I' = I_{S'}(F) = I \cdot S'$ bezeichnet man als das *Erweiterungsideal* von I. Umgekehrt können wir mit einem Ideal $I' \subset S'$ das *Kontraktionsideal* $c(I') := I' \cap S$ in S verbinden, das aus allen rationalen Kombinationen der Erzeugenden besteht, "in denen sich die Nenner wegkürzen". Sicherlich ist $I \subset c(I')$.

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 multiplikativen Menge U.

Zunächst wollen wir das Erweiterungsideal $I' = I \cdot S'$ genauer beschreiben. Ist $F = \{f_i,\ i = 1,\ldots,m\} \subset S$ 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.

Wir hatten gesehen, dass jedes Radikalideal I als Durchschnitt endlich vieler Primideale $I = \cap P_\alpha$ darstellbar ist. Eine bzgl. I unabhängige Variablenmenge $\mathbf{u}$ muss allerdings bzgl. einer dieser Primkomponenten, die ja größer sind als I, nicht mehr unabhängig sein. Wir erkennen das daran, ob $P_\alpha \cap U = \emptyset$ gilt (in diesem Fall bleibt die Variablenmenge unabhängig) oder nicht (in diesem Fall gibt es in P_α eine algebraische Beziehung zwischen den Variablen $\mathbf{u}$). Komponenten der ersten Art nennen wir *generisch*, Komponenten der zweiten Art *speziell*. Zerlegen wir das Nullstellengebilde der Voraussetzungen eines Geometrietheorems in seine Komponenten, so entsprechen letztere gewissen degenerierten Situationen, die eigentlich vermieden werden sollen.

Satz 20

(1) Sei 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 $u \in P_\alpha$. □

Korollar 1

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

Ist insbesondere g ein Polynom in S und $G = \texttt{gbasis}_{S'}(I)$, so gilt $NF_{S'}(g, G) = 0$ genau dann, wenn g auf allen generischen Komponenten von $V(I)$ verschwindet.

Wir sagen in diesem Fall, dass der geometrische Satz bzgl. der unabhängigen Variablenmenge $\mathbf{u}$ *generisch richtig ist*, was folgendes heißt: Der Satz $g = 0$ ist höchstens auf speziellen Komponenten von $V(I)$, auf denen aber die Variablen $\mathbf{u}$ nicht mehr unabhängig sind, falsch. Jede solche Komponente enthält im definierenden Ideal ein Polynom $h_i(\mathbf{u})$. Das Produkt dieser Polynome können wir als Nichtdegenerationsbedingung nehmen.

Ist umgekehrt $NF_{S'}(g,G) \neq 0$, so verschwindet g auf einer der generischen Komponenten nicht, d.h. kann durch keine Nichtdegenerationsbedingung, die nur die unabhängigen Parameter enthält, gerettet werden.

Generell, wenn $NF(g,G)$ nicht verschwindet, wie oben im Beispiel "Miquelscher Punkt", liefern uns Untersuchungen in S' Aussagen, die das Verhalten auf speziellen Komponenten ausblenden. In diesem Beispiel hat $V(I)$ 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 $V(I)$ 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.

4 Triangulare Systeme

4.1 Definitionen und Eigenschaften

Im letzten Kapitel hatten wir gesehen, dass wir in Geometrietheoremen ($F = 0 \;\Rightarrow\; g = 0$) statt der expliziten Angabe von Nichtdegenerationsbedingungen oft auf natürliche Weise einen Satz unabhängiger Koordinaten $\mathbf{u}$ fixieren können, von dem die verbleibenden Koordinaten $\mathbf{x}$ in $R = S/I(F)$ algebraisch abhängen. Setzen wir $K = k(\mathbf{u})$, so haben wir gesehen, dass das Erweiterungsideal $I' = I(F) \cdot S'$ in $S' = K[\mathbf{x}]$ die adäquate algebraische Struktur ist, in der wir eine durch Gleichungen $F \subset S = k[\mathbf{u}, \mathbf{x}]$ beschriebene geometrische Situation außerhalb spezieller Komponenten untersuchen können. Das Erweiterungsideal ist dabei ein nulldimensionales Ideal über K, hat also nur endlich viele Lösungen über dem algebraischen Abschluss von K.

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 $V(I(B))$ 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.

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

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

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.

Andererseits haben wir zwei Polynome zur Bestimmung von y zur Verfügung

$$\begin{array}{l} f_2 = y^2 - y + (-z^2 + z) \quad \text{und} \\ f_3 = 2(z^2 - 2)\,y + (z^4 - 5\,z^2 + 6) = 2(z^2 - 2)\,y + (z^2 - 2)(z^2 - 3) \end{array}$$

f_2 hat wieder einen konstanten Leitkoeffizienten, f_3 dagegen nicht. Wir können aus $f_3(y, z_0) = 0$ den zugehörigen Wert von y bei vorgegebenem $z = z_0$ mit $z_0^2 - 2 \neq 0$ eindeutig berechnen. Ist dagegen $z_0^2 - 2 = 0$, so wird $f_3(y, z_0)$ identisch zu Null und y kann nur aus $f_2(y, z_0) = 0$ bestimmt werden (zwei Lösungen zu vorgegebenem z_0). Die Existenz des Polynoms f_2 mit konstantem Leitkoeffizienten sichert die Endlichkeit der Nullstellenmenge.

Generell wissen wir von nulldimensionalen Idealen das folgende:

Satz 21 *$I \subset S$ ist ein nulldimensionales Ideal, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

1. *S/I ist ein endlich-dimensionaler K-Vektorraum.*
2. *Eine resp. 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.*

Beweis : siehe Vorlesung "Gröbnerbasen und deren Anwendungen". □

Aufgabe 23:

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 $gcd(q_i, q_i') = 1$)

Um in unserem Beispiel die Lösungsmenge $V(B)$ zu berechnen, können wir das Polynom

$$f_4 = z^6 - 10\,z^4 + 4\,z^3 + 19\,z^2 - 8\,z - 6 = (z^2 - 2z - 1)(z^2 - 2)(z + 3)(z - 1)$$

faktorisieren und $V(B)$ als Vereinigung der $V(B_i)$ bestimmen, die den einzelnen Faktoren von f_4 entsprechen. Berechnen wir für jede Komponente die Gröbnerbasis (dasselbe Ergebnis liefert der Gröbnerfaktorisierer), so erhalten wir

$$\begin{aligned} B_1 &= \{z^2 - 2\,z - 1, y + z - 1, x + z - 1\} \\ B_2 &= \{z^2 - 2, x + y - 1, y^2 - y + z - 2\} \\ B_3 &= \{z + 3, y + 3, x + 3\} \\ B_4 &= \{z - 1, y - 1, x - 1\} \end{aligned}$$

Jede der Basen ist ein triangulares System. Das ist zugleich die Zerlegung von $V(B)$ in irreduzible Komponenten.

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

Satz 22 *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 K-Vektorraum-Dimensionen 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. □

Es stellt sich heraus, dass Primideale stets Gröbnerbasen haben, die triangulare Systeme sind:

Satz 23 *Ist $P \subset S$ ein nulldimensionales Primideal (also zugleich 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. □

Beschreibt das triangulare System $B=\{f_1,\ldots,f_n\}$ ein Primideal $I(B)$, so muss insbesondere jedes der Polynome $f_1,\ldots,f_n$ irreduzibel (über dem Grundkörper) sein. Das ist jedoch keine hinreichende Bedingung, 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 in Primkomponenten

$$I(f_1,f_2,f_3) = I(x_1+x_2x_3, x_2^2-2, x_3^2-3)\ \cap I(x_1-x_2x_3, x_2^2-2, x_3^2-3).$$

Jede Primkomponentenzerlegung von I ist also 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 $V(B)=\cup V(B_\alpha)$ auch mit geringerem Aufwand möglich ist. Eine solche Zerlegung nennen wir eine *Triangulierung* von B.

4.2 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

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

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

$$f_4 := prem(f_2,f_3,y) = z^6-10z^4+4z^3+19z^2-8z-6$$

bzgl. der dritten ersetzen. Dieser berechnet sich wie folgt

$$\begin{aligned} f_2 \mapsto f_2' &= 2(z^2-2)f_2 - y\,f_3 = y(-z^4+3z^2-2)+(-2z^4+2z^3+4z^2-4z)\\ &= -y(z^2-1)(z^2-2)+(-2z^4+2z^3+4z^2-4z)\\ \mapsto f_2'' &= 2f_2'+(z^2-1)f_3 = z^6-10\,z^4+4\,z^3+19\,z^2-8\,z-6 \end{aligned}$$

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

$$\{x+y+z^2-3,\ 2\,y\,(z^2-2)+z^4-5\,z^2+6,\ z^6-10\,z^4+4\,z^3+19\,z^2-8\,z-6\}$$

und

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

wobei beim ersten System noch zu berücksichtigen ist, dass $z^2 \neq 2$ vorausgesetzt wurde. Damit fallen zwei Lösungen der letzten Gleichung

$$z^6 - 10\,z^4 + 4\,z^3 + 19\,z^2 - 8\,z - 6 = (z^2 - 2z - 1)(z^2 - 2)(z + 3)(z - 1)$$

zur Bestimmung von z weg und das System kann ersetzt werden durch

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

Jeder der beiden Zweige steuert also 4 Lösungen zur Lösungsmenge $V(B)$ 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.* $lc(f, x_i)$ 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 $l_i := lc(f_i, x_i)$ für $f_i \in B$, so kann man durch fortgesetzte Pseudodivision zu jedem Polynom $f \in R$ eine Normalform bzgl. B definieren.

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

Algorithmus prem(f,g)

Input: nicht konstante Polynome f, g

Output: Pseudorest von f bei Division durch 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

Algorithmus PNF(f,B)

Input: Polynom f, Polynomsystem B in Dreiecksform

Output: Pseudo-Normalformrest f' von f bzgl. B

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

eine *Pseudo-Normalform*, in der der Rückgabewert f' entweder verschwindet oder für alle i $deg(f', x_i) < deg(f_i, x_i)$ gilt. Da

$$f' \equiv l_1^{a_1} \ldots l_n^{a_n} \cdot f\ (mod\ I(B))$$

für geeignete Exponenten $a_1, \ldots, a_n \in \mathbf{N}$ gilt, verschwindet mit $PNF(f, B) = 0$ das Polynom f auf der relativen Nullstellenmenge

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

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

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

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

ist der zugehörige *Gradvektor*.

Wir nennen eine schwach triangulare Menge $B \subset I$ 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

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

Satz 24 *Sei $G = \{f_1, \dots, f_n\} \subset I$ eine schwach triangulare Menge, $J = I(G) \subset I$ das von G erzeugte Ideal und $l = l_1 \cdot \ldots \cdot l_n$ das Produkt der Leitkoeffizienten der f_i.*

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

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

gilt.

2) In diesem Fall ist $J \subseteq I \subseteq J : l^\infty$ und damit $V(G) \supset V(I) \supset V(G, l)$.

3) Ist I ein Primideal, dann gilt $I = J : l^\infty$ und somit

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

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 $G' = \{f'_1, \dots, f'_r\} \subset I$ schwach triangular mit einem Gradvektor $(d'_1, \dots, d'_n)$, 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

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

gilt.

3) 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, weil z.B. die Bestimmung des Polynoms $f_n(x_n) \in I$ kleinsten Grades zur Berechnung des Eliminationsideals $I \cap k[x_n]$ äquivalent ist. Dieses kann aus einer beliebigen Basis F des Ideals I nicht ohne größeren Aufwand bestimmt werden.

Ist $F = \{f_1, \dots, f_r\}$ eine Basis des Ideals I, so wollen wir deshalb wenigstens eine schwach triangulare Menge konstruieren, die noch einige gute Eigenschaften charakteristischer Mengen hat, deren Definition sich aber auf F und nicht auf I bezieht.

Definition: Wir nennen $G \subset I$ eine *erweitert charakteristische Menge* der Basis F bzgl. des Ideals I, 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 25 *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*

$$I(G) \subseteq I \subseteq I(G) : l^\infty$$

und somit auch

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

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. □

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:

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

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

Algorithmus 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:

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

Hier ist im ersten Durchlauf $G_1 = \{f_3\}, R = \{f_4, f_5\}$ mit

$$f_4 := PNF(f_1, G_1) = 2\,x\,(z^2 - 2) + z^4 - 5\,z^2 + 6$$
$$f_5 := PNF(f_2, G_1) = z^6 - 10\,z^4 + 4\,z^3 + 19\,z^2 - 8\,z - 6$$

und danach $F = \{f_1, f_2, f_3, f_4, f_5\}$. Im zweiten Durchlauf erhalten wir $G_2 = \{f_5, f_3, f_4\}$ und $R = \emptyset$. $G = G_2$ ist also die gesuchte erweitert charakteristische Menge. Wir hatten bereits oben gesehen, dass in der Tat

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

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

Aufgabe 24:

Zeigen Sie, dass obiger Algorithmus stets terminiert und die geforderte Spezifikation erfüllt.

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 $V(G)$ arbeiten, weil die im Normalfall zu groß werden. Wir suchen deshalb im weiteren eine Zerlegung

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

in triangulare Mengen 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 $f \in F$

$mvar(F) := max(mvar(f) \mid f \in F)$,
$F^{top} := \{f \in F \mid mvar(f) = mvar(F)\}$,
$lc(f) := lc(f, mvar(f))$ und
$red(f) := f - lc(f) * mvar(f)^{deg(f,mvar(f))}$.

so bedeutet letzteres gerade $V(\prod lc(f) \mid f \in T_i) \subset V(q_i)$. Solche Dreiecksmengen heißen in [3] bereits triangulare Systeme. Der folgende Algorithmus konstruiert eine solche Zerlegung:

Algorithmus Triang(F,q)

Input: Polynomsystem F mit Nebenbedingung q

Output: Liste von Dreiecksmengen (T_i, q_i), so dass $V(F, q) = \bigcup V(T_i, q_i)$ und $V(\prod lc(f) \mid f \in T_i) \subset V(q_i)$ gilt.

```
begin
  if inconsistent(F) then return ∅;
    (* etwa, wenn F ein Polynom vom Grad 0 enthält *)
  if F^top = {f} then
    begin
    Tr1:=for (Ti,qi) in Triang(F \ {f},q) collect ({f} ∪ Ti, lc(f) * qi);
      (* Zweig mit lc(f) ≠ 0 *)
    Tr2:=Triang({lc(f), red(f)} ∪ (F \ {f}),q);
      (* Zweig mit lc(f) = 0 *)
    return append(Tr1,Tr2);
    end
  else
    begin
    wähle f ∈ F^top von minimalem Grad.
    Tr1:=Triang({f} ∪ {prem(g,f) ≠ 0 | g ∈ F^top \ {f}} ∪ (F \ F^top), q * lc(f)));
      (* Zweig mit lc(f) ≠ 0 *)
    Tr2:=Triang({lc(f), red(f)} ∪ (F \ {f}),q);
      (* Zweig mit lc(f) = 0 *)
    return append(Tr1,Tr2);
    end
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 $F^{top} = \{f_2, f_3\}$, also wird mit $f = f_3$ einerseits $Triang((f_3, f_4), z^2 - 2)$ und andererseits $Triang((f_2, f_5 = red(f_3) = z^4 - 5\,z^2 + 6, z^2 - 2), 1)$ 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 Dreiecksform.

Satz 26 `Triang(F,q)` *terminiert nach endlich vielen Schritten mit einer Liste (T_i, q_i) von Systemen T_i in Dreiecksform, so dass $V(q_i) \supset V(lc(T_i))$ gilt und $V(F, q)$ die disjunkte Vereinigung der relativen Nullstellenmengen $V(T_i, q_i)$ ist.*

AUFGABE 25:

Beweisen Sie die Termination dieses Algorithmus.

Der zweite Teil der Behauptung ist offensichtlich: Wenn sie für jeden der beiden Zweige, die `Triang` 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 $lc(f) = 0$ oder $lc(f) \neq 0$ ist und die entsprechende Information wird entweder in T_i oder in q_i aufgenommen.

Beachte, dass $V(T, q)$ leer sein kann. Dies geschieht etwa, wenn $prem(q, T) = 0$ ist, da dann $V(q) \supset V(T, lc(T)) \supset V(T, q)$ gilt. Deshalb nennt Wang in [3] 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 `Triang` bzgl. $x_1 < x_2 < x_3$ in $(F, x_1 - x_2)$ und den leeren Zweig, also gilt $V(F) = V(F, x_1 - x_2)$. Aber aus den beiden ersten Gleichungen folgt $x_1 = x_2$, also $V(F) = \emptyset$.

AUFGABE 26:

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

$$\begin{aligned} f_1 &:= x + y + z^2 - 3, \\ f_2 &:= 2\,y\,(z^2 - 2) + z^4 - 5\,z^2 + 6, \\ f_3 &:= z^6 - 10\,z^4 + 4\,z^3 + 19\,z^2 - 8\,z - 6\} \end{aligned}$$

erläutern. Wegen $f_3 = (z^2 - 2) f_4$ 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 $V(T)$ 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 $a(z) = gcd(lc(f), g)$ 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 $gcd(lc(f), g/a) = 1$ und wir können wie oben verfahren.

5 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) 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.

2) 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.

3) 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.

4) 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.

5) 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.

6) Beweisen Sie die Flächeninhaltsformel

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

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

7) 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.

8) 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 $l(PF) = l(PG)$.

9) Zeigen Sie, daß der Feuerbachkreis den Inkreis und die drei Ankreise berührt.

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.

Literatur

[1] S.-C. Chou. Proving elementary geometry theorems using Wu's algorithm. In *Contemp. Math.*, volume 19, pages 243 – 286. AMS, Providence, Rhode Island, 1984.

[2] H.S.M. Coxeter and S.L. Greitzer. *Geometry revisted.* Toronto – New York, 1967.

[3] D. Wang. An elimination method for polynomial systems. *J. Symb. Comp.*, 16:83 – 114, 1993.

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