Skript zum Kurs
Mechanisiertes Theorembeweisen in der Geometrie
Sommersemester 1998

Hans-Gert Gräbe, Univ. Leipzig

14. Juli 1998

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 weiterentwickelt, aber sie ist heute, sicher vollkommen zu unrecht, in die zweite Reihe gerückt. Das findet insbesondere seinen Ausdruck im Curriculum der Schule, in dem geometrische Fragestellungen nur noch in geringem Umfang auftauchen.

Andererseits faszinieren geometrische 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 Aufgaben und Ideen, an denen man die eigene Argumentationskraft stets von Neuem schärfen 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 dann auch, 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 in diesem Fall insbesondere mit dem Namen F.Klein und dessen 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, Winkeln und Kreisen gibt es auch noch Strecken, 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 Strecken (in diesem Sinne) 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 Ordnungsrelationm 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. 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. 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 geometrische 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 dem Horizont 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. Da die hierbei zu lösenden Fragen oft recht diffzile Konstruktionen verwenden, werden wir darauf nicht näher eingehen. Insbesondere in der Monographie [4] von Wu sind dazu interessante Ausführungen enthalten, in denen auch Koordinatensysteme über nichtkommutativen Zahlbereichen eine Rolle spielen.

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

1. Satz vom Schnittpunkt der Winkelhalbierenden

Verwendet den Begriff der *Ortslinie*: 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.

Eine Ortslinie verbindet eine geometrische (Winkelhalbierende als Gerade) mit einer logischen (A mit $d(A, g_1) = d(A, g_2)$) Eigenschaft. Ihre Beweiskraft entwickeln Ortslinien aus dem Zusammenspiel beider Seiten.

Innenwinkel und Außenwinkel sind Begriffe der Ordnungsgeometrie. Ohne Ordnung kann man sie nicht unterscheiden, sondern nur vom *Paar der Winkelhalbierenden* sprechen. Die drei Winkelhalbierendenpaare haben (neben den Eckpunkten des Dreiecks) vier gemeinsame Punkte, den Inkreismittelpunkt und die drei Mittelpunkte der Ankreise.

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*.

2. Satz vom Schnittpunkt der Mittelsenkrechten

Betrachte dazu die Mittelsenkrechte als geometrischen Ort der Punkte, die von zwei gegebenen Punkten gleichweit entfernt sind. Zusatzeigenschaft des Schnittpunkts: M ist der Umkreismittelpunkt.

3. Satz vom Schnittpunkt der Seitenhalbierenden

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

4. Satz vom Höhenschnittpunkt

Mehrfachanwendung von Thaleskreisen, Sätzen über Winkel am Kreis (Peripheriewinkelsatz, Zentriwinkelsatz)

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 Die Sätze des Menelaos und des Ceva

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

Satz 1 (Satz des Menelaos) *Schneidet eine Transversale eines Dreiecks $\Delta\, ABC$, die nicht durch einen Eckpunkt geht, die Dreiecksseiten oder deren Verlängerungen in den Punkten D, E und F, so gilt für die (vorzeichenbehafteten) Längen der einzelnen Teilstrecken*

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

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

Beweis: Fälle die Lote von den drei Eckpunkten auf die Transversale und wende den Strahlensatz aus jedem der drei Eckpunkte an.

Beachte, daß für die Anwendung des Strahlensatzes nur relevant ist, daß die Lote untereinander parallel sind.

Satz 2 (Satz des Ceva) *Drei Ecktransversalen des Dreiecks $\Delta\, ABC$ mögen die gegenüberliegenden Seiten in den Punkten D, E, F schneiden. Diese drei Ecktransversalen gehen genau dann durch einen Punkt, wenn*

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

gilt.

Beweis: Sei P der Schnittpunkt. Wende Satz des Menelaos auf ABD mit FC und auf ACD mit BE an.

Zweiter Beweis verwendet 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. Zeigen Sie, daß man aus dem Satz des Ceva auch den Satz über den Schnittpunkt der Winkelhalbierenden herleiten kann. (Hinweis: Zeigen Sie, daß eine Winkelhalbierende die gegenüberliegende Seite im Verhältnis der beiden anliegenden Seiten teilt.)
>
> 2. Zeigen Sie, daß die Transversalen zu den Berührungspunkten des Inkreises sich in einem Punkt schneiden. (Hinweis: Berechnen Sie die Länge der einzelnen Tangentenabschnitte.)
>
> 3. Zeigen Sie, daß sich die Transversalen zu den drei Berührungspunkten der Ankreise in einem Punkt schneiden. (Dieser Punkt heißt auch *Nagelscher Punkt*)

1.3 Weitere Sätze am Dreieck

Satz 3 (Die Eulersche Gerade) *In einem Dreieck liegen der Höhenschnittpunkt H, der Schwerpunkt S und der Umkreismittelpunkt M auf einer Geraden. S teilt HM im Verhältnis 2:1.*

Im Beweis werden Dreiecke in Ähnlichkeitslage verwendet.

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

Satz 4 (Satz von Desargue) *1. Sind* $\Delta\,ABC$ *und* $\Delta\,A'B'C'$ *in Ähnlichkeitslage, d.h.* $AB \| A'B'$, $AC \| A'C'$ *und* $BC \| B'C'$, *so sind* AA', BB' *und* CC' *konkurrent oder parallel.*

2. Sind umgekehrt AA', BB' *und* CC' *konkurrent oder parallel und* $AB \| A'B', AC \| A'C'$, *so gilt auch* $BC \| B'C'$.

Der Beweis ergibt sich aus einer Strahlensatzfigur, die durch Verschiebung des Dreiecks ABC in A' entsteht.

Der Satz von Desargue spielt in der Fundierung der affinen Geometrie eine zentrale Rolle, da dort das Verschiebungsargument aus obigem Beweis nicht ohne weiteres verwendet werden kann, da es sich nicht aus den Axiomen herleiten läßt.

Satz 5 (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*

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. Daß er außerdem mit dem Umkreis des Höhenfußpunktdreiecks zusammenfällt, folgt aus der nächsten Aufgabe.

> Aufgabe: 1. Zeigen Sie, daß die Höhen des Dreiecks ABC die Winkelhalbierenden des entsprechenden Höhenfußpunktdreiecks sind.
>
> 2. Zeigen Sie, daß der Feuerbachkreis mit dem Umkreis des Höhenfußpunktdreiecks zusammenfällt.

Der Feuerbachkreis hat eine weitere, mit elementargeometrischen Mitteln nur schwer zu beweisende ([3, S. 39] ist nicht schlüssig[1]) Eigenschaft: Er berührt den Inkreis des Dreiecks $\Delta\,ABC$ und dessen drei Ankreise.

1.4 Sätze am Dreieck aus der neueren Forschung

Satz 6 (Der Miquelsche Punkt) *Nimmt man auf jeder Seite eines Dreiecks* $\Delta\,ABC$ *einen Punkt beliebig an und zeichnet durch jede Ecke und die beiden Punkte, die auf den zu dieser Ecke inzidenten Seiten liegen, Kreise, so gehen diese durch einen gemeinsamen Punkt.*

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

> Aufgabe: Umgekehrt kann man zu jedem Punkt P im Inneren des Dreiecks $\Delta\,ABC$ Punkte A_1, B_1, C_1 so auf den Dreiecksseiten finden, daß P der zugehörige Miquelsche Punkt ist.
>
> Es gibt mehrere Tripel (A_1, B_1, C_1), die denselben Miquelschen Punkt liefern. Zeigen Sie, daß all diese Dreiecke $\Delta\,A_1B_1C_1$ zueinander ähnlich sind.

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.

[1] Ein Beweis unter Verwendung von Inversionen am Kreis ist in [2] enthalten.

Aufgabe: 1. [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.

2. 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:

Satz 7 (Die Simsonsche Gerade) *Fällt man von einem Punkt P außerhalb eines Dreiecks $\Delta\,ABC$ die Lote auf die Dreiecksseiten oder deren verlängerungen, so liegen die drei Fußpunkte der Lote genau dann auf einer Geraden, wenn P auf dem Umkreis des Dreiecks $\Delta\,ABC$ liegt.*

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.

Aufgabe: 1. Leiten Sie aus der Flächeninhaltsformel für das Fußpunktdreieck einen zweiten Beweis für den Satz über die Simsonsche Gerade her.

2. Beweisen Sie die Umkehrung des Satzes von der Simsonschen Geraden: 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.

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.*

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.

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.*

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

Satz 9 (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: 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.

2 Vektorgeometrische Methoden in der Geometrie

Das zentrale Instrument für die Mechanisierung des Beweises geometrischer Sätze ist deren Überführung in eine symbolische Form durch Einführung entsprechender Koordinaten. Aus solchen Koordinaten lassen sich mit den Methoden der analytischen Geometrie Abstände, Winkelgrößen, Geradengleichungen, Schnittpunktkoordinaten usw. berechnen.

Wir wollen uns in diesem Abschnitt zunächst einmal die entsprechenden Begriffe ins Gedächtnis zurückrufen und an einigen Beispielen die Beweiskraft solcher vektorgeometrischer Argumentationen studieren.

Je nach Art der Geometrie benötigen wir für den Einsatz der Koordinatenmethode ein karthesisches (Euklidsche Geometrie) oder affines (affine Geometrie) Koordinatensystem.

Ein *affines* Koordinatensystem besteht aus zwei sich schneidenden Geraden als den Koordinatenachsen und je einem Punkt pro Koordinatengerade, die zusammen mit dem *Ursprung* O, dem Schnittpunkt der beiden Koordinatengeraden, die beiden *Einheitsstrecken* festlegen. Die Koordinaten eines beliebigen Punktes P ergeben sich dann aus einer Parallelogrammkonstruktion und der Bestimmung der entsprechenden Teilverhältnisse (bzgl. der Einheitsstrecken) der Projektionen P_x und P_y des Punktes P auf die beiden Koordinatengeraden.

In einem *karthesischen* Koordinatensystem stehen darüber hinaus die beiden Koordinatengeraden aufeinander senkrecht und die Einheitsstrecken sind gleichlang, womit auch die Berechnung von Längen und Winkelgrößen aus gegebenen Koordinaten auf einfache Weise möglich wird.

Da oftmals bei Rechnungen mit derartigen Koordinaten die Lage der Achsen und des Ursprungs von untergeordneter Bedeutung sind, wollen wir diese in den Bezeichnungen nicht berücksichtigen und für einen Punkt A unserer Ebene mit demselben Symbol sein Paar von Koordinaten bzgl. eines beliebigen, aber fixierten, affinen Koordinatensystems bezeichnen, d.h. in anderer Terminologie in der Bezeichnung nicht zwischen dem Punkt A und dem Ortsvektor zu diesem Punkt unterscheiden.

2.1 Teilverhältnisse und baryzentrische Koordinaten

Wir wollen nun für einige grundlegende geometrische Konstruktionen angeben, wie sich die Koordinaten abgeleiteter Punkte aus denen der "Basispunkte" ergeben.

Betrachten wir zunächst einen Punkt X auf der Geraden $g(AB)$. Für dessen Koordinaten ergibt sich aus der Punkt-Richtungsgleichung $X = A + b*(B-A)$ oder umgestellt $X = (1-b)*A+b*B$. b ist hierbei das Verhältnis der (vorzeichenbehafteten) Längen der Strecken AX und AB. Damit kann man den Parameter b als das *Teilverhältnis* $b = \frac{l(AX)}{l(AB)}$ berechnen. Wir erhalten die folgende **Darstellung durch baryzentrische Koordinaten**

$$X = \frac{l(XB)}{l(AB)} * A + \frac{l(AX)}{l(AB)} * B$$

Der Name rührt daher, daß nach den Hebelgesetzen X genau der Schwerpunkt eines Systems mit zwei in A und B konzentrierten Massen ist.

Satz 10 *Die Koordinaten jedes Punktes X einer Geraden $g(AB)$ lassen sich in der Form $X = (1-b)*A+b*B$ darstellen.*

Zwei solche Punkte sind genau dann gleich, wenn ihre baryzentrische Koordinate b *dieselbe ist.*

Für einen Punkt X der Ebene $\varepsilon(ABC)$ gibt es eine ähnliche Darstellung. Ist D der Schnittpunkt von $g(CX)$ und $g(AB)$, so gibt es Teilverhältnisse a, b mit

$$\begin{aligned} D &= a*A+(1-a)*b \\ X &= b*D+(1-b)*C \end{aligned}$$

also

$$X = ab*A+(1-a)b*B+(1-b)*C = x*A+y*b+z*C \text{ mit } x+y+z=1$$

Aufgabe: Zeigen Sie, daß die Parameter x, y, z mit Flächeninhalten von Teildreiecken wie folgt zusammenhängen:

$$x = \frac{F(BCX)}{F(ABC)}, y = \frac{F(ACX)}{F(ABC)}, z = \frac{F(ABX)}{F(ABC)}.$$

Satz 11 *Seien A, B, C drei nicht kollineare Punkte der Ebene.*

Die Koordinaten jedes Punktes X lassen sich dann in der Form $X = x*A+y*b+z*C$ mit geeigneten Zahlen x, y, z, für die $x+y+z=1$ gilt, darstellen.

Zwei solche Punkte sind genau dann gleich, wenn ihre baryzentrischen Koordinaten (x, y, z) *übereinstimmen.*

Beweis : Es bleibt nur zu zeigen, daß die baryzentrischen Koordinaten einen Punkt eindeutig bestimmen. Das folgt aber sofort aus der Beziehung

$$X = x*A+y*b+z*C = A+y*(B-A)+z*(C-A),$$

wonach sich wegen der linearen Unabhängigkeit der Vektoren $v(AB) = B - A$ und $v(AC) = C - A$ die Lage von X relativ zu A eindeutig ergibt. □ In einer beliebigen Punktekonfiguration bezeichnen wir drei fixierte nicht kollineare Punkte A, B, C als *Basispunkte*. Die baryzentrischen Koordinaten aller anderen Punkte bzgl. dieser Basispunkte sind dann eindeutig bestimmt.

Anwendungen:

1. Satz vom Schnittpunkt der Seitenhalbierenden

$D = \frac{1}{2} * A + \frac{1}{2} * B$ ist der Seitenmittelpunkt. Der Punkt S, der CD im Verhältnis 2:1 teilt, hat die baryzentrischen Koordinaten

$$S = \frac{1}{3} * C + \frac{2}{3} * D = \frac{1}{3} * (A + B + C)$$

Derselbe Punkt teilt also auch die beiden anderen Seitenhalbierenden im Verhältnis 2:1.

2. Satz vom Diagonalenschnittpunkt im Parallelogramm

Parallelogramm, also $B - A = D - C$. Dann fallen die Mittelpunkte $\frac{1}{2} * A + \frac{1}{2} * C$ und $\frac{1}{2} * B + \frac{1}{2} * D$ der beiden Diagonalen zusammen.

> Aufgabe: Beweisen Sie den Satz über iterierte Punktspiegelungen:
> Bezeichnet σ_O die Punktspiegelung mit Zentrum im Punkt O, so gilt für drei Punkte O_1, O_2, O_3
> $$(\sigma_{O_3} \circ \sigma_{O_2} \circ \sigma_{O_1})^2 = id$$

3. Dreieckstrisektion

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

$M = \frac{1}{2} * A + \frac{1}{2} * B,\ S = \frac{1}{2} * M + \frac{1}{2} * C$. N wird durch zwei Bedingungen beschrieben:

$$N = x * S + (1 - x) * A$$
$$N = y * B + (1 - y) * C$$

In der ersten Relation kommt noch S vor, was kein Basispunkt ist.

$$N = (1 - \tfrac{3}{4}x) * A + \tfrac{x}{4} * B + \tfrac{x}{2} * C$$

Aus der Eindeutigkeit der baryzentrischen Koordinaten erhalten wir durch Koeffizientenvergleich drei Gleichungen, von denen allerdings nur zwei voneinander unabhängig sind:

$$x + 2\,y - 2 = 0$$
$$x - 4\,y = 0$$
$$-3\,x + 4 = 0$$

woraus wir sofort die Lösung $(x = \frac{4}{3}, y = \frac{1}{3})$ ablesen können und sich die Behauptung ergibt.

Die entsprechenden Rechnungen kann man bereits einem CAS übertragen. Die folgenden Rechnungen wurden mit Reduce ausgeführt:

```
>> clear a,b,c;
>> m:=(a+b)/2;

      a + b
m := -------
        2

>> s:=(m+c)/2;

      a + b + 2*c
s := -------------
```

```
            4

>> n1:=x*S+(1-x)*A;

         - 3*a*x + 4*a + b*x + 2*c*x
n1 := ------------------------------
                     4

>> n2:=y*B+(1-y)*C;

n2 := b*y - c*y + c
```

Die Variablen n_1 und n_2 enthalten hierbei die beiden Bedingungen, die die Lage des Punktes N bestimmen. Zum Vergleich der entsprechenden baryzentrischen Koordinaten müssen wir aus $n_1 - n_2$ die Koeffizienten von A, B, C extrahieren. Da ein solch komplexes Anliegen meist nicht durch eine eingebaute Routine bearbeitet werden kann, müssen wir uns dazu eine eigene Prozedur schreiben:

```
procedure getcoord(u,base);
  % extract coordinates from list u wrt. base point list base.
  begin;
  for each x in base do u:=for each y in u join coeff(y,x);
  return u;
  end;
```

Wir erhalten damit für unser Beispiel schließlich

```
>> getcoord({n1-n2},{a,b,c});

    x + 2*y - 2   x - 4*y    - 3*x + 4
{0,-------------,---------,------------}
         2            4          4

>> solve(ws);

Unknowns: {x,y}

     4     1
{{x=---,y=---}}
     3     3
```

Ähnlich können wir generell für Sätze der affinen Geometrie vorgehen: Wähle in der Punktekonfiguration die Basispunkte und berechne die baryzentrischen Koordinaten der anderen Punkte bzgl. dieser Basispunkte aus gegebenen oder zu bestimmenden Teilverhältnissen. Koordinatenvergleich liefert dann eine Menge polynomialer Beziehungen zwischen den verschiedenen unbekannten Teilverhältnissen. Dieses Gleichungssystem ist dann zu lösen.

> Aufgabe: M teile die Seite AC des Dreiecks $\Delta\, ABC$ im Verhältnis $l(AM) : l(MC) = 1 : 2$. N liege auf $g(BC)$, so daß $l(NB) = l(BC)$ gilt. Schließlich sei P der Schnittpunkt von $g(MN)$ und $g(AB)$. In welchem Verhältnis teilt P die Strecke AB ?

4. Betrachten wir folgende Verallgemeinerung des Satzes vom Schwerpunkt:

   Im Dreieck $\Delta\, ABC$ seien auf den Seiten AB und AC und zwei Punkte P und Q gegeben, so daß die Teilverhältnisse $l(AP) : l(PB) = l(AQ) : l(QC) = x$ gleich sind. Dann liegt der Schnittpunkt der Strecken BQ und CP auf der Seitenhalbierenden durch A.

Als Basispunkte wählen wir die Eckpunkte A, B, C des Dreiecks. Für die beiden Punkte P, Q ergeben sich die folgenden baryzentrischen Koordinaten:

```
clear A,B,C;
P:=x*A+(1-x)*B;
Q:=x*A+(1-x)*C;
```

Die Koordinaten des Schnittpunkts Z der beiden Transversalen erfüllen dann

```
Z1:=u*B+(1-u)*Q;
Z2:=v*C+(1-v)*P;
```

mit geeigneten Parametern u, v. Diese können wir aus dem Vergleich der Koordinaten von Z gewinnen:

```
getcoord({Z1-Z2},{A,B,C});
sol:=solve(ws,{u,v});
```

Der erste Befehl extrahiert das entsprechende (lineare) Gleichungssystem

$$x\,u - x - u - v + 1 = -x\,v + x + u + v - 1 = -x\,u + x\,v = 0,$$

aus dem u, v in Abhängigkeit vom Parameter x zu bestimmen sind. Die Lösung lautet

$$u = v = \frac{x-1}{x-2}$$

Setzen wir die gefundenen Werte für u, v ein, so erhalten wir eine Formel für die baryzentrischen Koordinaten von Z bzgl. der Basispunkte, die nur noch vom Parameter x abhängt:

```
Z:=sub(sol,Z1);
```

$$Z = \frac{x}{2-x} * A + \frac{1-x}{2-x} * B + \frac{1-x}{2-x} * C$$

Um zu zeigen, daß Z auf der Seitenhalbierenden liegt, berechnen wir auf dieselbe Weise den Schnittpunkt M von $g(AZ)$ und $g(BC)$:

```
M1:=u*A+(1-u)*Z;
M2:=v*B+(1-v)*C;

getcoord({M1-M2},{A,B,C});
sol:=solve(ws,{u,v});
```

Wir erhalten

$$\{u = \frac{x}{2\,x-2}, v = \frac{1}{2}\},$$

woran bereits ersichtlich ist, daß M die Seite BC halbiert.

Ein elementarer Beweis des Satzes ergibt sich unmittelbar als Folgerung aus dem Satz von Ceva.

> Aufgabe: Gegeben sei ein Parallelogramm $ABCD$. Durch einen Punkt P in seinem Inneren seien die Parallelen zu den Seiten gelegt, die diese in den Punkten K, L, M, N schneiden. Q sei der Schwerpunkt des Vierecks $KLMN$, S der Schwerpunkt des Parallelogramms $ABCD$. Zeigen Sie, daß die drei Punkte P, Q, S auf einer Geraden liegen und bestimmen Sie das Teilverhältnis.

5. Betrachten wir als weiteres Beipsiel den Satz von Ceva:
Gegeben ΔABC, Punkte D, E, F auf den Dreiecksseiten, so daß AD, BE, CF sich in einem gemeinsamen Punkt P schneiden.

Vektorgeometrische Formulierung der Voraussetzungen: $\exists\ u, v, w, x, y, z$ mit

$$\begin{gathered} u * B + (1-u) * C = D \\ v * C + (1-v) * A = E \\ w * A + (1-w) * B = F \\ (1-x) * A + x * D = P \\ (1-y) * B + y * E = P \\ (1-z) * C + z * F = P \end{gathered}$$

Behauptung: $uvw - (1-u)(1-v)(1-w) = 0$.

Wir erhalten mit Reduce:

```
clear A,B,C;
D:=u*B+(1-u)*C;
Eh:=v*C+(1-v)*A;
F:=w*A+(1-w)*B;
P1:=(1-x)*A+x*D;
P2:=(1-y)*B+y*Eh;
P3:=(1-z)*C+z*F;

polys:=getcoord({p1-p2,p1-p3},{a,b,c});

polys := {- u*x - v*y + x, u*x + y - 1, v*y - x - y + 1,
- u*x + x + z - 1, u*x + w*z - z, - w*z - x + 1}$
```

Hier hilft die `Solve`-Routine allerdings nicht weiter, denn wir wollen ja aus den Gleichungen eine Beziehung zwischen u, v, w ableiten, deren Existenz etwa beim Auflösen nach x, y, z zur leeren Lösungsmenge führt. Wir wollen deshalb die Menge der Polynome geschickt aufteilen und aus einer ersten Teilmenge eine Darstellung von x, y, z durch u, v, w extrahieren und diese Darstellung in die zweite Teilmenge einsetzen. Auf diese Weise eliminieren wir die Variablen x, y, z aus unseren Gleichungen.

```
polys1:={ - u*x - v*y + x, u*x + y - 1, v*y - x - y + 1,
- u*x + x + z - 1}$

sol:=solve(polys1,{x,y,z});

          v
{{x=-------------,
     u*v - u + 1

       - u + 1
  y=-------------,
     u*v - u + 1

     2*u*v - u - v + 1
  z=-------------------}}
        u*v - u + 1


polys2:=sub(sol,{u*x + w*z - z, - w*z - x + 1});
```

```
  2*u*v*w - u*v - u*w + u - v*w + v + w - 1
{-----------------------------------------,
                 u*v - u + 1

   - 2*u*v*w + u*v + u*w - u + v*w - v - w + 1
 ---------------------------------------------}
                  u*v - u + 1
```

Wir sehen, daß wir aus beiden Polynomen der zweiten Teilmenge durch Substitution im Primzip dasselbe Ergebnis erhalten, in dessen Zähler die gesuchte Relation enthalten ist.

Wir haben damit in diesem Abschnitt einen ersten Ansatzpunkt für mechanisierte Beweise geometrischer Sachverhalte aus dem Bereich der affinen Geometrie kennengelernt.

3 Die Koordinatenmethode und geometrische Sätze vom konstruktiven Typ

3.1 Grundlegende geomtrische Zusammenhänge in koordinatengeometrischer Interpretation

Das übliche Vorgehen bei der Verwendung von Koordinaten besteht nicht wie im letzten Abschnitt in der Verwendung baryzentrischer Koordinaten, sondern in der Darstellung jedes Punktes aus der Punktekonfiguration durch zwei Parameter $P = (p_1, p_2)$, seine Koordinaten bzgl. eines fixierten Koordinatensystems. Mit diesen Parametern lassen sich auch Darstellungen für abgeleitete Objekte wie Geraden oder Kreise angeben.

In diesem Abschnitt wollen wir die wichtigsten aus der Schule und dem Grundkurs Mathematik bekannten koordinatengeometrischen Zusammenhänge zusammenstellen und zeigen, wie man diese durch entsprechend gestaltete Datentypen für mechanisierte Beweisverfahren in Form von Funktionen und Prozeduren für eine klassische Programmiersprache aufbereiten kann.

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

$P = (p_1, p_2)$ bezeichnet dabei den Punkt P mit den Koordinaten (p_1, p_2), während $g = (g_1, g_2, g_3)$ die Gerade $g_1x_1 + g_2x_2 + g_3 = 0$ bezeichnet. Letztere Darstellung nennt man *homogene Koordinaten* der Geraden g. Die wichtigsten geometrischen Eigenschaften 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".

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

  Man beachte an dieser Stelle, daß die homogenen Koordinaten einer Geraden nur bis auf einen skalaren Faktor eindeutig bestimmt sind.
- Damit ergeben sich die Parameter der Parallelen h zu g durch einen Punkt P 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
$$(p_1, p_2) = (\frac{d_1}{d}, \frac{d_2}{d}) \quad \text{mit} \quad d = \begin{vmatrix} g_1 & g_2 \\ h_1 & h_2 \end{vmatrix}, d_1 = \begin{vmatrix} g_2 & g_3 \\ h_2 & h_3 \end{vmatrix}, d_2 = \begin{vmatrix} g_3 & g_1 \\ h_3 & h_1 \end{vmatrix}$$
- 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 weitgehend 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 aueinander 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
$$(h_1, h_2, h_3) = (g_2, -g_1, g_1 p_2 - g_2 p_1).$$

3.2 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`.

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 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 point(Line g,Line h) {
  Scalar d=g.a*h.b-g.b*h.a;
  if (d==0) 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 lot(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(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 Point((p.x+q.x)/2, (p.y+q.y)/2);
}
```

den Mittelpunkt der Strecke PQ.

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

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

die Mittelsenkrechte auf der Seite BC im Dreieck ABC als

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

die Höhe entsprechend als

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

und die Seitenhalbierende als

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

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:

```
parallel(g,h:Line):Boolean== (g.a*h.b-h.a*g.b = 0)
```

bzw.

```
orthogonal(g,h:Line):Boolean== (g.a*h.a+g.b*h.b = 0)
```

```
pointOnLine(P:Point,g:Line):Boolean== (g.a*P.x+g.b*P.y+g.c = 0)
```

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 `collinear(A,B,C:Point):Boolean` bzw. `concurrent(a,b,c:Line):Boolean`.

> Aufgabe: Führen Sie die Implementierung entsprechender Funktionen wie oben begonnen in einer klassischen Programmiersprache (Pascal oder C bzw. C++) 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

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

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

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

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

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

zu testen, d.h. die letzte Zeile durch

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

zu ersetzen.

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

Beispiel 2: Der Satz von der Eulerschen Geraden:

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

> Aufgabe: Modifizieren Sie das Programm so, daß es den Satz vom Feuerbachschen Kreis testet. Schreiben Sie Programme, mit denen man weitere Sätze prüfen kann, so die oben betrachtete iterierte Punktspiegelung, die Dreieckstrisektion oder den Satz von Desargue.

3.3 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: 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 `point(mp(A,B,C),mp(B,C,A))` in

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

die Komponenten von m, n durch die entsprechenden rationalen Ausdrücke

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

bzw.

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

zu ersetzen sind. Diese Ausdrücke sind ihrerseits während des Aufrufs

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

in einem Substitutions- und Simplifikationsprozeß (der Tiefe 2) nach demselben Prinzip entstanden. 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.3` 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 `point` und `choosePoint`, wo die entsprechenden Nenner nicht verschwinden dürfen. Eine Modifikation der Funktionen erlaubt es, die (Zähler der) entsprechenden Nichtdegenerationsbedingungen in einer global definierten Liste aufzusammeln.

3.4 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* $f \in R$, 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 12 *(Über das mechanisierte Beweisen geometrischer Sätze vom konstruktiven Typ):*
Eine geometrische Behauptung g vom konstruktiven Typ in einer (nicht widersprüchlichen) AGK (M, f), die in endlich vielen Konstruktionsschritten aus der leeren AGK $\{\emptyset, 1\}$ gewonnen worden ist, gilt genau dann, wenn g als rationale Funktion in K identisch Null ist.

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

ϕ mit $\phi_R(p) \cdot \phi_R(q) \neq 0$, d.h. $\phi_K(g) \neq 0$. $\square$

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.

4 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=varpoint(B,C,u)`, `E=varpoint(C,A,v)`, `F=varpoint(A,B,w)` auf den Dreiecksseiten. Wenn dann 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:={a1,a2}; B:={b1,b2}; C:={c1,c2};
D:=varpoint(B,C,u);
E:=varpoint(C,A,v);
F:=varpoint(A,B,w);

pre:=concurrent(line(A,D),line(B,E),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.

Analysiert man die beiden anderen Faktoren genauer, so erkennt man, daß sie genau der Bedingung `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:={a1,a2}; B:={b1,b2}; C:={c1,c2};
D:={d1,d2}; Eh:={e1,e2}; F:={f1,f2};

pre:={ parallel(line(A,B),line(D,Eh)),
       parallel(line(B,C),line(Eh,F)),
       parallel(line(A,C),line(D,F))};

con:=concurrent(line(A,D),line(B,Eh),line(C,F));
```

Die Voraussetzung entspricht hier also einer Menge von drei Polynomen

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

die Behauptung dem deutlich komplizierteren Polynom

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

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:={0,0}; B:={0,1}; C:={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);

    e1*f2*( - e1 - e2 + f1 + f2)
```

woran wir erkennen, daß jede gemeinsame Nullstelle von *pre* auch eine Nullstelle von *con* ist.

Aufgabe: 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.

4.1 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

$$(x - x_0)^2 + (y - y_0)^2 - r^2 = (x^2 + y^2) + c_1\,x + c_2\,y + c_3$$

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.

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

```
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

$$\begin{gathered}2 * m_1 * (-a_1 + b_1) + 2 * m_2 * (-a_2 + b_2) + a_1^2 + a_2^2 - b_1^2 - b_2^2,\\ 2 * m_1 * (-a_1 + c_1) + 2 * m_2 * (-a_2 + c_2) + a_1^2 + a_2^2 - c_1^2 - c_2^2\end{gathered}$$

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 übereinstimmt, verschieden von 0 ist.

```
solve(polys,M);
```

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:=point(mp(A,B,C),mp(B,C,A));
```

Drei Punkte bestimmen also einen Kreis eindeutig, genau wie zwei Punkte eine Gerade eindeutig bestimmen. Wir wollen deshalb als nächstes charakterisieren, wann 4 Punkte A, B, C, D auf einer gemeinsamen Kreislinie liegen. Wir bestimmen dazu die Koordinaten des Umkreismittelpunkts M von ABC

```
M:=point(mp(A,B,C),mp(B,C,A));
```

Die gesuchte Bedingung lautet dann

```
uhu:=sqrdist(M,A)-sqrdist(M,D);
```

Wir erhalten (wenn man den Bruch kürzt), ein Zählerpolynom p vierten Grades, das die entsprechende Bedingung beschreibt. Wir können auch dieses Polynom extrahieren und als Prozedur zur weiteren Verwendung in unsere Programmsammlung aufnehmen.

Satz 13 *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*

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

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

die Fußpunkte der Lote aus D auf die drei Seiten des Dreiecks ABC oder deren Verlängerungen. Der Satz von Simson behauptet, daß D genau dann auf dem Umkreis von ABC liegt, wenn R, S, T kollinear sind. Die Voraussetzung *pre* wird genau durch das oben hergeleitete Polynom p 4. Grades charakterisiert. Die Behauptung

```
con:=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.

Auf ähnliche Weise kann man auch den folgenden Satz herleiten.

Satz 14 (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:

$$\begin{aligned}&(a\,c)^2 + (b\,d)^2 - (e\,f)^2 = 2\,a\,b\,c\,d\\ &((a\,c)^2 + (b\,d)^2 - (e\,f)^2)^2 - (2\,a\,b\,c\,d)^2 = 0\end{aligned}$$

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.

Für kompliziertere Anwendungen, die stärker auf einem analytischen Ansatz beruhen, ist es natürlich besser, mit der zweiten Kreisdarstellung zu arbeiten.

> Aufgabe: Bestimmen Sie Formeln, mit denen man aus Zentrum und Radius die drei Parameter $c = (c_2, c_3, c_4)$ berechnen kann und umgekehrt.

Ist `circle(M,s)` eine Funktion, die aus Zentrum M und Sqradius s die entsprechenden Parameter c bestimmt, so ergeben sich die Parameter des Kreises durch die drei Punkte A, B, C zu

```
A:={a1,a2}; B:={b1,b2}; C:={c1,c2};
M:=point(mp(A,B,C),mp(B,C,A));
circle(M,sqrdist(M,A));
```

Die Parameter dieses Kreises sind rationale Funktionen der Parameter der Punkte A, B, C, wobei im Nenner wiederum das Polynom $collinear(A, B, C)$ 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.

Vier Punkte $A = (a_1, a_2), B = (b_1, b_2), C = (c_1, c_2), D = (d_1, d_2)$ liegen damit genau dann auf einem gemeinsamen Kreis, wenn es eine nichttriviale Lösung $x = (x_1, x_2, x_3, x_4)$ des Gleichungssystems

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

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. Dies ist genau die Bedingung aus obigem Satz.

Wir können auf dieser Basis nun den Satz vom Miquelschen Punkt in Angriff nehmen. Die allgemeine geometrische Konfiguration, in der der Satz formuliert wird, lautet:

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

Die Behauptung lautet hier, daß die drei Kreise durch AST, BRT und CRS durch einen gemeinsamen Punkt gehen. Eine mögliche algebraische Formulierung dieser Behauptung könnte etwa lauten

> Es gibt einen Punkt $P = (x_1, x_2)$, so daß die drei Gleichungen

```
polys:={four_points_on_a_circle(A,S,T,P),
four_points_on_a_circle(B,R,T,P),
four_points_on_a_circle(C,R,S,P)};
```

als Gleichungen in (x_1, x_2) mit rationalen Koeffizienten in den Koordinaten der beteiligten Punkte verstanden, eine gemeinsame Lösung haben.

Die gemeinsamen Lösungen der drei Polynome, jeweils vom Grad 2 in x_1 und x_2, die in den speziellen Koordinaten

```
A:={0,0}; B:={0,b2}; C:={c1,c2};
```

bereits 32, 28 und 22 Terme haben, kann man mit Hilfe des `solve`-Operators (und einiger Geduld) noch gerade so finden:

```
solve(polys,P);
```

Wir können auch zuerst eine Bedingung auf die allgemeinen Kreisparameter b, c, d finden, unter denen drei gegebene Kreise durch einen gemeinsamen Punkt gehen. Dazu ist obiges Eliminationsproblem allgemein zu lösen:

```
P:={x,y};
polys:={point_on_circle1(P,{b1,b2,b3,b4}),
    point_on_circle1(P,{c1,c2,c3,c4}),
    point_on_circle1(P,{d1,d2,d3,d4})};

load cali;
vars:={x,y,b1,b2,b3,b4,c1,c2,c3,c4,d1,d2,d3,d4};
setring(vars,{},lex);
eliminate(polys,{x,y});
```

Im Ergebnis erhalten wir ein Polynom vom Grad 6 mit 75 Termen, das die Bedingung beschreibt, wann drei gegebene Kreise durch einen gemeinsamen Punkt gehen.

Ein wichtiges Problem, das im Zusammenhang mit nichtlinearen Bedingungen auftritt, ist die Tatsache, daß, im Gegensatz zu obigen Koordinaten des Miquelschen Punkts, Schnittpunktkoordinaten oft nicht mehr rational durch die Ausgangskoordinaten ausgedrückt werden können. So erhalten wir etwa für die Schnittpunkte zweier Kreise mit den Radien r_1 und r_2 und dem Mittelpunktsabstand $2u$

```
polys:={
    point_on_circle1(P,circle({-u,0},r1^2)),
    point_on_circle1(P,circle({u,0},r2^2))};

solve(polys,P);
```

als Ergebnis

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

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(line(A,B),line(P,B));
v:=angle(line(P,B),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 point_on_bisector(P,A,B,C);
  begin scalar u,v;
  u:=angle(line(A,B),line(P,B));
  v:=angle(line(P,B),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: 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 die folgende algebraische Formulierung verwenden:

```
A:={0,0}; B:={0,1}; C:={c1,c2}; P:={x,y};

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

Zur Vereinfachung der Rechnungen gehen wir dabei von einem speziellen Koordinatensystem aus. Es ist wiederum zu beweisen, daß die drei Polynome eine gemeinsame Lösung in (x, y) besitzen, wobei die anderen Variablen als Parameter zu verstehen sind. In diesem Fall ist das Lösen allerdings um Größenordnungen schwieriger als in den bisher betrachteten Beispielen, da es nicht eine, sondern vier verschiedene Lösungen gibt, den Inkreismittelpunkt und die drei Ankreismittelpunkte des gegebenen Dreiecks. Eine genauere Analyse des Gleichungssystems zeigt diese Struktur auch recht deutlich.

Alternativ hätten wir folgendermaßen vorgehen können: Wir bestimmen die Koordinaten des Schnittpunkts zweier der Winkelhalbierenden und prüfen, daß dieser Punkt auch auf der dritten Winkelhalbierenden liegt. Die Voraussetzung

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

solve(polys,P);
```

ergibt wiederum vier nichtrationale Lösungen (zudem komplizierter Bauart), so daß direktes Substituieren auch hier nicht möglich ist, sondern andere Prinzipien zum Beweisen herangezogen werden müssen.

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

> AUFGABE: 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.

4.2 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 $PF = PG$.

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:={u2,x1}; C:={u3,x2}; D:={u4,x3};
```

$P = (x_4, x_5)$ 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:={0,0}; A:={u1,0}; B:={u2,x1}; C:={u3,x2}; D:={u4,x3};
P:={x4,x5};
h:=lot(P,line(O,P));
F:={x6,x7}; G:={x8,x9};

polys:={sqrdist(O,B)-u1^2, sqrdist(O,C)-u1^2, sqrdist(O,D)-u1^2,
        point_on_line(P,line(A,C)), point_on_line(P,line(B,D)),
        point_on_line(F,h), point_on_line(F,line(A,D)),
        point_on_line(G,h), point_on_line(G,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)

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

polys:={sqrdist(O,B)-sqrdist(O,A),
        sqrdist(O,C)-sqrdist(O,A),
        sqrdist(O,D)-sqrdist(O,A),
        point_on_line(P,line(A,C)), point_on_line(P,line(B,D)),
        point_on_line(F,line(A,D)), point_on_line(G,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: 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.

4.3 Ideale und Nullstellengebilde

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, das von dieser Menge erzeugt wird, denn es gilt offensichtlich $Z(F) = Z(I(F))$.

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: 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.

Mengen, die sich als Nullstellengebilde $Z(I)$ eines Ideals darstellen lassen, bezeichnen wir als *algebraische Mengen*.

Umgekehrt kann man nach denjenigen Polynomen fragen, die auf einer vorgegebenen Menge Z verschwinden:

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

Es stellt sich heraus, daß $J(Z)$ selbst wieder ein Ideal ist. Allerdings ist der Zusammenhang zwischen Idealen und Nullstellenmengen nicht so einfach wie in der linearen Algebra, wo beide Begriffe ja im wesentlichen dual zueinander sind. 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.

Um diese Unbestimmtheit zu eliminieren, wollen wir zusammen mit jedem Ideal I auch das größte Ideal mit derselben Nullstellenmenge, das *Radikal* $rad(I)$ von I betrachten. 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. daß

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

gilt. Die Bestimmung einer Basis des Radikals ist recht schwierig. Die meisten als allgemeine geometrische Voraussetzungen auftretenden Ideale sind allerdings bereits *Radikalideale*, d.h. solche, für die $I = rad(I)$ gilt. Ebenso ist offensichtlich $J(Z)$ ein Radikalideal.

Es stellt sich heraus, daß die Zuordnung, die einer algebraischen Menge Z ihr (Radikal)-Ideal $J(Z)$ zuordnet und die Zuordnung, die einem Radikalideal I dessen Nullstellengebilde $Z(I)$ zuordnet, zueinander inverse inklusionsumkehrende Zuordnungen zwischen Radikalidealen und Nullstellengebilden sind.

> AUFGABE: Startet man bei einem Ideal I, geht zur Nullstellenmenge $Z = Z(I)$ über und untersucht dann das Ideal $J(Z)$, so erhält man $rad(I)$.
>
> Zeigen Sie daß die Beziehung auf der Seite der algebraischen Mengen nicht so kompliziert ist, daß nämlich die Nullstellenmenge $Z(J)$ des Ideals $J = J(Z)$ einer algebraischen Menge Z bereits wieder Z ergibt.

Sehen wir einmal von der Nichtdegenerationsbedingung h ab, läßt sich ein Satz vom Gleichungstyp

g verschwindet auf allen gemeinsamen Nullstellen des Polynomsystems F

demzufolge auf die Frage $g \in rad(I(F))$ zurückführen. Eine dafür hinreichende Bedingung ist $g \in I(F)$, die im Falle eines Radikalideals sogar zur Ausgangsfrage äquivalent ist. Idealenthaltenseinstests spielen also im Weiteren eine zentrale Rolle.

Die eben beschriebene Zuordnung wollen wir noch etwas genauer betrachten. Eine algebraische Menge Z heißt *reduzibel*, wenn sie sich als Vereinigung zweier echter algebraischer Teilmengen $Z = Z_1 \cup Z_2$ darstellen läßt. Für die zugehörigen Ideale gilt dann offensichtlich $J(Z) = J(Z_1) \cap J(Z_2)$.

Eine nicht weiter zerlegbare algebraische Menge heißt *irreduzibel*. Solchen Mengen entsprechen Primideale, d.h. solche Ideale I, für die

$$f \cdot g \in I \;\Rightarrow\; f \in I \text{ oder } g \in I$$

gilt.

Satz 15 *Die algebraische Menge Z ist genau dann irreduzibel, wenn $J(Z)$ ein Primideal ist.*

Beweis : Ist $Z = Z_1 \cup Z_2$ zerlegbar, so gilt $J(Z) = J(Z_1) \cap J(Z_2)$, aber $J(Z) \neq J(Z_i),\ i = 1, 2$. Wähle $f_i \in J(Z_i) \setminus J(Z)$. Dann ist $f = f_1 \cdot f_2$ als Vielfaches von f_1 in $J(Z_1)$ und als Vielfaches von f_2 in $J(Z_2)$, also in $J(Z) = J(Z_1) \cap J(Z_2)$ enthalten.

Ist umgekehrt $I = J(Z)$ nicht prim, also existiert $f = f_1 \cdot f_2$ mit $f_1, f_2 \notin I$, so ergibt $Z = Z(I + I(f_1)) \cap Z(I + I(f_2))$ eine nichttriviale Zerlegung von Z. $\square$

Jedes Radikalideal läßt sich in einem Noetherschen Ring als Durchschnitt endlich vieler Primideale darstellen.

Folglich läßt sich jede algebraische Menge als endliche Vereinigung irreduzibler algebraischer Mengen darstellen. Diese Teile nennt man die *Komponenten* der Menge Z.

Betrachten wir als Beispiel einen zweiten Beweis des Satzes vom Miquelschen Punkt. Wir verwenden die Formulierung "Wenn P der Schnittpunkt zweier der Kreise ist, dann liegt er auch auf dem dritten Kreis". In speziellen Koordinaten läßt sich die Frage wie folgt kodieren:

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

P:={x1,x2};

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

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

Es stellt sich heraus, daß in diesem Fall $Z(polys)$ aus zwei Teilen besteht, wobei auf einem Teil die Behauptung richtig ist, auf dem zweiten Teil dagegen nicht:

```
load cali;
setring(P,{},lex);
uhu:=isolatedprimes polys;
length uhu;
for each x in uhu collect con mod x;
```

Die Nullstellenmenge der geometrischen Bedingungen *polys* besteht also aus zwei Komponenten, wobei auf einer von ihnen die Behauptung *con* zu Null reduziert, auf der anderen hingegen nicht. Eine genauere Analyse zeigt, daß dies nicht verwunderlich ist, denn die beiden in der Voraussetzung auftretenden Kreise schneiden sich außer in P natürlich noch in T. Dies könnte man durch eine entsprechende Nichtdegenerationsbedingung $h = x_1$ (was bedeutet, daß P nicht auf der Geraden AB liegen darf) ausschließen.

Betrachten wir zum Abschluß noch den Einfluß von Nichtdegenerationsbedingungen. Offensichtlich ist $Z(F) \setminus Z(h)$ 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 $Z(F) \setminus Z(h)$ enthält, die also vom Ideal $J(Z(F) \setminus Z(h))$ beschrieben wird. Das ist offensichtlich genau die Menge

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

Aufgabe: 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*

$$(F = 0,\; h \neq 0 \;\Rightarrow\; g = 0)$$

läßt sich als der stabile Idealquotient

$$J = I(F/g) = I(F) : g^\infty$$

berechnen.

Wegen $Z(h) \supset Z(J)$ für $h \in J$ kann dabei *jedes* Element aus $I(F/g)$ als Nichtdegenerationsbedingung verwendet werden. Insbesondere gibt es keine "minimale" Nichtdegenerationsbedingung, wenn das Ideal J von mehreren Polynomen erzeugt wird.

4.4 Idealtest, Normalformen und Gröbnerbasen

Wir hatten im vorigen Abschnitt gesehen, daß beim mechanisierten Beweisen von Geometrietheoremen vom Gleichungstyp Polynome $g \in R$, die auf einer vorgegebenen Nullstellenmenge $Z = Z(I)$ ebenfalls verschwinden, eine zentrale Rolle spielen. Wir wollen hier die allgemeinere Frage nach Polynomen $f, g \in R$ untersuchen, die in allen Punkten von Z dieselben Werte annehmen. Dies ist offensichtlich genau dann der Fall, wenn $f - g$ auf ganz Z verschwindet. Die (etwas stärkere) zugehörige algebraische Bedingung lautet $f - g \in I$.

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 $F = \{f_1, \ldots, f_m\}$, 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.*

Damit steht mit der Idealbasis F eine gewisse Menge von Ersetzungsregeln zur Verfügung, die man auf ein gegebenes Polynom $f \in R$ anwenden kann, um es durch ein anderes, in einem noch zu präzisierenden Sinne "einfacheres" Polynom f' mit $f \equiv f' \ (mod\ I)$ zu ersetzen. Auf das Ergebnis kann man die Ersetzungsregeln wiederum anwenden und so fortfahren, bis keine Ersetzungen mehr ausgeführt werden können.

Ohne spezielle Vorkehrungen kann sich ein solches Ersetzungsverfahren natürlich im Kreis drehen. Um dies zu vermeiden wollen wir (in einem zu spezifizierenden Sinne) stets "größere" durch "kleinere" Terme ersetzen. Wir halten dazu auf dem Termmonoid $T = T(x_1, \ldots, x_n)$ 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. Da jedoch T aus unendlich vielen Termen besteht, garantiert das noch nicht die Termination. Wir müssen dafür zusätzlich fordern, daß es keine unendlichen streng absteigenden Ketten $m_1 > m_2 > \ldots$ 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.

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. 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

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

Die Umkehrung gilt, wie auch bei Unterraumtests in der linearen Algebra, nicht unbedingt. Um bei einem entsprechenden Reduktionsverfahren in der linearen Algebra in einem gegebenen Unterraum enthaltene Vektoren stets als solche zu erkennen, benötigen wir eine Basis G des Unterraums in Dreiecksform. Ähnlich kann man auch im nichtlinearen Fall eine Basis F so in eine andere Basis G umformen, daß

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

gilt. Eine solche Basis bezeichnet man als *Gröbnerbasis*. Für eine solche Gröbnerbasis ist außerdem das Ergebnis der Normalformberechnung unabhängig vom gewählten Reduktionsweg.

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:={0,0}; B:={1,0}; C:={1,1}; D:={0,1}; P:={x1,x2}; Q:={x3,1};

polys:={point_on_line(P,par(C,line(B,D))),
      sqrdist(B,D)-sqrdist(B,P),
      point_on_line(Q,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

```
vars:={x1,x2,x3};
load cali;
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. Formt man diese Basis dagegen in Dreiecksform um

```
gbasis polys;
```

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

so 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 $Z = Z(I)$ in die beiden Teile $Z(I + I(f_1)) \cup Z(I + I(f_2))$. 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 $Z(F) = \cup_i Z(G_i)$ gilt. Diese Variante des Gröbneralgorithmus bezeichnet man als den *Gröbnerfaktorisierer*. Obwohl dies nicht garantiert werden kann, ist die dabei produzierte Zerlegung in praktischen Anwendungen oft nahe an der Primideal-Zerlegung.

Betrachten wir das Beispiel des Schnittpunkts der Winkelhalbierenden:

```
A:={0,0}; B:={1,0}; C:={c1,c2}; P:={x,y};

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

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

vars:={x,y,c1,c2};
setring(vars,{},lex);
uhu:=groebfactor polys;
for each x in uhu 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

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

Die faktorisierte Gröbnerbasis besteht aus zwei Komponenten, wovon auf der einen $con \equiv 0$ 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.

4.5 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 $Z(I)$. 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.

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:={u1,u2}; B:={u3,u4}; C:={u5,u6};

P:={u7,u8}; Q:={u9,x1}; R:={x2,x3};

pre:={  parallel(line(A,C),line(P,R)),
        parallel(line(B,C),line(Q,R)),
        parallel(line(A,B),line(P,Q))};

con:=   concurrent(line(A,P),line(B,Q),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:={u7,x1}; Q:={u8,x2}; R:={u9,x3};
pre:={  parallel(line(A,C),line(P,R)),
        parallel(line(B,C),line(Q,R)),
        parallel(line(A,B),line(P,Q))};
```

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

```
solve(pre,{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.

4.6 Geometrietheoreme vom linearen Typ

Untersuchen wir nun zunächst 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 17 *(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: 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: Beweisen Sie auf diese Weise den Satz von Pappus.

4.7 Generisch gültige Geometrietheoreme

Im Fall der Geometrietheoreme vom konstruktiven Typ haben wir also 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 Algebra in $\mathbf{x}$ über einem solchen Funktionenkörper treiben, d.h. unsere Rechnungen im Ring $S' = k(\mathbf{u})[\mathbf{x}]$ statt wie bisher im Ring $S = k[\mathbf{u}, \mathbf{x}]$ ausführen.

Betrachten wir zunächst einige Beispiele.

Beispiel 1 : Satz vom Miquelschen Punkt

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

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

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

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

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

Diese Gröbnerbasis hat eine recht einfache Struktur

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

so daß das zugehörige Gleichungssystem zwei Lösungen (x_1, x_2) mit $x_{1.1} = 0$ und $x_{1.2} = -\frac{p_2(\mathbf{u})}{p_1(\mathbf{u})}$ besitzt. Die erste Lösung entspricht dem Schnittpunkt F der beiden Kreise, die zweite dem Punkt P und erfüllt die Gleichung *con*.

Beispiel 2 : Satz vom Schnittpunkt der Winkelhalbierenden

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

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

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

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

Als Gröbnerbasis erhalten wir hier

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

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

Beispiel 3 : Die Simsonsche Gerade

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

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

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

xvars:=reverse for i:=1:7 collect mkid(x,i);
setring(xvars,{},lex);

setideal(polys,polys);

gbasis polys;

con mod ws;
```

Die Gröbnerbasis des entsprechenden Gleichungssystems

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

besteht aus Gleichungen vom Grad 1 und 2 in den abhängigen Variablen und erlaubt es wieder, die abhängigen Variablen durch die unabhängigen auszudrücken, wenn es auch 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 auf *allen* diesen Nullstellen verschwindet, braucht man aber nicht in dieser Erweiterung zu rechnen, sondern kann die Aussagen aus der Idealtheorie, die wir oben allgemein zusammengetragen haben, auf diesen speziellen Kontext anwenden.

Ist $F \subset k[\mathbf{u},\mathbf{x}]$ ein System von Polynomen, so betrachten wir das Ideal $I' = I_{S'}(F)$, das von diesen Polynomen in S' erzeugt wird. $\mathbf{u}$ ist eine maximale Menge von unabhängigen Variablen, wenn alle anderen Variablen algebraisch über $k(\mathbf{u})$ sind und damit 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. Eine notwendige Bedingung ist $g \in I'$, die für Radikalideale wieder äquivalent zum Verschwinden auf allen Nullstellen ist.

$g(\mathbf{x},\mathbf{u}) \in I'$ 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 18 *(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, für den $\mathbf{u}$ eine maximal unabhängige Teilmenge der Variablen ist.

Gilt $g \in I' = I_{S'}(F)$ als Polynome in $S' = k(\mathbf{u})[\mathbf{x}]$, etwa weil $NF(g,\texttt{gbasis}_{S'}(F)) = 0$, 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 $(F/h \Rightarrow g)$ gilt.

Wie oben gesehen kann man die Nichtdegenerationsbedingung h aus der polynomialen Darstellung von g durch $f \in F$ gewinnen. Eine solche Darstellung kann man mit einiger Mühe aus der Berechnung einer Gröbnerbasis $G = gbasis(F)$ und der Normalformberechnung $NF(g,G) = 0$ extrahieren. Die Menge derjenigen Spezifikationen der unabhängigen Parameter, für die $h(\mathbf{u}_0) = 0$ gilt, ist jedoch nur eine Hyperfläche im Parameterraum, 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 $NF(g,\texttt{gbasis}_{S'}(F))$ 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. F erzeugt also auch in diesem Ring ein Ideal $I' = I \cdot S'$, das *Erweiterungsideal* von I. Umgekehrt können wir mit einem Ideal $I' \subset S'$ das Ideal $c(I') := I' \cap S$ ins S verbinden, das aus allen rationalen Kombinationen der Erzeugenden besteht, "in denen sich die Nenner wegkürzen". $c(I')$ bezeichnet man als das *Kontraktionsideal* von I'. 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 19

(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 $u \in P_\alpha$. $\square$

Korollar 1

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

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

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

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

Generell, wenn $NF(h, G)$ 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 $Z(I)$ zwei generische Komponenten. Eine entspricht dem Schnittpunkt F der Kreise durch A, F, E und B, F, D, die andere dem gesuchten Schnittpunkt X. Auf der ersteren Komponente gilt der Satz nicht, auf der zweiteren sehr wohl. Der Gröbnerfaktorisierer zeigt, daß $Z(I)$ daneben noch wenigstens 5 weitere spezielle Komponenten hat, die die Bedingungen $u_2 = 0, u_5 = 0, u_3 = 1, u_5 = 1$ und $u_3 = u_5 = 1$ enthalten, also degenerierten Lagen entsprechen, wo z.B. zwei der drei Punkte, die einen Kreis bestimmen sollen, zusammenfallen. In einem solchen Fall ist aber der Kreis und damit auch der Schnittpunkt X nicht mehr eindeutig bestimmt, so daß wir auch nicht prüfen können, ob er auf dem dritten Kreis liegt.

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. *Contemp. Math.*, 19:243 – 286, 1984.

[2] H.S.M. Coxeter and S.L. Greitzer. *Geometry revisted.* Toronto - New York, 1967. Russ. Übersetzung: Nauka 1978.

[3] E. Donath. *Die merkwürdigen Punkte und Linien des ebenen Dreiecks.* Mathematische Schülerbücherei, Band 44. Deutscher Verlag der Wissenschaften Berlin, 1969.

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