

Theorie und Visualisierung algebraischer Kurven und Flächen

(Fortbildung für Mathematiklehrer)

Stephan Klaus
Oliver Labs
Thomas Markwig
Mathematisches Forschungsinstitut
Oberwolfach

Vortragsausarbeitung

März 2009

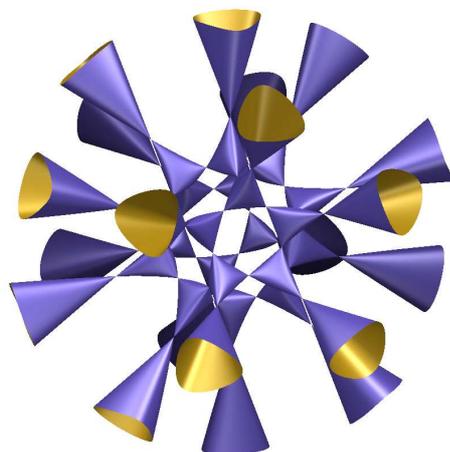
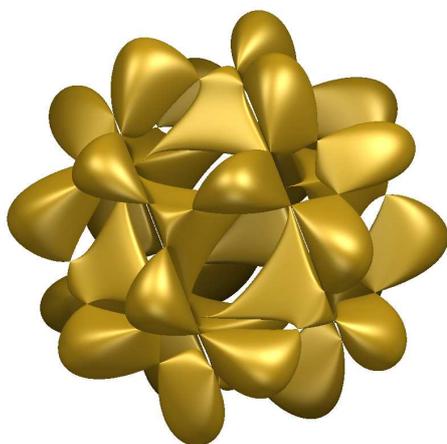
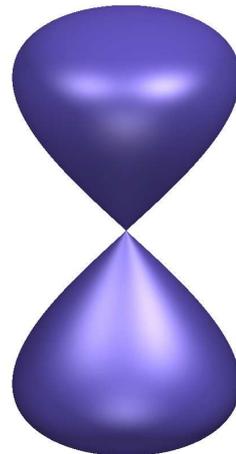
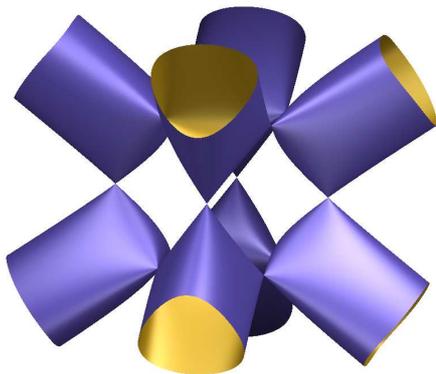
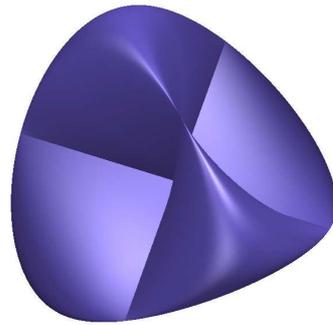
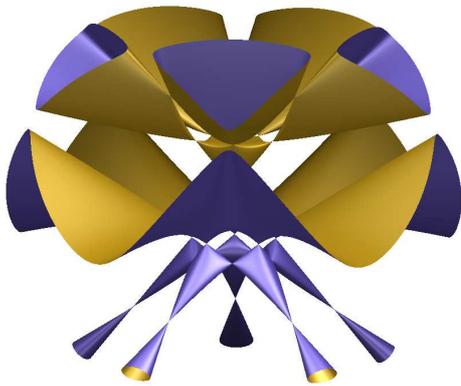
INHALTSVERZEICHNIS

1. WAS IST ALGEBRAISCHE GEOMETRIE?	1
2. KEGELSCHNITTE	30
3. DIE PROJEKTIVE EBENE	31
4. DER SATZ VON BÉZOUT	55
5. SINGULARITÄTEN	76
6. ENUMERATIVE GEOMETRIE	77
7. ANGEWANDTE ALGEBRAISCHE GEOMETRIE	112
8. SURFEX	128
LITERATUR	129

1 WAS IST ALGEBRAISCHE GEOMETRIE?

(VON THOMAS MARKWIG)

Das ist algebraische Geometrie



A) Implizite Darstellungen versus Parametrisierungen

Ich habe in einer Veranstaltung mit dem Titel *Elementarmathematik vom höheren Standpunkt aus* angehenden Lehrern die Frage gestellt, was eine Gerade ist. Folgende Antworten habe ich erhalten:

- Eine Gerade ist eine Aneinanderreihung von Punkten.
- Eine Gerade ist eine Linie.
- Eine Gerade ist wie eine Strecke, nur ohne Ende.
- Eine Gerade ist durch eine Gleichung der Form $y = m \cdot x + n$ gegeben.

Keine der Antworten ist falsch, und zugleich erklärt keine der Antworten zufriedenstellend, was eine Gerade ist. Dabei handelt es sich bei einer Geraden doch um ein wirklich elementares geometrisches Objekt, von dem jeder eine recht klare Vorstellung hat. Es ist bezeichnend, daß es uns schwer fällt, diese klare Vorstellung in klare Worte zu fassen, selbst nach einigen Semestern Mathematikstudium. Ich will mich deshalb selbst an einer Definition versuchen, an deren Ende zwei mögliche Beschreibungen stehen, die ein erstes Gefühl dafür geben sollen, was algebraische Geometrie ist und weshalb sie hilfreich ist.

Der Geometrieunterricht (der Mittelstufe) beruht heute noch genauso wie vor zweihundert Jahren auf Euklids *Elementen* [Euk91], und Euklid führt unmittelbar nach dem Punkt den Begriff der Geraden ein als:

Eine Gerade ist breitenlose Länge.

Nach meinem Verständnis ist diese Definition weder exakter noch hilfreicher als die oben angeführten. Ihnen allen ist gemein, daß sie gewisse Eigenschaften angeben, die Geraden erfüllen sollen; ihnen allen fehlt aber ein wichtiger Aspekt, den zweifellos alle ungesagt unterstellen:

Eine Gerade ist eine Menge, deren Elemente wir Punkte nennen, und die gewisse Eigenschaften hat.

Erst wenn wir wissen, daß eine Gerade eine Menge ist, können wir versuchen Eigenschaften zu spezifizieren, die die Punkte dieser Menge erfüllen sollen, so daß die Menge eine Gerade wird.

Nun wollen wir Eigenschaften festlegen, die die Punktmenge erfüllen muß, um eine Gerade genannt zu werden. Diese hängen letztlich vom Standpunkt ab, den man einnehmen möchte.

In der axiomatischen Geometrie gibt man sich einen umgebenden Raum als Punktmenge vor sowie gewisse Teilmengen dieses Raumes, die die Geraden werden sollen. Dann fordert man einige naheliegende Eigenschaften, etwa, daß je zwei Punkte auf genau einer Geraden liegen. Auf diese Weise wird Euklids Geometrie mit Hilfe der mathematischen Sprache des 19. Jahrhunderts präzisiert und alle elementaren Eigenschaften der ebenen Euklidischen Geometrie lassen sich mit Euklids Beweisen

zeigen. Zudem entstehen auch ganz andere Geometrien, die der Entwicklung der Mathematik wesentliche Impulse gegeben haben. Unser Standpunkt wird ein ganz anderer sein.

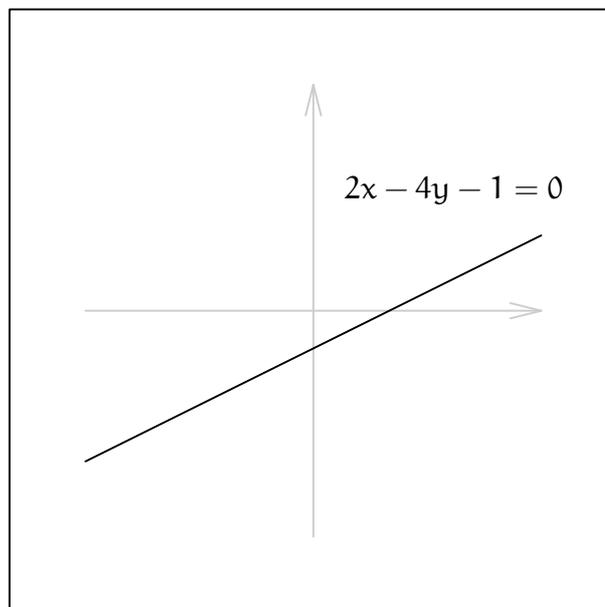
In seiner Schrift *Discours de la Méthode* aus dem Jahr 1637 führte René Descartes die Idee ein, Punkte in der Ebene durch die Angabe von zwei Koordinaten zu beschreiben. Damit machte er es möglich, in der Geometrie die Methoden der Algebra zur Beschreibung und Untersuchung von geometrischen Objekten einzusetzen, die *Algebraische Geometrie* war geboren. Auch der letzte der oben angeführten Defini-
onsversuche des Begriffs Gerade macht sich diesen Umstand zunutze. Etwas präziser gefaßt lautet er:

Eine Gerade ist eine Teilmenge der reellen Zahlenebene \mathbb{R}^2 , deren Punkte genau die Lösungsmenge einer Gleichung der Form

$$a \cdot x + b \cdot y + c = 0 \quad (1)$$

für geeignete reelle Zahlen $a, b, c \in \mathbb{R}$ mit $(a, b) \neq (0, 0)$ bilden.

Diese etwas allgemeinere Form der Gleichung schließt Geraden ein, die parallel zur y -Achse sind. Die Gerade legt dabei die Gleichung nur bis auf ein skalares Vielfaches fest.



Geraden, die wir auf diesem Weg einführen, erfüllen auch die in der axiomatischen Geometrie geforderte Eigenschaft, daß durch je zwei Punkte genau eine Gerade geht. Geben wir uns zwei Punkte $P = (p_1, p_2)$ und $Q = (q_1, q_2)$ in der reellen Zahlenebene vor, dann suchen wir reelle Zahlen $a, b, c \in \mathbb{R}$ derart, daß die Gleichungen

$$a \cdot p_1 + b \cdot p_2 + c = 0$$

und

$$\mathbf{a} \cdot \mathbf{q}_1 + \mathbf{b} \cdot \mathbf{q}_2 + c = 0$$

erfüllt sind. Der Umstand, daß die Punkte verschieden sind, sorgt dafür, daß die Koeffizientenmatrix des Gleichungssystems

$$\begin{pmatrix} p_1 & p_2 & 1 \\ q_1 & q_2 & 1 \end{pmatrix}$$

den Rang zwei hat. Man findet also einen eindimensionalen Lösungsraum, der eine Lösung $(\mathbf{a}, \mathbf{b}, c)$ mit $(\mathbf{a}, \mathbf{b}) \neq (0, 0)$ enthält.

Ausgehend von zwei Punkten $P = (p_1, p_2)$ und $Q = (q_1, q_2)$ kann man sich die Algebra und Koordinaten aber auch auf andere Weise nutzbar machen, um eine Gerade zu beschreiben. Dazu fassen wir die Punkte der reellen Zahlenebene als Vektoren auf und erlauben es, sie zu addieren, zu subtrahieren oder mit Skalaren zu multiplizieren. Die Differenz $P - Q = (p_1 - q_1, p_2 - q_2)$ liefert uns einen Vektor, der in Richtung der Geraden zeigt, und wir können den Begriff der Geraden dann auch einführen als:

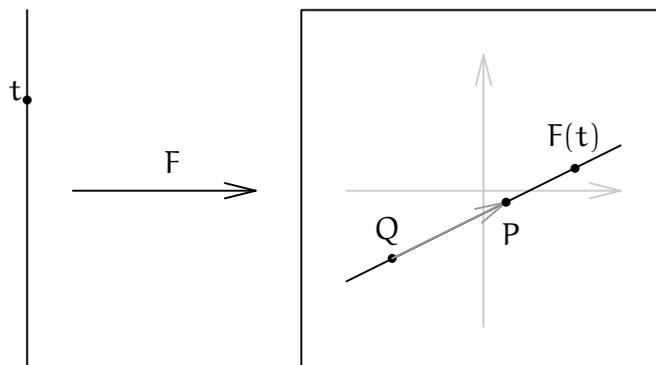
Eine Gerade ist eine Teilmenge der reellen Zahlenebene \mathbb{R}^2 der Form

$$\{Q + t \cdot (P - Q) \mid t \in \mathbb{R}\}, \quad (2)$$

wobei P und Q zwei verschiedene Punkte der reellen Zahlenebene sind.

Unser Ziel ist es, geometrische Objekte, die mit Hilfe algebraischer Mittel beschrieben wurden, zu *visualisieren*. In dieser Hinsicht sind die beiden Beschreibungen einer Geraden in (1) und (2) von fundamental unterschiedlicher Qualität. (2) ist die bei weitem geeignetere Darstellung, da man durch schlichtes Einsetzen von Werten für den Parameter t eine beliebige Anzahl von Punkten auf der Geraden bestimmen kann. Wir sprechen deshalb von einer *Parametrisierung* der Geraden. Etwas mathematischer ausgedrückt, haben wir die Gerade als Bild folgender Abbildung dargestellt:

$$F : \mathbb{R} \longrightarrow \mathbb{R}^2 : t \mapsto Q + t \cdot (P - Q).$$



Da von uns nicht mehr verlangt wird, als Werte in eine Gleichung einzusetzen, um Punkte zu bestimmen, sprechen wir bei der Parametrisierung auch von einer *expliziten Darstellung*. (1) stellt weit höhere Anforderungen, auch wenn dies bei einer Geraden auf den ersten Blick noch nicht offensichtlich ist. Um Punkte (x, y) auf der Geraden zu finden, müssen wir eine Gleichung lösen, sprich versuchen, eine der Veränderlichen in Abhängigkeit der anderen darzustellen. Das ist an sich schon ein größerer Aufwand. Aber um dem Leser gleich jede Illusion zu nehmen, es ist im allgemeinen gar nicht möglich, oder möchten Sie die Gleichung

$$(x^2 + y^2)^2 + 3x^2y - y^3 = 0 \quad (3)$$

nach einer der beiden Variablen auflösen müssen? Wir sprechen im Fall einer Darstellung durch eine oder mehrere *Gleichungen* wie im Fall (1) von einer *impliziten Darstellung*.

Die Gleichung (3) liefert ein dreiblättriges Kleeblatt und die Kurve besitzt eine recht

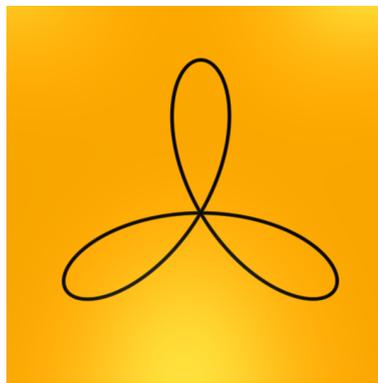


ABBILDUNG 1. Kleeblatt $(x^2 + y^2)^2 + 3x^2y - y^3 = 0$

einfache Parametrisierung:

$$t \mapsto \left(\frac{t^3 - 3t}{(1 + t^2)^2}, \frac{t^4 - 3t^2}{(1 + t^2)^2} \right).$$

Wir werden etwas später sehen, wie man die Parametrisierung in diesem Fall aus der Gleichung gewinnen kann bzw. umgekehrt die Gleichung aus der Parametrisierung. Das Bild des Kleeblattes ist aus der impliziten Gleichung erstellt worden mit Hilfe des Raytracers **Surf** [EHO⁺08]. Schauen wir uns die etwas kompliziertere Gleichung

$$(x^4 + y^4)^2 - x^3y^3 \cdot (x + y) = 0$$

an, so versagt der Raytracer jedoch seinen Dienst und liefert das unkorrekte Bild in Abbildung 2, während die Parametrisierung

$$t \mapsto \left(\frac{t^4 + t^3}{(1 + t^4)^2}, \frac{t^5 + t^3}{(1 + t^4)^2} \right)$$

mit Hilfe von **Maple** das weit bessere Ergebnis bringt (siehe Abbildung 3). Die Probleme, in die der Raytracer hier läuft, haben mit dem Begriff der *Singularität* zu tun, den wir uns in Kapitel 5 näher anschauen werden.

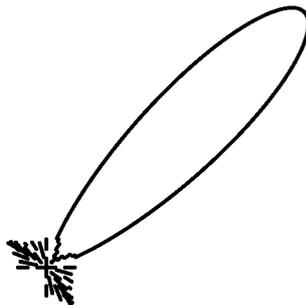


ABBILDUNG 2. Implizit: $(x^4 + y^4)^2 - x^3y^3 \cdot (x + y) = 0$

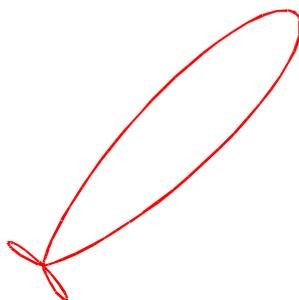


ABBILDUNG 3. Parametrisiert: $(x^4 + y^4)^2 - x^3y^3 \cdot (x + y) = 0$

Da die implizite Darstellung für die Visualisierung die herausforderndere ist und da Parametrisierungen ohnehin in den interessanten Fällen nicht existieren, werden wir uns im Folgenden auf implizite Darstellungen konzentrieren.

Nach diesen einführenden Bemerkungen können wir beantworten, womit sich die algebraische Geometrie beschäftigt:

In der algebraischen Geometrie werden die Lösungsmengen polynomialer Gleichungssysteme sowie die Bilder rationaler Abbildungen untersucht.

Polynomial bedeutet in diesem Zusammenhang, daß die Terme der Gleichungen Polynome in den Veränderlichen sein müssen, und rational, daß die Komponentenfunktionen der Parametrisierung Brüche von Polynomen sind. Es sind keine analytischen Ausdrücke wie etwa $\cos(x)$ oder e^x zugelassen.

Da es unser Ziel ist, die geometrischen Objekte, die entstehen, visualisieren zu können, werden wir uns in unseren Beispielen darauf beschränken, Polynome in zwei

oder in drei Veränderlichen zu betrachten, so daß die Lösungsmengen von Gleichungen oder Ausschnitte selbiger entweder in der Ebene \mathbb{R}^2 oder im Anschauungsraum \mathbb{R}^3 dargestellt werden können. Die Terminologie, die wir benötigen, sowie die Ergebnisse der algebraischen Geometrie, die wir besprechen wollen, werden wir z.T. aber in größerer Allgemeinheit formulieren, um Wiederholungen zu vermeiden.

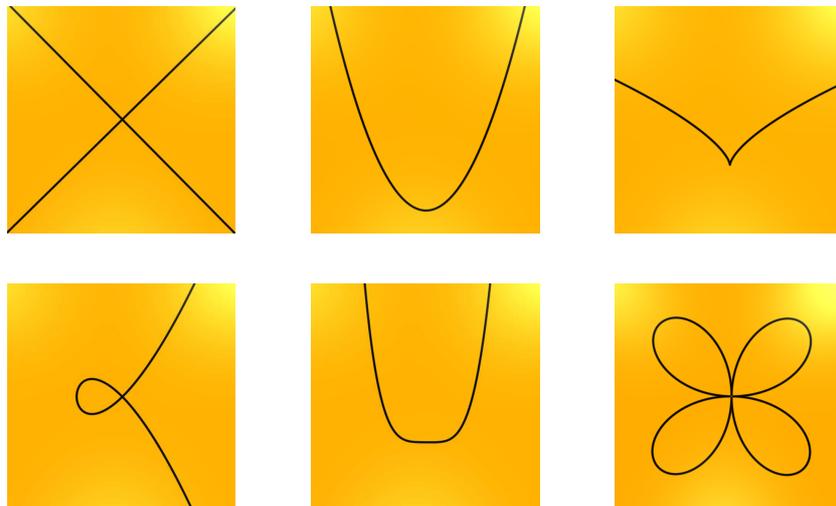
Wenden wir uns nun ersten Beispielen zu. Wir empfehlen dem Leser dabei, zunächst ohne Zuhilfenahme von Rechnern zu entscheiden, wie die Lösungsmenge der gegebenen Gleichung oder das Bild der gegebenen Parametrisierung aussieht.

Beispiel 1.1 (Kurven in der reellen Zahlenebene)

Wie sehen die Lösungsmengen folgender Gleichungen im \mathbb{R}^2 aus?

- $y - x^2 = 0$.
- $y - x^4 + 1 = 0$.
- $y^2 - x^2 = 0$.
- $x^2 - y^3 = 0$.
- $y^2 - x^2 - x^3 = 0$.
- $(x^2 + y^2)^3 - 4x^2y^2 = 0$.

Welches Bild gehört zu welcher Gleichung?

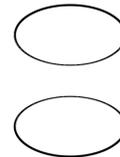
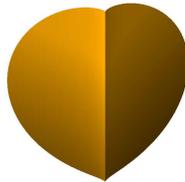
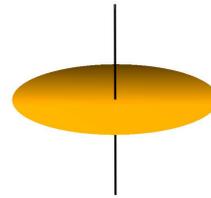
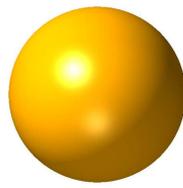


Beispiel 1.2 (Flächen und Kurven im Anschauungsraum)

Wie sehen die Lösungsmengen folgender Gleichungen im \mathbb{R}^3 aus?

- $x^2 - y^3 = 0$.
- $z - x^2 - y^2 = 0$.
- $z^2 - x^2 - y^2 = 0$.
- $z^2 - x^2 - y^2 = 0$ und $z^2 - 1 = 0$.
- $xz = 0$ und $yz = 0$.
- $x^2 + y^2 + z^2 - 1 = 0$.

Welches Bild gehört zu welchem Gleichungssystem?

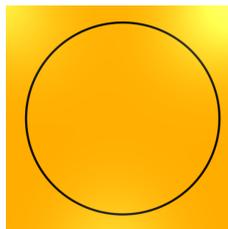


Beispiel 1.3 (Parametrisierungen von Kurven und Flächen)

Wie sehen die Bilder folgender Parametrisierungen aus?

- $t \mapsto (t^3, t^2)$.
- $t \mapsto (t, t^2)$.
- $t \mapsto (t^2 - 1, t^3 - t)$.
- $t \mapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1} \right)$.
- $(s, t) \mapsto (s, t, s^2 + t^2)$.
- $(s, t) \mapsto \left(\frac{t^2-1}{t^2+1} \cdot \frac{s^2-1}{s^2+1}, \frac{t^2-1}{t^2+1} \cdot \frac{2s}{s^2+1}, \frac{2t}{t^2+1} \right)$.

Bis auf den Kreis



finden sich alle Bilder bereits oben!

B) Körper und Polynome

Nachdem wir erste Beispiele von Kurven und Flächen, d.h. Beispiele von sogenannten *algebraischen Varietäten*, kennen gelernt haben, wollen wir die grundlegenden Begriffe der algebraischen Geometrie etwas exakter einführen. Wie bereits angedeutet erlauben wir dabei mehr als drei Dimensionen. Dafür gibt es gute Gründe. Wie wir in Kapitel 7 sehen werden, tauchen polynomiale Gleichungssysteme in vielen Anwendungen auf, und die Zahl der Veränderlichen kann dabei leicht hundert und mehr betragen.

In unseren Beispielen oben sind wir immer davon ausgegangen, daß wir Lösungen in den reellen Zahlen suchen. Von dieser Sichtweise wollen wir uns für die Einführung der Theorie und müssen wir uns für einige Ergebnisse verabschieden. Selbst für die Anwendungen ist hier eine allgemeinere Sicht unabdingbar, wie wir später sehen werden. Wir wollen die reellen Zahlen durch einen beliebigen *Körper* ersetzen.

Arbeitsdefinition 1.4

Ein *Körper* ist eine Menge K zusammen mit zwei Operationen “+” und “·”, so daß die üblichen Rechengesetze gelten, die wir für rationale Zahlen kennen.

Beispiel 1.5

a. Die Menge

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$$

der rationalen Zahlen ist ein Körper.

b. Die Menge \mathbb{R} der reellen Zahlen ist ein Körper.

c. Die Menge

$$\mathbb{C} = \{a + i \cdot b \mid a, b \in \mathbb{R}\}$$

der komplexen Zahlen ist ein Körper, wobei $i^2 = -1$ gilt.

d. Die Menge $\mathbb{F}_2 = \{0, 1\}$ wird ein Körper, wenn wir die Addition und Multiplikation durch folgende Tabellen definieren:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Bei der Multiplikation gibt es keinerlei Überraschungen, bei der Addition ist nur die Regel $1 + 1 = 0$ gewöhnungsbedürftig. \mathbb{F}_2 ist ein Beispiel für einen endlichen Körper, und wenn man die Zahlen 0 und 1 mit den Zuständen *inaktiv* bzw. *aktiv* für Bits interpretiert, dann liegt es nahe, daß dieser Körper für die Beschreibung von Vorgängen der Informatik und Elektrotechnik durchaus sehr interessant ist.

Für unsere Betrachtungen innerhalb der algebraischen Geometrie gilt für die Verwendung der Körper die folgende *Philosophie*:

- Für Rechnungen verwenden wir die rationalen Zahlen \mathbb{Q} .
- Alle Graphiken zeichnen wir über den reellen Zahlen \mathbb{R} .
- Die Theorie funktioniert am Besten über den komplexen Zahlen \mathbb{C} .

Wir wollen nun definieren, was wir unter einem Polynom in n Veränderlichen verstehen. Dazu führen wir zunächst folgende Notation ein.

Notation 1.6

Für einen Vektor $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ setzen wir

$$|\alpha| = \alpha_1 + \dots + \alpha_n,$$

und für $\underline{x} = (x_1, \dots, x_n)$ definieren wir

$$\underline{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Wir nennen einen Ausdruck der Form \underline{x}^α ein *Monom*, und die Menge der Monome in den Veränderlichen x_1, \dots, x_n bezeichnen wir mit $\text{Mon}(\underline{x})$. Auf dieser Menge können wir eine *Multiplikation* einführen durch

$$\underline{x}^\alpha \cdot \underline{x}^\beta = \underline{x}^{\alpha+\beta}$$

wobei

$$\alpha + \beta = (\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n).$$

Definition 1.7

Ein *Polynom* in den Veränderlichen x_1, \dots, x_n über einem Körper K ist ein Ausdruck der Form

$$\sum_{\substack{|\alpha|=0, \dots, d \\ \alpha \in \mathbb{N}^n}} \mathbf{a}_\alpha \cdot \underline{x}^\alpha,$$

wobei $d \in \mathbb{N}$ eine natürliche Zahl ist und $\mathbf{a}_\alpha \in K$. Wir nennen die \mathbf{a}_α die *Koeffizienten* des Polynoms und

$$\deg \left(\sum_{\substack{|\alpha|=0, \dots, d \\ \alpha \in \mathbb{N}^n}} \mathbf{a}_\alpha \cdot \underline{x}^\alpha \right) = \sup\{|\alpha| \mid \mathbf{a}_\alpha \neq 0\}$$

seinen *Grad*. Die Menge aller Polynome über K bezeichnen wir mit

$$K[x_1, \dots, x_n] = \left\{ \sum_{\substack{|\alpha|=0, \dots, d \\ \alpha \in \mathbb{N}^n}} \mathbf{a}_\alpha \cdot \underline{x}^\alpha \mid d \in \mathbb{N}, \mathbf{a}_\alpha \in K \right\}$$

und nennen sie den *Polynomring* über K in den Veränderlichen x_1, \dots, x_n .

Bemerkung 1.8

Wir können auf dem Polynomring eine Addition definieren, indem wir einfach die Koeffizienten der Polynome addieren, und wir können die Multiplikation auf $\text{Mon}(\underline{x})$ unter Verwendung des Distributivgesetzes auf den Polynomring fortsetzen. Wenn wir dies tun, so gelten die üblichen Rechengesetze, die wir von den ganzen Zahlen her kennen. Der Polynomring ist ein *kommutativer Ring mit Eins*.

Im Fall $n = 2$ bezeichnen wir die Veränderlichen meist mit x und y statt x_1 und x_2 , und im Fall $n = 3$ verwenden wir meist x , y und z entsprechend.

Beispiel 1.9

Für die Polynome $f = xy + 3x \in \mathbb{Q}[x, y]$ und $g = 2y^3 + x \in \mathbb{Q}[x, y]$ gilt

$$f + g = 2y^3 + xy + 4x$$

und

$$\begin{aligned} f \cdot g &= (xy + 3x) \cdot (2y^3 + x) \\ &= xy \cdot 2y^3 + xy \cdot x + 3x \cdot 2y^3 + 3x \cdot x = 2xy^4 + x^2y + 6xy^3 + 3x^2. \end{aligned}$$

C) Der affine Raum und affine Varietäten

Nach diesen Vorbereitungen sind wir in der Lage, Kurven, Flächen und allgemein algebraische Varietäten zu definieren.

Definition 1.10

Ist K ein Körper, so nennen wir die Menge

$$\mathbb{A}_K^n = K^n = \{\underline{a} = (a_1, \dots, a_n) \mid a_i \in K\}$$

den *affinen Raum* der Dimension n .

Für Polynome $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ bezeichnen wir mit

$$V(f_1, \dots, f_k) = \{\underline{a} \in \mathbb{A}_K^n \mid f_1(\underline{a}) = \dots = f_k(\underline{a}) = 0\}$$

die Lösungsmenge des Gleichungssystems:

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ f_2(x_1, \dots, x_n) &= 0 \\ &\vdots \\ f_k(x_1, \dots, x_n) &= 0 \end{aligned}$$

Eine Teilmenge $V \subseteq \mathbb{A}_K^n$ heißt eine *affine algebraische Varietät*, wenn es Polynome $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ gibt, so daß

$$V = V(f_1, \dots, f_k).$$

Ist $f \in K[x_1, \dots, x_n] \setminus K$ ein nicht-konstantes Polynom, so nennen wir $V(f)$ die durch f definierte affine *Hyperfläche*. Ist $n = 2$, so nennen wir $V(f)$ eine affine *ebene Kurve*, und ist $n = 3$, so heißt $V(f)$ entsprechend eine affine *Fläche* im Raum.

Beispiel 1.11

Wir haben in Beispiel 1.1 Beispiele affiner ebener Kurven gesehen, und die ersten drei Beispiele in Beispiel 1.2 sind Flächen im Raum. Das fünfte Beispiel in Beispiel 1.2

$$V(xz, yz) = V(xz) \cap V(yz) = V(x, y) \cup V(z)$$

ist die Vereinigung der z -Achse mit der xy -Ebene.

Bemerkung 1.12

Offenbar ist $V(0) = \mathbb{A}_K^n$ der ganze affine Raum und für ein konstantes Polynom $0 \neq \mathbf{a} \in K$, das nicht das Nullpolynom ist, ist $V(\mathbf{a}) = \emptyset$ die leere Menge. Diese beiden affinen Varietäten nennt man die *trivialen* affinen algebraischen Varietäten.

Gibt man sich mehrere nicht-konstante Polynome $f_1, \dots, f_k \in K[x_1, \dots, x_n] \setminus K$ vor, so ist

$$V(f_1, \dots, f_k) = \bigcap_{i=1}^k V(f_i)$$

der Durchschnitt der von den f_i definierten Hyperflächen. Insbesondere ist jede nicht triviale affine algebraische Varietät Durchschnitt von endlich vielen Hyperflächen.

Sind $f, g \in K[x_1, \dots, x_n]$ zwei Polynome, so gilt

$$V(f \cdot g) = V(f) \cup V(g),$$

da $(f \cdot g)(\underline{\mathbf{a}}) = f(\underline{\mathbf{a}}) \cdot g(\underline{\mathbf{a}})$ genau dann null wird, wenn $f(\underline{\mathbf{a}}) = 0$ oder $g(\underline{\mathbf{a}}) = 0$ gilt.

D) Erste Schritte in Singular und Visualisierung mit Surf

Um eine algebraische Kurve zu visualisieren, ist der Raytracer **Surf** [EHO⁺08] ein geeignetes Mittel. Wir werden dieses Programm von SINGULAR aus starten, da wir im weiteren Verlauf ohnehin die Syntax von SINGULAR in ihren Grundzügen lernen müssen. SINGULAR [GPS05] ist ein Computeralgebrasystem, das speziell für Rechnungen in Polynomringen im Rahmen der algebraischen Geometrie und der Singularitätentheorie entwickelt worden ist. SINGULAR ist eine freie Software, die man kostenlos unter dem folgenden Link erhält:

<http://www.singular.uni-kl.de>

Wenn man SINGULAR gestartet hat, erhält man je nach Programmversion folgende Information:

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-1-0
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Aug 2008
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
>
```

Das Zeichen `>` ist die Eingabeaufforderung, kurz Prompt genannt. Wenn die letzte Zeile des Programms dieses Zeichen zeigt, können Befehle eingegeben werden, ansonsten ist das Programm sehr wahrscheinlich noch am Rechnen.

Wenn wir in SINGULAR Polynome verwenden wollen, dann müssen wir SINGULAR zunächst mitteilen, welchen Grundkörper und welche Veränderlichen wir verwenden wollen. Dies tun wir, indem wir etwa mit folgendem Befehl den Polynomring $\mathbb{Q}[x, y]$ definieren:

```
> ring r=0,(x,y),dp;
```

Die Bedeutung des Befehls ist wie folgt: `ring` bedeutet, daß wir eine Variable vom Typ `ring` definieren wollen; sie erhält den Namen `r`; die `Null` bedeutet, daß die Koeffizienten aus dem Körper der rationalen Zahlen \mathbb{Q} stammen;¹ `(x,y)` legt fest, daß als Variablen `x` und `y` erlaubt sind; der Zusatz `dp` legt fest, wie die Polynome intern repräsentiert werden, ist aber für unsere Belange nicht wesentlich.

Wichtiger Hinweis: in SINGULAR schließt jeder Befehl mit einem Semikolon ab!

Wenn wir SINGULAR unseren Grundring mitgeteilt haben, dann können wir ein Polynom definieren. Das Polynom $f = y^2 - 5 \cdot x^2 - x^3$ teilen wir SINGULAR durch folgenden Befehl mit:

```
> poly f=y^2-5*x^2-x^3;
```

Analog zur Definition eines Ringes führen wir durch diesen Befehl eine Variable `f` ein, die vom Typ `poly`, also ein Polynom, ist, und weisen ihr den Wert $y^2 - x^2 - x^3$ zu.

Wollen wir die zugehörige Kurve mit `Surf` zeichnen, so müssen wir zunächst eine Bibliothek in SINGULAR laden, die das Aufrufen von `Surf` ermöglicht:

```
> LIB "surf.lib";
```

Dann können wir die Kurve zeichnen lassen mit dem Befehl `plot`:

```
> plot(f);
```

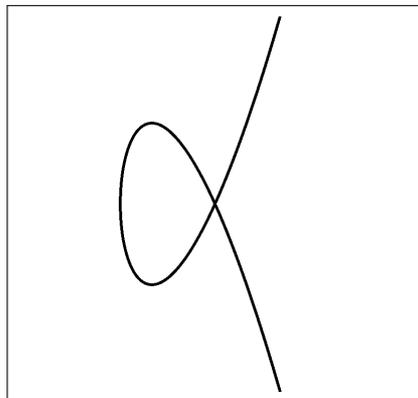


ABBILDUNG 4. Ein Newtonscher Knoten $y^2 - 5x^2 - x^3 = 0$

In der Gesamtheit sieht unsere SINGULAR Sitzung wie folgt aus:

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-1-0
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Aug 2008
FB Mathematik der Universitaet, D-67653 Kaiserslautern \

```

¹Der Körper der rationalen Zahlen \mathbb{Q} ist der Primkörper der Charakteristik null. Ersetzt man die Zahl null durch eine Primzahl p , so legt man statt dessen den Primkörper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Charakteristik p als Grundkörper fest.

```

> ring r=0,(x,y),dp;
> poly f=y2-x2-x3;
> LIB "surf.lib";
// ** loaded /usr/local/Singular/3-1-0/LIB/surf.lib (1.28,2007/07/13)
> plot(f);
Press q to exit from 'surf'

```

Die Kurve erscheint in einem neuen Fenster. SINGULAR kann erst dann weiterverwendet werden, wenn Surf geschlossen wurde. Dazu drückt man die Taste q im Surf Fenster. Surf wird geschlossen und in SINGULAR erhalten wir wieder einen Prompt. Wir könnten nun auch andere Polynome definieren und zeichnen lassen, ggf. auch einen neuen Ring definieren mit anderen Veränderlichen. Man beachte dabei, daß nur Polynomringe mit zwei oder drei Veränderlichen zugelassen sind. Andernfalls ist eine Visualisierung aus naheliegenden Gründen nicht möglich.

*Man beachte bitte auch, daß man stets nur einen Ausschnitt der affinen algebraischen Kurve oder Fläche sieht, dessen Mittelpunkt standardmäßig der Ursprung der affinen Ebene $\mathbb{A}_{\mathbb{R}}^2$ oder des affinen Anschauungsraumes $\mathbb{A}_{\mathbb{R}}^3$ ist. Um zu erfahren, wie man die Größe des Ausschnitts oder den Mittelpunkt verändern kann, sollte man das Handbuch von **Surf** konsultieren (siehe [EHO⁺08]).*

E) Parametrisierungen und Elimination

Als nächstes wollen wir den Begriff der Parametrisierung einführen. Die Parameter werden wir in der allgemeinen Form mit t_i bezeichnen. Wenn nur ein Parameter vorkommt, nennen wir ihn gemeinhin t , bei zweien nennen wir sie s und t . Als Komponentenfunktionen einer Parametrisierung wollen wir Quotienten $\frac{f}{g}$ von Polynomen zulassen. Dann dürfen wir natürlich nur noch Werte einsetzen, die nicht in $V(g)$ liegen, d.h. Werte \underline{t} , für die $g(\underline{t})$ nicht null ist.

Definition 1.13

Sind $f_1, \dots, f_n, g_1, \dots, g_n \in K[t_1, \dots, t_m]$ Polynome. Die Abbildung

$$F: \mathbb{A}_K^m \setminus V(g_1 \cdots g_n) \longrightarrow \mathbb{A}_K^n: \underline{t} = (t_1, \dots, t_m) \mapsto \left(\frac{f_1}{g_1}(\underline{t}), \dots, \frac{f_n}{g_n}(\underline{t}) \right)$$

wird eine rationale *Parametrisierung* genannt, wenn $V(g_1 \cdots g_n) \neq \mathbb{A}_K^m$.

Die Menge

$$\text{Graph}(F) = \{ (\underline{t}, F(\underline{t})) \in \mathbb{A}_K^{m+n} \mid \underline{t} \in \mathbb{A}_K^m \setminus V \}$$

nennen wir den *Graphen* der Parametrisierung.

Die Bedingung $V(\mathfrak{g}_1, \dots, \mathfrak{g}_n) \neq \mathbb{A}_K^m$ ist recht naheliegend, da der Definitionsbereich von F sonst leer wäre.

Bemerkung 1.14

Ist $F : \mathbb{A}_K^m \setminus V \rightarrow \mathbb{A}_K^n$ eine Parametrisierung und ist

$$\pi : \mathbb{A}_K^{m+n} \rightarrow \mathbb{A}_K^n : (\mathfrak{a}_1, \dots, \mathfrak{a}_m, \mathfrak{b}_1, \dots, \mathfrak{b}_n) \mapsto (\mathfrak{b}_1, \dots, \mathfrak{b}_n)$$

die Projektion auf die letzten n Komponenten, so stimmen das Bild $\text{Im}(F)$ von F und die Projektion des Graphen von F überein, d.h.

$$\text{Im}(F) = \{F(\underline{t}) \mid \underline{t} \in \mathbb{A}_K^m \setminus V\} = \pi(\text{Graph}(F)).$$

Beispiel 1.15

Die Abbildung

$$F : \mathbb{A}_R^1 \rightarrow \mathbb{A}_R^2 : t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

ist eine Parametrisierung, und der Graph von F ist die Menge

$$\text{Graph}(F) = \left\{ (t, F(t)) \mid t \in \mathbb{R} \right\} = \left\{ \left(t, \frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \mid t \in \mathbb{R} \right\}.$$

Es handelt sich dabei um eine Kurve im Raum, die auf der Oberfläche eines Zylinders liegt. Die Koordinaten des Raumes sind t , x und y , und die Achse des Zylinders ist die t -Achse. Projiziert man die Kurve in die xy -Ebene, so erhält man einen Kreis. Dieser ist das Bild der Parametrisierung. Die Parametrisierung, ihr Graph und die Projektion sind dargestellt in Abbildung 5.

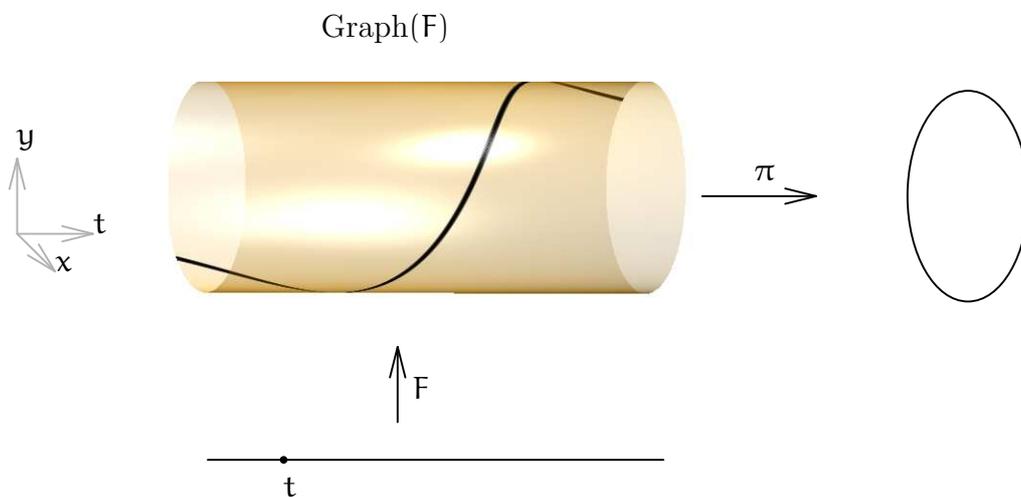


ABBILDUNG 5. Die schwarze Kurve auf dem Zylinder ist der Graph(F).

Dieser Zusammenhang zwischen dem Graphen einer Parametrisierung und ihrem Bild kommt uns zugute, da der Satz 1.18 uns sagt, wie wir das Bild einer Varietät unter einer Projektion berechnen können. Allerdings benötigen wir begrifflich ein wenig Vorbereitung.

Definition 1.16

Sind $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ Polynome, so nennen wir die Menge

$$\langle f_1, \dots, f_k \rangle = \{g_1 \cdot f_1 + \dots + g_k \cdot f_k \mid g_1, \dots, g_k \in K[x_1, \dots, x_n]\}$$

der Linearkombinationen von f_1, \dots, f_k das von f_1, \dots, f_k erzeugte *Ideal*.

Bemerkung 1.17

Sind $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ Polynome und ist $I = \langle f_1, \dots, f_k \rangle$ das von den f_i erzeugte Ideal, dann gilt

$$\underline{a} \in V(f_1, \dots, f_k) \iff g(\underline{a}) = 0 \text{ für alle } g \in I.$$

Will man eine affine algebraische Varietät beschreiben, so kann man statt der endlich vielen Gleichungen

$$f_i(x_1, \dots, x_n) = 0, \quad i = 1, \dots, n,$$

auch die unendlich vielen Gleichungen

$$g(x_1, \dots, x_n) = 0, \quad g \in I,$$

betrachten. Auf den ersten Blick scheint man sich das Leben damit schwerer gemacht zu haben. Das Gegenteil ist aber der Fall! Ideale haben gute Eigenschaften und erlauben es uns die Methoden der kommutativen Algebra und der Computeralgebra effizient zum Studium von affinen algebraischen Varietäten einzusetzen.

Im folgenden Satz beachten wir, daß jedes Polynom in den Veränderlichen x_1, \dots, x_n auch als ein Polynom in den Veränderlichen $t_1, \dots, t_m, x_1, \dots, x_n$ aufgefaßt werden kann, bei dem die Veränderlichen t_i nicht auftauchen. Damit ist der Polynomring $K[x_1, \dots, x_n]$ also eine Teilmenge des Polynomrings $K[t_1, \dots, t_m, x_1, \dots, x_n]$.

Satz 1.18

Es seien $h_1, \dots, h_k \in K[t_1, \dots, t_m, x_1, \dots, x_n]$ Polynome, $I = \langle h_1, \dots, h_k \rangle$ sei das von den h_i erzeugte Ideal und $V = V(h_1, \dots, h_k) \subseteq \mathbb{A}_K^{m+n}$ sei die durch die h_i definierte affine algebraische Varietät. Dann gelten die folgenden Aussagen:

- a. Es gibt Polynome $p_1, \dots, p_l \in K[x_1, \dots, x_n]$, so daß der Schnitt

$$I \cap K[x_1, \dots, x_n] = \langle p_1, \dots, p_l \rangle$$

von I mit $K[x_1, \dots, x_n]$ das von den p_i erzeugte Ideal in $K[x_1, \dots, x_n]$ ist.

- b. Ist $\pi : \mathbb{A}_K^{m+n} \rightarrow \mathbb{A}_K^n$ die Projektion auf die letzten n Komponenten, so liegt das Bild $\pi(V)$ von V unter der Projektion π dicht in der von den p_i gegebenen affinen algebraischen Varietät $V(p_1, \dots, p_l)$.

Bemerkung 1.19

Um den Begriff *dicht* mathematisch sauber einzuführen, müßten wir an dieser Stelle von der Zariski-Topologie affiner algebraischer Varietäten sprechen. Darauf möchten

wir verzichten. Uns reicht, daß die Aussage “ $\pi(V)$ liegt dicht in $V(p_1, \dots, p_l)$ ” bedeutet, daß auf alle Fälle

$$\pi(V) \subseteq V(p_1, \dots, p_l)$$

gilt und daß die beiden Mengen *im wesentlichen* auch gleich sind. D.h., das was zur Gleichheit fehlt ist vernachlässigbar klein (siehe Beispiel 1.23). Wir können also sagen:

$$“\pi(V) = V(p_1, \dots, p_l)”.$$

Bemerkung 1.20

Ist

$$F : \mathbb{A}_K^m \setminus V(g_1, \dots, g_n) \longrightarrow \mathbb{A}_K^n : \underline{t} = (t_1, \dots, t_m) \mapsto \left(\frac{f_1}{g_1}(\underline{t}), \dots, \frac{f_n}{g_n}(\underline{t}) \right)$$

eine Parametrisierung wie in Definition 1.13, so genügen die letzten n Koordinaten eines Punktes $(\underline{a}, F(\underline{a})) \in \text{Graph}(F)$ im Graphen von F den Bedingungen

$$x_i = \frac{f_i(\underline{a})}{g_i(\underline{a})}, \quad i = 1, \dots, n,$$

und damit den Bedingungen

$$x_i \cdot g_i(\underline{a}) = f_i(\underline{a}), \quad i = 1, \dots, n.$$

Ähnlich wie beim Bild einer Projektion ist der Graph der Parametrisierung F dann dicht in der affinen algebraischen Varietät $V(x_1 \cdot g_1 - f_1, \dots, x_n \cdot g_n - f_n) \subseteq \mathbb{A}_K^{m+n}$, d.h. im wesentlichen gilt

$$“\text{Graph}(F) = V(x_1 \cdot g_1 - f_1, \dots, x_n \cdot g_n - f_n)”.$$

Verknüpfen wir dieses Ergebnis mit den Ergebnissen von Bemerkung 1.14 und von Satz 1.18, so erhalten wir im wesentlichen folgende Gleichheit:

$$“\text{Im}(F) = \pi(\text{Graph}(F)) = \pi(V(x_1 \cdot g_1 - f_1, \dots, x_n \cdot g_n - f_n)) = V(p_1, \dots, p_l)”,$$

wenn die Polynome p_1, \dots, p_l Erzeuger des Ideals

$$\langle x_1 \cdot g_1 - f_1, \dots, x_n \cdot g_n - f_n \rangle \cap K[x_1, \dots, x_n]$$

sind. Solche Polynome können wir aber mit Hilfe von *Variablenelimination* und Computeralgebra ausrechnen.

Mit Hilfe von Elimination können wir für jede Parametrisierung Gleichungen ihres Bildes ausrechnen. Wir können also jede explizite Darstellung in eine implizite Darstellung überführen.

Wir wollen dies nun an einem Beispiel illustrieren. Dabei verwenden wir das Computeralgebrasystem SINGULAR.

Beispiel 1.21

Wir wollen die Parametrisierung

$$F: \mathbb{A}_{\mathbb{R}}^2 \longrightarrow \mathbb{A}_{\mathbb{R}}^3: (s, t) \mapsto \left(\left(3 + \frac{s^2 - 1}{s^2 + 1} \right) \cdot \frac{t^2 - 1}{t^2 + 1}, \left(3 + \frac{s^2 - 1}{s^2 + 1} \right) \cdot \frac{2 \cdot t}{t^2 + 1}, \frac{2 \cdot s}{s^2 + 1} \right)$$

betrachten. Mit den Notationen von Bemerkung 1.20 gilt dann:

$$f_1 = (3 \cdot (s^2 + 1) + (s^2 - 1)) \cdot (t^2 - 1)$$

$$g_1 = (s^2 + 1) \cdot (t^2 + 1)$$

$$f_2 = (3 \cdot (s^2 + 1) + (s^2 - 1)) \cdot 2 \cdot t$$

$$g_2 = (s^2 + 1) \cdot (t^2 + 1)$$

$$f_3 = 2 \cdot s$$

$$g_3 = s^2 + 1$$

Wir müssen also das Ideal

$$\begin{aligned} \langle g_1 \cdot x - f_1, g_2 \cdot x - f_2, g_3 \cdot x - f_3 \rangle = \\ \langle (s^2 + 1) \cdot (t^2 + 1) \cdot x - (3 \cdot (s^2 + 1) + (s^2 - 1)) \cdot (t^2 - 1), \\ (s^2 + 1) \cdot (t^2 + 1) \cdot y - (3 \cdot (s^2 + 1) + (s^2 - 1)) \cdot 2 \cdot t, \\ (s^2 + 1) \cdot z - 2 \cdot s \rangle \subseteq \mathbb{R}[s, t, x, y, z] \end{aligned}$$

mit dem Polynomring $\mathbb{R}[x, y, z]$ schneiden. Dies geschieht mittels folgender SINGULAR -Kommandos:

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0,(s,t,x,y,z),dp;
> poly f1=(3*(s^2+1)+(s^2-1))*(t^2-1);
> poly g1=(s^2+1)*(t^2+1);
> poly f2=(3*(s^2+1)+(s^2-1))*2*t;
> poly g2=(s^2+1)*(t^2+1);
> poly f3=2*s;
> poly g3=s^2+1;
> ideal I=g1*x-f1,g2*y-f2,g3*z-f3;
> ideal J=eliminate(I,st);
> J;
J[1]=x4z2+2x2y2z2+y4z2+2x2z4+2y2z4+z6+8x4+16x2y2
+8y4-4x2z2-4y2z2+24z4-160x2-160y2+192z2+512

```

In dieser Sitzung definieren wir zunächst wieder einen Polynomring und teilen SINGULAR dadurch mit, welche Veränderlichen wir verwenden wollen. Dann definieren wir die Polynome f_i und g_i für $i = 1, 2, 3$ sowie das Ideal I . Letzteres ist eine Variable

vom Typ `ideal` und wir weisen Ihr als Wert die Erzeuger des Ideals zu. Dann rufen wir die SINGULAR Prozedur `eliminate` auf. Sie erwartet als erste Eingabe ein Ideal und als zweite Eingabe ein Produkt von Veränderlichen, die eliminiert werden sollen. Dabei bezeichnen wir den Vorgang des Schneidens mit $\mathbb{R}[x, y, z]$ als *Elimination* von s und t . Das Ergebnis ist, wie wir wissen, wieder ein Ideal. Um es weiter verwenden zu können, speichern wir es in einer neuen Variablen mit dem Namen J . Durch das Kommando `J;` können wir uns den Wert der Variablen, das heißt in diesem Fall die Erzeuger des Ideals, anzeigen lassen. Wir erhalten das Polynom

$$p = x^4z^2 + 2 \cdot x^2y^2z^2 + y^4z^2 + 2 \cdot x^2z^4 + 2 \cdot y^2z^4 + z^6 + 8 \cdot x^4 + 16 \cdot x^2y^2 + 8 \cdot y^4 - 4 \cdot x^2z^2 - 4 \cdot y^2z^2 + 24 \cdot z^4 - 160 \cdot x^2 - 160 \cdot y^2 + 192 \cdot z^2 + 512,$$

so daß das Bild unserer Parametrisierung gerade die Fläche $V(g)$ ist. Wir können sie nun von `Surf` zeichnen lassen, indem wir in unserer SINGULAR Sitzung fortfahren:

```
> LIB "surf.lib";
> plot(J[1]);
```

Man kann dem `plot` Befehl auch Parameter angeben, die eine Skalierung und Drehung der Fläche bewirken. Für unser Beispiel sind folgende Parameter gut:

```
> LIB "surf.lib";
> plot(J[1], "scale_x=0.4;scale_y=0.4;scale_z=0.4;rot_x=2;");
```

Durch diese Skalierung und Drehung erhalten wir das Bild in Abbildung 6, das einem Fahrradschlauch ähnelt und in der Mathematik gemeinhin als *Torus* bekannt ist.



ABBILDUNG 6. Der Torus

Wir führen unsere Rechnungen mit SINGULAR wieder über \mathbb{Q} durch, die Theorie sagt uns aber, daß das Ergebnis beim Prozeß der Elimination dann auch über \mathbb{R} korrekt ist.

Da der Torus uns in Form einer Parametrisierung gegeben ist, können wir natürlich auch Visualisierungsprogramme für Parametrisierungen verwenden, um das Bild zu erhalten, etwa das kostenlose Programm `k3dsurf` (siehe Abbildung 7). Man gibt hier

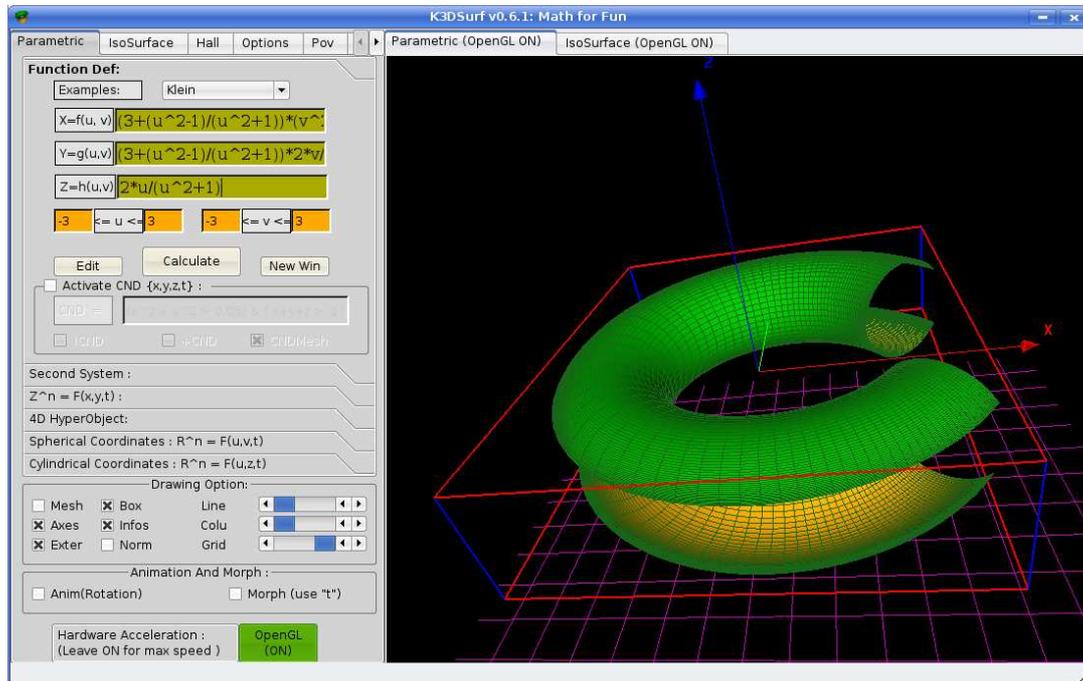


ABBILDUNG 7. k3dsurf

die Parametrisierung mit Parametern u und v ein, spezifiziert den Wertebereich der Parameter und erhält ein Bild. Der Torus ist nicht geschlossen, da wir recht kleine Wertebereiche für die Parameter gewählt haben. Wählt man größere Bereiche, ist das Ergebnis jedoch stark verzerrt. Das dürfte daran liegen, daß das Programm für eine feste Anzahl an Werten von u und v die Bildpunkte berechnet und diese Werte äquidistant auf den gewählten Intervallen verteilt. Anschließend werden die so erhaltenen Punkte verbunden. Das kann in unserem Beispiel nur zu einem miserablen Ergebnis führen, da die Bildpunkte für betragsmäßig große u und v sehr dicht beieinander liegen, während sie im Bereich um null weit auseinander liegen. Wir sehen daran, daß Parametrisierungen nur dann besser geeignet sind zur Visualisierung als implizite Darstellungen, wenn man das Verhalten der Parametrisierung untersucht und sein Vorgehen diesem Verhalten anpaßt!

Wir haben anfangs behauptet, daß nicht jede affine algebraische Varietät parametrisiert werden kann. Den Sachverhalt näher zu untersuchen, führt an dieser Stelle zu weit. Aber merken sollten wir ihn uns schon.

Nicht jede affine algebraische Varietät kann parametrisiert werden!

Beispiel 1.22

Ist $a \in \mathbb{R} \setminus \{0, 1\}$, so besitzt die affine algebraische Kurve

$$V(y^2 - x \cdot (x - 1) \cdot (x - a)) \subset \mathbb{A}_{\mathbb{R}}^2$$

keine rationale Parametrisierung.

Für den Beweis benötigt man die Primfaktorzerlegung im Polynomring $\mathbb{C}[t]$ (vgl. Bemerkung 1.28). Die Details sind ausgeführt in [Rei92, Theorem (2.2)] und die Argumente sind ohne weitere Vorkenntnisse verständlich.

Beispiel 1.23

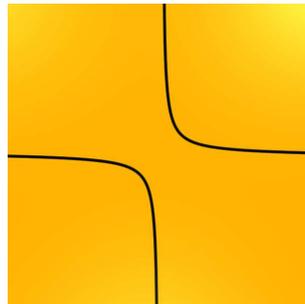
Betrachten wir die affine algebraische Varietät

$$V(t \cdot x - 1) \subseteq \mathbb{A}_{\mathbb{R}}^2$$

und die Projektion

$$\pi: \mathbb{A}_{\mathbb{R}}^2 \longrightarrow \mathbb{A}_{\mathbb{R}}^1: (t, x) \mapsto x$$

auf die zweite Komponente. Die Gleichung $tx - 1 = 0$ beschreibt eine Hyperbel



und ihre Projektion auf die x -Achse ergibt alle Punkte der x -Achse außer dem Nullpunkt, d.h.

$$\pi(V(tx - 1)) = \mathbb{R} \setminus \{0\}.$$

Schneiden wir das Ideal $\langle tx - 1 \rangle$ aber mit dem Ring $\mathbb{R}[x]$, so erhalten wir nur das Nullpolynom und

$$V(0) = \mathbb{R}.$$

Dies ist ein Beispiel dafür, daß die Projektion einer affinen algebraischen Varietät nicht gleich der Varietät sein muß, die durch die Erzeuger des Eliminationsideals definiert wird. Es fehlt allerdings nur ein einziger Punkt, so daß die beiden *im wesentlichen* übereinstimmen.

Allgemein gilt, daß sich das Bild einer affinen algebraischen Varietät unter einer Projektion nur durch eine Teilmenge niedriger Dimension von der affinen algebraischen Varietät unterscheidet, die durch das Eliminationsideal definiert wird.

F) Dimension und der Krullsche Hauptidealsatz

Zum Abschluß dieses Kapitels wollen wir noch einige Begriffe der algebraischen Geometrie thematisieren, die im weiteren Verlauf immer wieder auftauchen.

Bemerkung 1.24 (Dimension)

Wir werden darauf verzichten, den Begriff der *Dimension* exakt zu fassen. Statt dessen appellieren wir an die Intuition des Lesers. Ein Punkt sollte nulldimensional sein, eine Gerade eindimensional, eine Ebene zweidimensional und der affine Raum \mathbb{A}_K^n n -dimensional. Der leeren Menge ordnen wir die Dimension $-\infty$ zu.

Es ist natürlich etwas Vorsicht geboten. Der Raum $\mathbb{A}_{\mathbb{R}}^1 = \mathbb{R}$ ist die reelle Zahlengerade und hat Dimension eins. Entsprechend sollte $\mathbb{A}_{\mathbb{C}}^1 = \mathbb{C}$ als "komplexe Zahlengerade" die Dimension eins haben. Wir sind es aber gewohnt, die komplexen Zahlen als Menge mit der reellen Zahlenebene \mathbb{R}^2 zu identifizieren, die doch zweidimensional ist. Wie paßt das zusammen?

Die Dimension ist ein Begriff, der von dem Grundkörper abhängt, über dem man arbeitet, und wir fordern $\dim_K(\mathbb{A}_K^n) = n$!

Das paßt auch mit unserer Erfahrung im Bereich der linearen Algebra zusammen, wo wir analog $\dim_K(K^n) = n$ haben. Um bei der Analogie zu bleiben, betrachten wir ein homogenes lineares Gleichungssystem

$$\begin{array}{rcl} a_{11} \cdot x_1 + \dots + a_{1n} \cdot x_n & = & 0 \\ & \vdots & \\ a_{m1} \cdot x_1 + \dots + a_{mn} \cdot x_n & = & 0 \end{array}$$

mit m Gleichungen und n Unbekannten. Wir wissen dann, daß die Dimension des Lösungsraumes mit jeder Gleichung um höchstens eins sinkt, sprich daß die Dimension mindestens $n - m$ ist. Eine entsprechende Aussage hätten wir auch gerne in der algebraischen Geometrie. Es wäre schön, wenn $V(f_1, \dots, f_m) \subseteq \mathbb{A}_K^n$ mindestens die Dimension $n - m$ hätte. Das ist zuviel verlangt. Schon bei einem linearen Gleichungssystem geht dies schief, wenn wir auf der rechten Seite Inhomogenitäten ungleich null zulassen. Die Lösungsmenge kann auf einmal leer sein.

Die Situation ist etwas besser, wenn wir uns nur eine Gleichung vorgeben und über dem Körper der komplexen Zahlen arbeiten.

Satz 1.25 (Krullscher Hauptidealsatz)

Ist $f \in \mathbb{C}[x_1, \dots, x_n]$ ein nicht-konstantes Polynom, so hat die Hyperfläche $V(f)$ die Dimension $\dim_{\mathbb{C}}(V(f)) = n - 1$.

Dieser Satz ist eine Verallgemeinerung des Hauptsatzes der Algebra. Starten wir mit einem nicht-konstanten Polynom $f \in \mathbb{C}[x]$ in nur einer Veränderlichen, so sagt der Krullsche Hauptidealsatz lediglich, daß f Nullstellen besitzt.

Satz 1.26 (Hauptsatz der Algebra)

Ist $f \in \mathbb{C}[x]$ ein nicht-konstantes Polynom vom Grad $\deg(f) = d$, so hat f genau d Nullstellen, wenn wir diese mit ihrer Vielfachheit² zählen.

Über den reellen Zahlen ist das leider nicht mehr richtig. Der Grad eines Polynoms in einer Veränderlichen ist dort nur noch eine obere Schranke für die mögliche Anzahl an Nullstellen.

Beispiel 1.27

Betrachten wir das Polynom $f = x^2 + y^2 + 1 = 0$, so gilt

$$\{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\} = \emptyset,$$

während

$$\{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\} = \left\{ \left(\frac{i \cdot (t^2 - 1)}{t^2 + 1}, \frac{2 \cdot i \cdot t}{t^2 + 1} \right) \mid t \in \mathbb{C} \right\}$$

eine Kurve ist und die komplexe Dimension eins besitzt.

Der Hauptsatz der Algebra ist der wesentliche Grund dafür, daß die Theorie der algebraischen Geometrie über \mathbb{C} besser funktioniert als über \mathbb{R} .

G) Irreduzible Komponenten**Bemerkung 1.28** (Irreduzible Komponenten)

Wir nennen ein nicht-konstantes Polynom $f \in \mathbb{K}[x_1, \dots, x_n]$ *irreduzibel* oder auch *prim*, wenn es sich nicht als Produkt von zwei nicht-konstanten Polynomen schreiben läßt. So wie sich jede ganze Zahl als Produkt von Primzahlen schreiben läßt, kann jedes Polynom als Produkt von irreduziblen Polynomen geschrieben werden. Dies ist die Aussage eines *Satzes von Gauß*. Wir erhalten also eine Primfaktorzerlegung für Polynome.

Außerdem nennen wir ein Polynom f *quadratfrei*, wenn es nicht vom Quadrat eines nicht-konstanten Polynoms geteilt wird. In der Primfaktorzerlegung eines quadratfreien Polynoms kommt jeder Primfaktor also nur einmal vor. Quadratfreie Polynome sind deshalb für uns interessant, weil $V(f^2) = V(f)$ gilt. Es reicht also die Hyperflächen aller quadratfreien Polynome zu kennen, um alle Hyperflächen zu kennen.

Betrachten wir eine Hyperfläche $V(f) \subset \mathbb{A}_k^n$, die durch ein nicht-konstantes, quadratfreies Polynom f mit Primfaktorzerlegung $f = p_1 \cdots p_k$ definiert wird

$$V(f) = V(p_1) \cup \dots \cup V(p_k).$$

²Für eine genauere Betrachtung des Hauptsatzes der Algebra siehe Bemerkung 4.2.

Wir nennen die $V(\mathfrak{p}_i)$ die *irreduziblen Komponenten* von $V(f)$. Sie selbst lassen sich nicht mehr als endliche Vereinigung echt kleinerer affiner algebraischer Varietäten schreiben.

Man kann den Begriff entsprechend verallgemeinern, so daß etwa die Vereinigung der z -Achse mit der xy -Ebene

$$V(xz, yz) = V(x, y) \cup V(z) \subset \mathbb{A}_{\mathbb{R}}^3$$

aus Beispiel 1.2 aus den beiden irreduziblen Komponenten $V(x, y)$ und $V(z)$ besteht.

Beispiel 1.29

Ist $f = x^2 - y^2 = (x - y) \cdot (x + y)$, so ist

$$V(f) = V(x - y) \cup V(x + y)$$

die Vereinigung der beiden Winkelhalbierenden. Sie sind die irreduziblen Komponenten von $V(f)$.

Im Gegensatz zur Elimination ist die Frage nach den irreduziblen Komponenten abhängig vom Grundkörper!

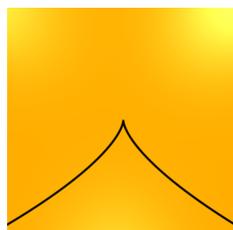
H) Familien von Varietäten

Bemerkung 1.30 (Familien von Varietäten)

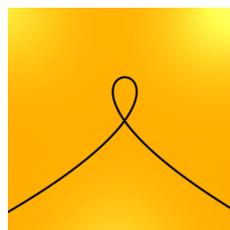
Sehr oft wollen wir in der algebraischen Geometrie die Koeffizienten einer Gleichung variieren und schauen, wie sich das auf die Lösungsmenge auswirkt. Betrachten wir etwa die Polynome

$$f_t = x^2 - y^2 \cdot (t^2 - y) \in \mathbb{R}[x, y]$$

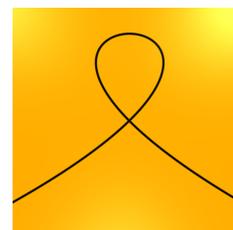
für verschiedene Werte des Parameters $t \in \mathbb{R}$. Für $t = 0$, $t = \frac{1}{2}$ und $t = 1$ erhalten wir die Bilder:



$t = 0$

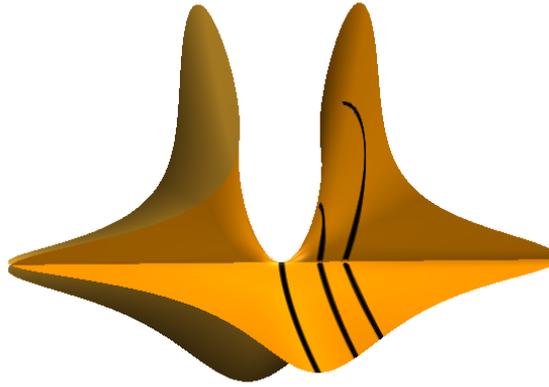


$t = \frac{1}{2}$



$t = 1$

Betrachtet man dies für alle $t \in \mathbb{R}$ zugleich, so erhalten wir schlicht die affine algebraische Varietät $V(x^2 - y^2 \cdot (t^2 - y)) \subset \mathbb{A}_{\mathbb{R}}^3$, indem wir t , x und y als Veränderliche auffassen:



Auf der Fläche sind schwarz die drei Kurven eingezeichnet, die wir erhalten, wenn wir für t die oben betrachteten Werte einsetzen.

Betrachten wir Gleichungen, deren Koeffizienten von Parametern abhängen, sowie die zugehörigen Varietäten, so sprechen wir auch von *Familien* von Varietäten. Die Zahl der Parameter kann dabei recht groß sein, und es ist nicht verlangt, daß wir für verschiedenen Parameter auch verschiedene Gleichungen oder Varietäten erhalten. In obigem Beispiel verwenden wir für die Familie der Polynome die Notation

$$(x^2 - y^2 \cdot (t^2 - y))_{t \in \mathbb{R}}.$$

Ein einfaches, aber zugleich wichtiges Beispiel ist die Familie

$$(ax^2 + bxy + cy^2 + dx + ey + f)_{(a,b,c,d,e,f) \in T}$$

aller Polynome vom Grad zwei, wobei $T = \{(a, b, c, d, e, f) \in \mathbb{R}^6 \mid (a, b, c) \neq (0, 0, 0)\}$. Die zugehörigen affinen algebraischen Varietäten nennt man affine *Kegelschnitte* oder affine *Quadriken*.

I) Visualisierung mit Surfex

Bemerkung 1.31

Das Programm **Surfex** (siehe [HL08]) bietet eine graphische Oberfläche, um Flächen im Raum sowie Kurven auf Flächen im Raum visualisieren zu können. Man kann **Surfex** entweder von **SINGULAR** aus starten oder unabhängig davon als eigenständiges Programm. Will man **Surfex** von **SINGULAR** aus starten, so muß man zunächst die Bibliothek `surfex.lib` laden. Der Befehl zum visualisieren der Fläche, die durch das Polynom definiert wird, lautet dann `plotRot`. Wir führen dies am Beispiel des Polynoms $f = x^2 - y^2 \cdot (t^2 - y)$ vor.

```
SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
```

```

                                0<
    by: G.-M. Greuel, G. Pfister, H. Schoenemann      \   Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0,(t,x,y),dp;
> poly f=x^2-y^2*(t^2-y);
> LIB "surfex.lib";
> plotRot(f);

```

Durch den Aufruf von `plotRot` wird das Programm `Surfex` gestartet, es öffnen sich drei neue Fenster (siehe Abbildung 8). Im linken Fenster werden die Gleichungen

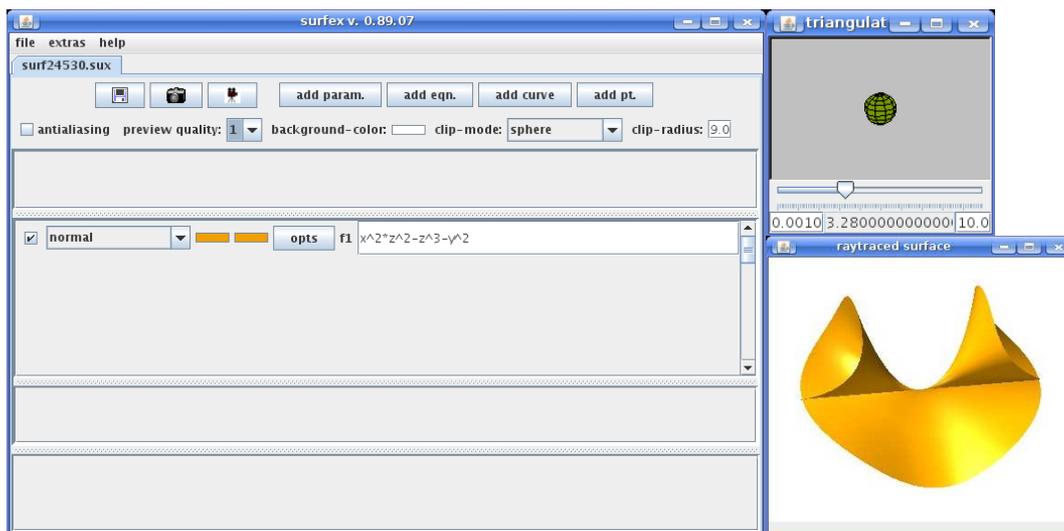


ABBILDUNG 8. Surfex

eingetragen; das obere rechte Fenster dient dazu, die Fläche zu drehen und die Größe des Ausschnitts zu verändern; im dritten Fenster wird die Fläche angezeigt.

Wie bei `Surf` kann man auch bei `Surfex` mit `SINGULAR` erst fortfahren, wenn man `Surfex` beendet hat. Zudem gibt es eine Besonderheit zu beachten. Wenn man `Surfex` von `SINGULAR` aufruft, dann werden die Variablennamen wie folgt verändert: die erste Variable in der Ringdefinition in `SINGULAR` wird zu x umbenannt, die zweite zu y und die dritte zu z . In unserem Beispiel oben wird also t zu x , x zu y und y zu z . Damit wird aus dem Polynom $x^2 - y^2 \cdot (t^2 - y)$ das Polynom $y^2 - z^2 \cdot (y^2 - z)$.

Wie erwähnt, kann man `Surfex` auch verwenden, um zwei Flächen miteinander zu schneiden und sich den Schnitt der beiden Flächen auf einer der Flächen anzuzeigen. Wir führen dies am Beispiel des Polynoms $y^2 - z^2 \cdot (y^2 - z)$ und der Ebene $V(x - 1)$ vor. Wir haben in Abbildung 9 dem Polynom $y^2 - z^2 \cdot (y^2 - z)$, das bereits in Abbildung 8 zu sehen war, das Polynom $x - 1$ hinzugefügt, indem wir den Knopf `add eqn` verwendet haben. Die beiden Gleichungen erscheinen im dritten Teil des Fensters. Die beiden Flächen sind im linken Teil von Abbildung 10 zu sehen. Man sieht dort zudem in Schwarz die Schnittkurve der beiden Flächen. Um diese zu erzeugen haben wir den Knopf `add curve` verwendet. Dadurch wurde uns im vierten

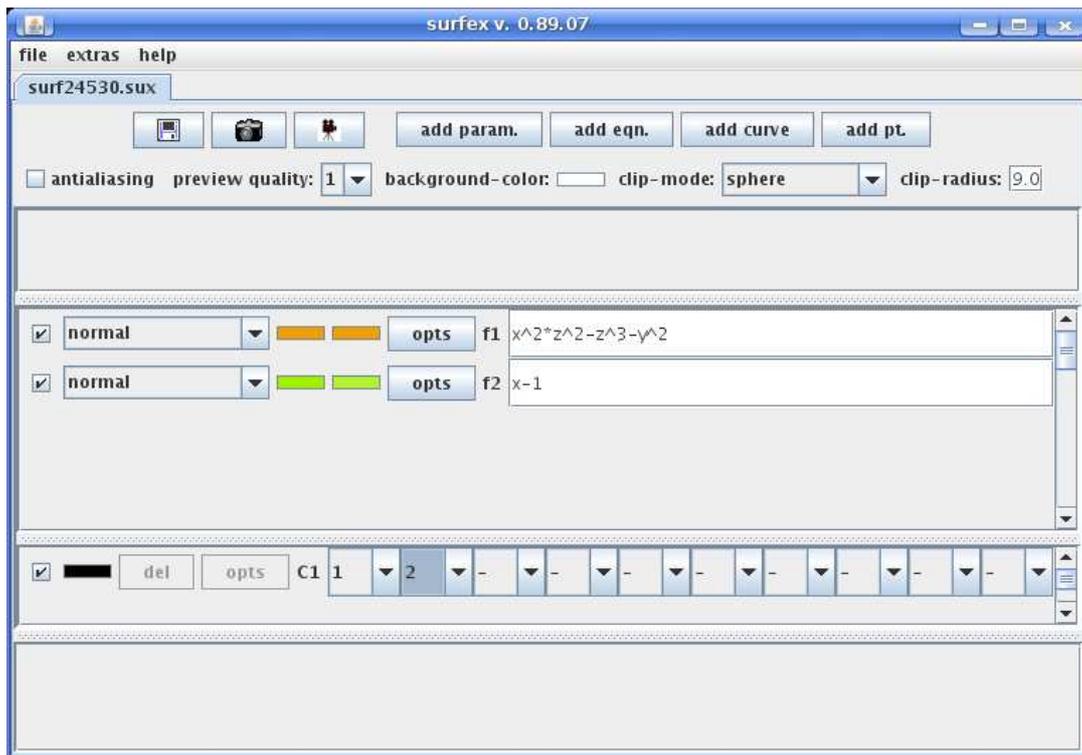


ABBILDUNG 9. Der Schnitt von $V(y^2 - z^2 \cdot (y^2 - z))$ und $V(x - 1)$

Teil des Fensters die Möglichkeit gegeben, Zahlen auszuwählen. Wir haben die Zahlen 1 und 2 ausgewählt. Dies bedeutet, daß auf der Fläche, die durch das Polynom f_1 definiert wird, der Schnitt mit der Fläche abgebildet werden soll, die durch das Polynom f_2 definiert wird. Im rechten Teil von Abbildung 10 sind nur die Fläche $V(y^2 - z^2 \cdot (y^2 - z))$ und die Schnittkurve zu sehen. Dies erreicht man, indem man in Surfex (Abbildung 9) den Haken vor dem Polynom $x - 1$ entfernt.

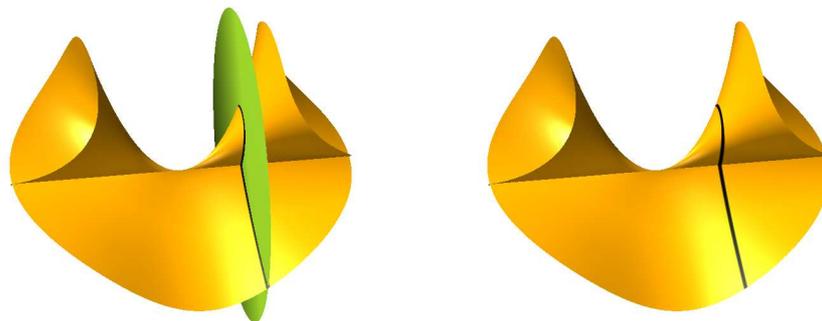


ABBILDUNG 10. Der Schnitt von $V(y^2 - z^2 \cdot (y^2 - z))$ und $V(x - 1)$

Für weitere Hinweise zur Benutzung von Surfex verweisen wir auf Kapitel 8.

J) Aufgaben**Aufgabe 1.32**

Visualisieren Sie die Lösungsmengen der folgenden Gleichungen zunächst ohne Zuhilfenahme des Rechners, und dann mit Hilfe von Surf:

a. $y^2 - x^4 + 2x^2 - 1 = 0.$

b. $\frac{1}{4} \cdot x^2 + \frac{1}{9} \cdot y^2 = 1.$

c. $x^3 - y^2 - z^2 = 0.$

Aufgabe 1.33

Visualisieren Sie die Lösungsmenge der folgenden Gleichungen mit Surf:

a. $(x^2 + y^2)^3 - 4x^2y^2 = 0.$

b. $x^4 + 6x^2y - y^3 = 0.$

c. $516x^4y - 340x^2y^3 + 57y^5 - 640x^4 - 168x^2y^2 + 132y^4 - 384x^2y + 292y^3 + 1024x^2 = 0.$

Aufgabe 1.34

Visualisieren Sie die Lösungsmenge der folgenden Gleichungen mit Surfex:

a. $(2 \cdot x^2 + y^2 + z^2 - 1)^3 - 1/10 \cdot x^2 \cdot z^3 - y^2 \cdot z^3 = 0.$

b. $(1 - 3x - 3y - 3z) \cdot (xy + yz + zx) + 5xyz = 0.$

c. $256x^3 - 128x^2z^2 + 144xy^2z + 16xz^4 - 27y^4 - 4y^2z^3 = 0.$

d. $(x + y + z - 1) \cdot (x - y - z - 1) \cdot (y - x - z - 1) \cdot (z - x - y - 1) \cdot (x + y + z + 1) \cdot (x - y - z + 1) \cdot (y - x - z + 1) \cdot (z - x - y + 1) + (x^2 + y^2 + z^2 - 1) \cdot (x^2 + y^2 + z^2 - 1) \cdot (x^2 + y^2 + z^2 - 2) \cdot (x^2 + y^2 + z^2 - 2) = 0.$

Aufgabe 1.35

Visualisieren Sie die Lösungsmenge des folgenden Gleichungssystems mit Surfex:

$$x^2 + y^2 + z^2 = 1 \quad \text{und} \quad x^2z - y^3 = 0.$$

Aufgabe 1.36

Visualisieren Sie die Lösungsmenge des folgenden Gleichungssystems mit Surfex:

$$xz - y^2 = 0, \quad y - z^2 = 0 \quad \text{und} \quad x - yz = 0.$$

Aufgabe 1.37

Seien $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ und $I = \langle f_1, \dots, f_k \rangle$ das von den f_i erzeugte Ideal. Beweisen Sie, daß

$$\underline{a} \in V(f_1, \dots, f_k) \iff g(\underline{a}) = 0 \quad \text{für alle } g \in I.$$

Aufgabe 1.38

Berechnen Sie die Gleichung des Bildes der Parametrisierung

$$F: \mathbb{A}_{\mathbb{R}} \longrightarrow \mathbb{A}_{\mathbb{R}}^2 : t \mapsto \left(\frac{-t^4 - 6 \cdot t^3 + 3}{3 \cdot (1 + t^2)^2}, \frac{8 \cdot t^3}{3 \cdot (1 + t^2)^2} \right),$$

und visualisieren Sie diese mit Surf.

Aufgabe 1.39

Berechnen Sie die Gleichung des Bildes der Parametrisierung

$$F: \mathbb{A}_{\mathbb{R}} \longrightarrow \mathbb{A}_{\mathbb{R}}^2 : t \mapsto \left(\frac{t^3 + 1}{t^4 + 1}, \frac{t^4 + t}{t^4 + 1} \right),$$

und visualisieren Sie diese mit **Surf**.

Aufgabe 1.40

Berechne die Gleichung des Bildes der Parametrisierung

$$F: \mathbb{A}_{\mathbb{R}} \longrightarrow \mathbb{A}_{\mathbb{R}}^2 : s \mapsto \left(\frac{-24s^3 + 12s^2 - 2s + 1}{16s^4 + 24s^2 + 1}, \frac{24s^3 + 12s^2 + 2s + 1}{16s^4 + 24s^2 + 1} \right)$$

und visualisieren Sie diese mit **Surf**.

Aufgabe 1.41

Berechnen Sie die Gleichung des Bildes der Parametrisierung

$$F: \mathbb{A}_{\mathbb{R}}^2 \longrightarrow \mathbb{A}_{\mathbb{R}}^3 : (s, t) \mapsto (s^2, st, t^2)$$

und visualisieren Sie diese mit **Surf** oder mit **Surfex**.

Aufgabe 1.42

Berechnen Sie die Gleichung des Bildes der Parametrisierung

$$F: \mathbb{A}_{\mathbb{R}}^2 \longrightarrow \mathbb{A}_{\mathbb{R}}^3 : (s, t) \mapsto (t^2 - st, s^2 - st, t^2 - s^2)$$

und visualisieren Sie diese mit **Surf** oder mit **Surfex**.

Aufgabe 1.43

Visualisieren Sie die Familie von Kurven die durch die Familie von Polynomen

$$f_t = x^2y - y^3 + t^2 \cdot x^5, \quad t \in \mathbb{R},$$

gegeben ist mit **Surfex**, und zeichnen Sie auf dieser Familie die Kurven für $t = 0$, $t = 1$ und $t = 2$ ein. Visualisieren Sie diese Kurven auch mit **Surf**.

2 KEGELSCHNITTE

(VON OLIVER LABS)

Siehe Olivers Skript.

3 DIE PROJEKTIVE EBENE

(VON THOMAS MARKWIG)

A) Die Konstruktion der projektiven Ebene

Wir haben unsere Betrachtungen mit der Frage begonnen, was eine Gerade ist, und die Frage hat uns zu einer Beschreibung von Geraden in der affinen Ebene geführt. Die Geraden werden es nun auch wieder sein, die uns von der affinen Geometrie wegführen. Zwei (verschiedene) Geraden in der affinen Ebene können sich schneiden oder sie können parallel sein. Ein derartig inkonsistentes Verhalten ist unbefriedigend!

Beispiel 3.1

Betrachten wir die Geraden

$$G_1 = V(x - y - 1)$$

und

$$G_2 = V(x + y - 1)$$

so schneiden sie sich im Punkt

$$G_1 \cap G_2 = \{(1, 0)\},$$

während die Gerade G_1 mit der Geraden

$$G_3 = V(x - y + 1)$$

keinen Schnittpunkt hat; die beiden sind parallel zueinander.



ABBILDUNG 11. Schnittverhalten von Geraden in der affinen Ebene

Wir wollen die affine Ebene deshalb erweitern, neue Punkte hinzunehmen. Wäre es nicht schön, wenn wir für jede Parallelenschar von Geraden einen neuen Punkt hinzufügen könnten, in dem sich die Geraden der Parallelenschar schneiden? Erstaunlicherweise läßt sich dies recht einfach und effizient realisieren. Das Ergebnis nennen wir die projektive Ebene. Dieser wollen wir uns nun schrittweise nähern.

Konstruktion 3.2 (Projektive Ebene)

Wir betten die affine Ebene $\mathbb{A}_{\mathbb{R}}^2$ zunächst in den dreidimensionalen Anschauungsraum \mathbb{R}^3 ein, indem wir die Punkte mit z-Koordinate eins betrachten (siehe Abbildung 12):

$$\mathbb{A}_{\mathbb{R}}^2 \equiv \{(x, y, 1) \in \mathbb{R}^3 \mid x, y \in \mathbb{R}\} = E$$

Etwas mathematischer ausgedrückt bedeutet dies, daß die Abbildung

$$\varphi : \mathbb{A}_{\mathbb{R}}^2 \longrightarrow \mathbb{R}^3 : (x, y) \mapsto (x, y, 1)$$

eine injektive Abbildung mit Bild $\text{Im}(\varphi) = E$ ist (siehe Abbildung 12).

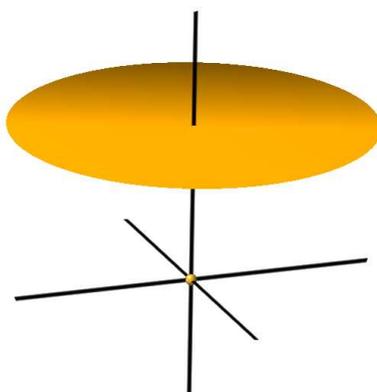


ABBILDUNG 12. Die affine Ebene eingebettet im \mathbb{R}^3 mit Koordinatenkreuz

Durch den Ursprung $O = (0, 0, 0) \in \mathbb{R}^3$ des Anschauungsraumes und einen Punkt $P \in E$ der Ebene E geht genau eine Gerade G_P , und für zwei verschiedenen Punkte $P \neq Q$ von E erhalten wir zwei verschiedene Geraden $G_P \neq G_Q$ (siehe Abbildung 13).

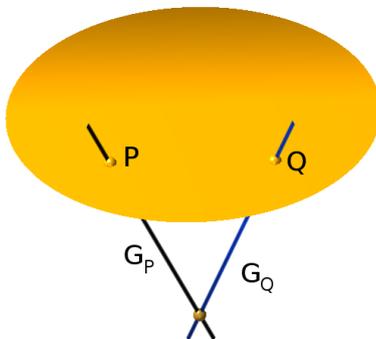


ABBILDUNG 13. Die Punkte P und Q in E mit den Geraden G_P und G_Q

Wir können die Punkte von E (und damit die Punkte der affinen Ebene $\mathbb{A}_{\mathbb{R}}^2$) also mit gewissen Ursprungsgraden in \mathbb{R}^3 identifizieren:

$$\psi : E \leftrightarrow \mathbb{P} = \{L \subseteq \mathbb{R}^3 \mid L \text{ ist Ursprungsgerade}\} : P \mapsto G_P.$$

Freilich erhalten wir auf diesem Weg nicht alle Ursprungsgeraden im Anschauungsraum. Eine Gerade in der xy -Ebene ist parallel zur Ebene E und wird diese nicht schneiden. Wir haben also noch einige Ursprungsgeraden in der Hinterhand (siehe Abbildung 14).

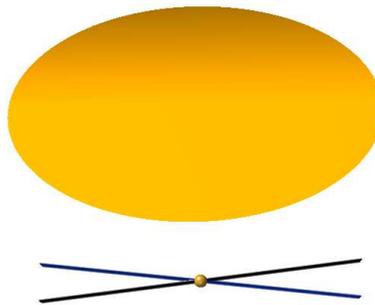


ABBILDUNG 14. Die Ebene E mit zwei parallelen Ursprungsgeraden

Betrachten wir nun die Punkte einer Geraden $L \subset E$ in der Ebene E , so liegen die zugehörigen Ursprungsgeraden G_P , $P \in L$, sämtlich in einer festen Ursprungsebene E_L . In diesem Sinne kann man eine Gerade L in der Ebene E also mit einer Ursprungsebene E_L identifizieren (siehe Abbildung 15).

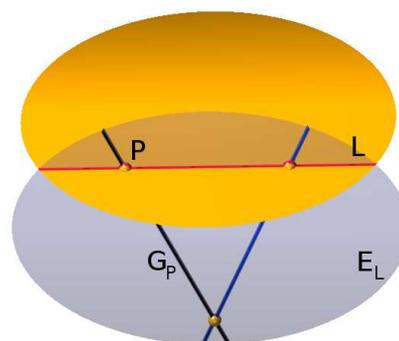


ABBILDUNG 15. Die Gerade L in E und die Ursprungsebene E_L

Je zwei solcher Ursprungsebenen E_L und $E_{L'}$ schneiden sich in einer Ursprungsgeraden. Haben L und L' in E den Schnittpunkt P , so muß diese Ursprungsgerade G_P sein, da eine Gerade durch zwei Punkte festgelegt ist, in diesem Fall durch die

Punkte O und P . Wir können den Schnittpunkt von L und L' also unmittelbar an E_L und $E_{L'}$ ablesen (siehe Abbildung 16).

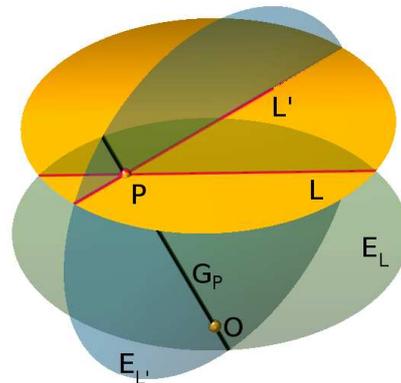


ABBILDUNG 16. $P = L \cap L'$ und $E_L \cap E_{L'} = G_P$

Wären L und L' jedoch parallel, so wird die Schnittgerade G von E_L und $E_{L'}$ eine Ursprungsgerade sein, die E nicht schneidet. Sie liegt mithin in der xy -Ebene. Der Richtungsvektor der Schnittgeraden in der xy -Ebene ist der Richtungsvektor der beiden parallelen Geraden L und L' in der Ebene E . Da die Schnittgerade G durch den Punkt O und ihren Richtungsvektor festgelegt ist, liefert der Schnitt von E_L mit $E_{L''}$ für jede zu L parallele Gerade L'' die gleiche Ursprungsgerade G (siehe Abbildung 17).

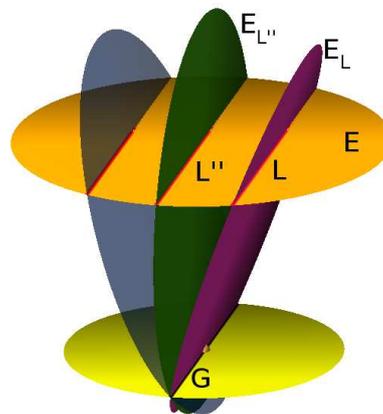


ABBILDUNG 17. $E_L \cap E_{L''} = G$ ist eine Gerade in der xy -Ebene

Unsere Identifizierung der Punkte P von E mit gewissen Ursprungsgeraden G_P in der Menge aller Ursprungsgeraden \mathbb{P} war strukturerhaltend insofern, als wir dabei Geraden und Schnittpunkte von Geraden wiederfinden konnten. In \mathbb{P} haben wir aber mehr ‘‘Punkte’’ zur Verfügung als in E . Und wir finden auf diese Weise für die zu L parallelen Geraden den gemeinsamen ‘‘Schnittpunkt’’ G in \mathbb{P} , einen Punkt, der in E keine Entsprechung hatte. \square

Wir wollen nun diese Beschreibung der *projektiven Ebene* als Ursprungsgeraden im \mathbb{R}^3 mathematisch präziser fassen. Dabei werden wir uns zugleich Koordinaten in der projektiven Ebene besorgen, die unabdingbar sind, wenn wir Kurven mit Mitteln der Algebra beschreiben wollen. Außerdem werden wir \mathbb{R} wieder durch einen beliebigen Körper K ersetzen.

Definition 3.3 (Die projektive Ebene)

Für einen Punkt $(0, 0, 0) \neq (x, y, z) \in K^3$ bezeichnen wir mit

$$(x : y : z) = \{(\lambda \cdot x, \lambda \cdot y, \lambda \cdot z) \mid \lambda \in K\}$$

die Ursprungsgerade durch den Punkt (x, y, z) . Wir nennen die Menge

$$\mathbb{P}_K^2 = \{(x : y : z) \mid (0, 0, 0) \neq (x, y, z) \in K^3\}$$

die *projektive Ebene* über K , und wir nennen $(x : y : z)$ die *projektiven Koordinaten* des Punktes.

Bemerkung 3.4

Die projektiven Koordinaten eines Punktes der projektiven Ebene sind nur bis auf ein skalares Vielfaches eindeutig bestimmt. Z.B.

$$(1 : 1 : 0) = \{(\lambda, \lambda, 0) \mid \lambda \in \mathbb{R}\} = (2 : 2 : 0) \in \mathbb{P}_{\mathbb{R}}^2.$$

Bemerkung 3.5 (Die Einbettung der affinen Ebene)

Die Abbildung

$$\varphi : \mathbb{A}_K^2 \longrightarrow \mathbb{P}_K^2 : (x, y) \mapsto (x : y : 1)$$

ist injektiv, d.h. verschiedene Punkte in der affinen Ebene werden auf verschiedene Punkte in der projektiven Ebene abgebildet. Wir können die affine Ebene also mit ihrem Bild

$$E = \text{Im}(\varphi) = \{(x : y : 1) \mid (x, y) \in \mathbb{A}_K^2\}$$

identifizieren. E füllt die projektive Ebene fast ganz aus,

$$\mathbb{P}_K^2 \setminus E = \{(x : y : 0) \mid (x, y) \neq (0, 0)\} = \{(x : 1 : 0) \mid x \in K\} \cup \{(0 : 1 : 0)\},$$

es fehlen nur die Ursprungsgeraden, die in der xy -Ebene liegen. Man kann dies mit Hilfe von Begriffen aus der Topologie auch präziser formulieren: E ist eine offene dichte Teilmenge der projektiven Ebene. Wir verzichten hier aber wieder darauf eine entsprechende Topologie auf der projektiven Ebene einzuführen.

B) Projektive Kurven

Wir möchten nun auch den Begriff der Geraden oder allgemeiner den Begriff algebraischer Kurven in der projektiven Ebene definieren und dabei den Ansatz in der affinen Ebene imitieren. Eine Kurve sollte also die Lösungsmenge einer polynomialen Gleichung sein. Dabei stoßen wir aber auf Probleme, da die projektiven Koordinaten nicht eindeutig sind.

Beispiel 3.6

Ist der Punkt $(1 : 1 : 1) \in \mathbb{P}_{\mathbb{R}}^2$ eine Lösung der polynomialen Gleichung

$$x^2 - y - z = 0?$$

Setzen wir die Koordinaten ein, so erhalten wir

$$1^2 - 1 - 1 = -1 \neq 0.$$

Die Antwort scheint also nein zu sein. Wir erinnern uns aber, daß die projektiven Koordinaten nur bis auf ein skalares Vielfaches bestimmt sind. Also gilt:

$$(1 : 1 : 1) = (2 : 2 : 2).$$

Setzen wir nun diese Koordinaten ein, so erhalten wir

$$2^2 - 2 - 2 = 0,$$

die Gleichung ist erfüllt! Was lernen wir daraus?

Die Frage, ob ein Punkt der projektiven Ebene mit Koordinaten $(a : b : c)$ die Gleichung $x^2 - y - z = 0$ erfüllt, ist *keine sinnvolle Frage*, sie ist schlicht unzulässig!

Ist unser Ansatz damit gestorben? Nein! Aber wir müssen uns bei der Frage auf solche Gleichungen beschränken, die unabhängig von den gewählten Koordinaten eines Punktes erfüllt oder nicht erfüllt sind! Dazu führen wir den Begriff des *homogenen* Polynoms ein. Wir tun dies für Polynome in einer beliebigen Anzahl an Veränderlichen.

Definition 3.7 (Homogene Polynome)

Ein Polynom $0 \neq F \in \mathbb{K}[x_1, \dots, x_n]$ heißt *homogen* vom Grad d , wenn es die Form

$$F = \sum_{|\alpha|=d} a_{\alpha} \cdot \underline{x}^{\alpha}$$

hat, d.h. wenn jedes Monom von F den Grad d hat. Wir werden im folgenden der besseren Unterscheidbarkeit halber homogene Polynome meist mit Großbuchstaben bezeichnen und nicht homogene Polynome meist mit Kleinbuchstaben.

Beispiel 3.8

Das Polynom

$$F = x^4 + 3x^2y^2 - 5xyz^2 + z^4$$

ist homogen vom Grad 4, da die Monome von f ,

$$x^4, x^2y^2, xyz^2 \text{ und } z^4,$$

alle den Grad 4 haben. Hingegen ist das Polynom

$$g = x^2 - y - z$$

nicht homogen, da das Monom x^2 den Grad 2 hat, die Monome y und z aber den Grad 1.

Bemerkung 3.9 (Homogene Polynome)

Ist $0 \neq F \in \mathbb{K}[x_1, \dots, x_n]$ homogen vom Grad d und sind $\lambda, c_1, \dots, c_n \in \mathbb{K}$, so gilt

$$\begin{aligned} F(\lambda \cdot c_1, \dots, \lambda \cdot c_n) &= \sum_{|\alpha|=d} a_\alpha \cdot (\lambda \cdot c_1)^{\alpha_1} \cdots (\lambda \cdot c_n)^{\alpha_n} \\ &= \sum_{\alpha_1 + \dots + \alpha_n = d} a_\alpha \cdot \lambda^{\alpha_1 + \dots + \alpha_n} \cdot c_1^{\alpha_1} \cdots c_n^{\alpha_n} \\ &= \lambda^d \cdot \sum_{\alpha_1 + \dots + \alpha_n = d} a_\alpha \cdot c_1^{\alpha_1} \cdots c_n^{\alpha_n} \\ &= \lambda^d \cdot F(c_1, \dots, c_n). \end{aligned}$$

Ist λ ungleich null, so gilt für ein homogenes Polynom also

$$F(c_1, \dots, c_n) = 0 \iff F(\lambda \cdot c_1, \dots, \lambda \cdot c_n) = 0.$$

Ist $F \in \mathbb{K}[x, y, z]$ ein homogenes Polynom, so können wir also fragen, ob ein Punkt der projektiven Ebene mit Koordinaten $(a : b : c)$ der Gleichung $F(a, b, c) = 0$ genügt, und die Antwort wird nicht von den gewählten Koordinaten abhängen!

Beispiel 3.10

Der Punkt $(1 : 1 : 1) = (2 : 2 : 2) \in \mathbb{P}_{\mathbb{K}}^2$ erfüllt die Gleichung

$$x^4 + 3x^2y^2 - 5xyz^2 + z^4 = 0,$$

und wir können dazu

$$1^4 + 3 \cdot 1^2 \cdot 1^2 - 5 \cdot 1 \cdot 1 \cdot 1^2 + 1^4 = 0$$

testen oder alternativ

$$2^4 + 3 \cdot 2^2 \cdot 2^2 - 5 \cdot 2 \cdot 2 \cdot 2^2 + 2^4 = 0.$$

Definition 3.11 (Projektive Kurven)

Ist $F \in \mathbb{K}[x, y, z]$ ein nicht-konstantes homogenes Polynom vom Grad d , so nennen wir

$$V(F) = \{(x : y : z) \in \mathbb{P}_{\mathbb{K}}^2 \mid F(x, y, z) = 0\}$$

die durch F definierte *ebene projektive algebraische Kurve* vom Grad d . Ist $d = 1$, so nennen wir $V(F)$ eine *projektive Gerade*. Die Gerade $V(z)$ heißt die *unendlich ferne Gerade*.

Bemerkung 3.12

Die projektive Ebene

$$\mathbb{P}_{\mathbb{K}}^2 = E \cup V(z)$$

ist die disjunkte Vereinigung der affinen Ebene E mit der unendlich fernen Geraden.

Wir wollen nun den Zusammenhang zwischen ebenen affinen und projektiven algebraischen Kurven betrachten.

Bemerkung 3.13 (Der projektive Abschluß einer affinen Kurve)

Ist $F \in K[x, y, z]$ ein homogenes Polynom, so nennen wir

$$F^{\text{dh}} = F(x, y, 1) \in K[x, y]$$

die *Dehomogenisierung* von F . Ist $f \in K[x, y]$ ein Polynom, so nennen wir

$$f^{\text{h}} = z^{\deg(f)} \cdot f\left(\frac{x}{z}, \frac{y}{z}\right) \in K[x, y, z]$$

die *Homogenisierung* von f . f^{h} ist ein homogenes Polynom, und es gilt die algebraische Beziehung

$$(f^{\text{h}})^{\text{dh}} = f \quad \text{und} \quad z^{\deg(F) - \deg(f)} \cdot (F^{\text{dh}})^{\text{h}} = F.$$

Uns interessieren aber weit mehr die geometrischen Beziehungen

$$V(f) = V(f^{\text{h}}) \cap E$$

und

$$V(F^{\text{dh}}) = V(F) \cap E,$$

wenn wir die affine Ebene $\mathbb{A}_{\mathbb{K}}^2$ mit der Ebene E mittels der Injektion φ aus Bemerkung 3.5 identifizieren.

Wir können einer affinen algebraischen Kurve $V(f)$ also die projektive algebraische Kurve zuordnen, die durch das Homogenisieren ihrer Gleichung entsteht. Im affinen Teil E der projektiven Ebene stimmt diese mit der ursprünglichen Kurve $V(f)$ überein. Wir bekommen lediglich auf der unendlich fernen Geraden $V(z)$ weitere Punkte dazu.

Mit den Begriffen der Topologie gilt, daß $V(f^{\text{h}})$ der Abschluß der affinen Kurve $V(f)$ in der projektiven Ebene ist. Wir nennen $V(f^{\text{h}})$ deshalb auch den *projektiven Abschluß* von $V(f)$.

Man beachte, ist f ein Polynom, so erhält man f^{h} , indem man jedes Monom $x^i y^j$ von f durch Multiplikation mit $z^{\deg(f) - i - j}$ auf den Grad $\deg(f)$ bringt!

Beispiel 3.14

Homogenisieren wir das Polynom $f = x - y - 1$, so erhalten wir

$$f^{\text{h}} = z^{\deg(f)} \cdot \left(\frac{x}{z} - \frac{y}{z} - 1\right) = x - y - z,$$

und entsprechend homogenisiert das Polynom $g = x - y + 1$ zu

$$g^{\text{h}} = x - y + z.$$

Wollen wir nun den Schnitt der beiden projektiven Geraden $V(x - y - z)$ und $V(x - y + z)$ berechnen, so müssen wir das lineare Gleichungssystem

$$x - y - z = 0$$

$$x - y + z = 0$$

lösen, und erhalten als Lösung die Ursprungsgerade

$$(1 : 1 : 0) = \{(\lambda, \lambda, 0) \mid \lambda \in \mathbb{K}\} \in \mathbb{P}_{\mathbb{R}}^2.$$

In der affinen Ebene waren die beiden Geraden $V(f)$ und $V(g)$ parallel, ihr projektiver Abschluß hat den Schnittpunkt $(1 : 1 : 0)$. Dabei ist der Vektor $(1, 1)$ der Richtungsvektor der beiden Geraden $V(f)$ und $V(g)$.

Beispiel 3.15 (Projektive Geraden)

Durch je zwei verschiedene Punkte $P = (a : b : c)$ und $P' = (a' : b' : c')$ der projektiven Ebene $\mathbb{P}_{\mathbb{K}}^2$ geht genau eine projektive Gerade. Daß die Punkte verschieden sind, bedeutet, daß die Matrix

$$A = \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$$

den Rang zwei hat. Das homogene lineare Gleichungssystem

$$\begin{aligned} ax + by + cz &= 0 \\ a'x + b'y + c'z &= 0 \end{aligned}$$

hat also einen eindimensionalen Lösungsraum $\text{Ker}(A)$. Ist $(0, 0, 0) \neq (\alpha, \beta, \gamma) \in \text{Ker}(A)$ ein vom Nullvektor verschiedener Punkt im Lösungsraum, so liegen die Punkte P und P' auf der projektiven Geraden

$$V(\alpha \cdot x + \beta \cdot y + \gamma \cdot z).$$

Zudem müssen die Koeffizienten jeder Geraden, die durch P und P' geht, in $\text{Ker}(A)$ liegen. Da $\text{Ker}(A)$ eindimensional ist, kann sich die Gleichung von $\alpha \cdot x + \beta \cdot y + \gamma \cdot z = 0$ aber nur um ein skalares Vielfaches unterscheiden. Damit stimmen die beiden Geraden aber überein.

Beispiel 3.16

Der projektive Abschluß der affinen algebraischen Kurve $V(xy + x^2y - y^3)$ schneidet die unendlich ferne Gerade in drei Punkten. Um dies zu sehen, berechnen wir

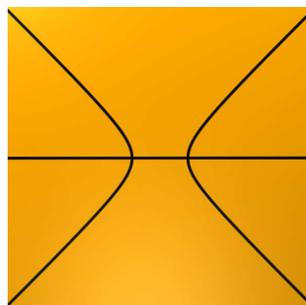


ABBILDUNG 18. Die affine algebraische Kurve $V(xy + x^2y - y^3)$

zunächst die Homogenisierung

$$f^h = xyz + x^2y - y^3$$

von $f = xy - x^2y - y^3$. Dann müssen wir das Gleichungssystem

$$\begin{aligned}xyz + x^2y - y^3 &= 0 \\z &= 0\end{aligned}$$

lösen. Da die zweite Gleichung bereits nach z aufgelöst ist, können wir z in der ersten Gleichung ersetzen und erhalten das gleichwertige Gleichungssystem:

$$\begin{aligned}x^2y - y^3 &= 0 \\z &= 0\end{aligned}$$

Die linke Seite der ersten Gleichung zerfällt dabei in das folgende Produkt von Linearfaktoren:

$$x^2y - y^3 = y \cdot (x - y) \cdot (x + y).$$

Wir erhalten als Lösung mithin die Ursprungsgeraden

$$y = 0 \quad \text{und} \quad z = 0$$

sowie

$$x = y \quad \text{und} \quad z = 0$$

und schließlich

$$x = -y \quad \text{und} \quad z = 0.$$

Insgesamt erhalten wir also

$$V(f^h) \cap V(z) = \{(1 : 0 : 0), (1 : 1 : 0), (1 : -1 : 0)\}$$

als den Schnitt des projektiven Abschlusses von $V(xy + x^2y - y^3)$ mit der unendlich fernen Geraden.

C) Visualisierung projektiver Kurven

Das Bild in Abbildung 18 zeigt die affine Kurve $V(xy + x^2y - y^3)$, oder genauer gesagt, einen Ausschnitt dieser Kurve. Können wir auch die projektive Kurve in ihrer Gesamtheit visualisieren? In der Tat können wir das!

Beispiel 3.17

Wollen wir die projektive Kurve $V(xyz + x^2y - y^3) \subset \mathbb{P}_{\mathbb{R}}^2$ visualisieren, so können wir statt dessen einfach die Menge

$$\{(x, y, z) \in \mathbb{R}^3 \mid xyz + x^2y - y^3 = 0\} \subset \mathbb{R}^3$$

betrachten. Dies ist eine Fläche im \mathbb{R}^3 , die die Vereinigung von Ursprungsgeraden ist, und diese Ursprungsgeraden bilden unsere projektive Kurve (siehe Abbildung 19). Sehr erhellend ist dieses Bild jedoch nicht. Schneiden wir diese Fläche mit der Ebene $E = \{z = 1\}$, so erhalten wir das zugehörige affine Bild (siehe Abbildung 20).

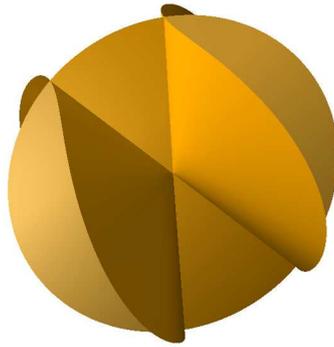


ABBILDUNG 19. Die Fläche $xyz + x^2y - y^3 = 0$.

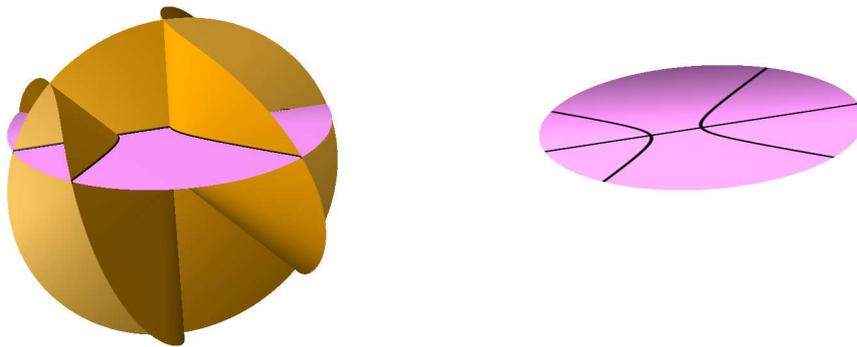


ABBILDUNG 20. Die Fläche $xyz + x^2y - y^3 = 0$ geschnitten mit E .

Diese Art der Visualisierung ist unbefriedigend. Im ersten Bild sehen wir die projektive Kurve als Fläche. Durch diese zusätzliche Dimension übersehen wir wesentliche Eigenschaften. Im zweiten Bild haben wir wieder nur einen affinen Ausschnitt. Wie können wir die projektiven Kurven *eindimensional* visualisieren und dennoch *alle* Punkte sehen, auch die auf der unendlich fernen Geraden?

Die Punkte der projektiven Ebene sind Ursprungsgeraden im Anschauungsraum. Wir haben das Gros dieser Ursprungsgeraden mit Punkten in der affinen Ebene identifiziert, indem wir die Ursprungsgeraden mit einer Ebene E geschnitten haben, die parallel zur xy -Ebene war. Jede Ursprungsgerade, die nicht in der xy -Ebene lag, hat uns dabei genau einen Punkt in der Ebene geliefert. Allerdings haben einige der projektiven Punkte, sprich einige Ursprungsgeraden, keinen Punkt in der affinen Ebene geliefert, weil sie die affine Ebene nicht geschnitten haben. Wir sollten die Ebene E also durch eine Fläche ersetzen, die von jeder Ursprungsgeraden geschnitten wird! Dafür müssen wir allerdings die Forderung aufgeben, daß die Fläche von jeder Geraden nur einmal geschnitten wird!

Bemerkung 3.18 (Visualisierung projektiver Kurven)

Die Oberfläche der Einheitskugel

$$\mathbb{S}_{\mathbb{R}}^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$$

wird die *2-Sphäre* genannt. Den Schnitt mit der xy -Ebene nennen wir den *Äquator*, die Punkte oberhalb der xy -Ebene die *obere Hemisphäre* (siehe Abbildung 21).

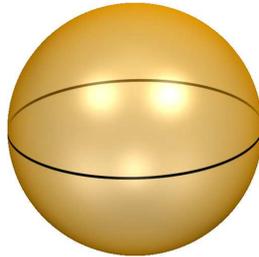


ABBILDUNG 21. Die 2-Sphäre mit Äquator.

Jede Ursprungsgerade trifft die 2-Sphäre in genau zwei Punkten, und jede Ursprungsgerade, die nicht in der xy -Ebene liegt, trifft die obere Hemisphäre in genau einem Punkt (siehe Abbildung 22).

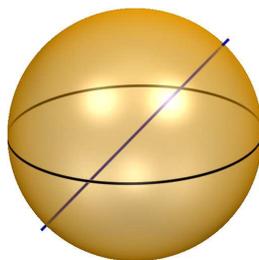


ABBILDUNG 22. Die 2-Sphäre mit einer Ursprungsgeraden.

Wir können die obere Hemisphäre also mit der affinen Ebene identifizieren. Außerdem trifft jede Ursprungsgerade, die in der xy -Ebene liegt, den Äquator in einem Punktepaar, das punktsymmetrisch zum Ursprung liegt. Wir können einen Punkt der unendlich fernen Geraden also mit einem solchen Punktepaar identifizieren. Wenn wir dies tun, so können wir die obere Hemisphäre der 2-Sphäre zusammen mit dem Äquator als ein Modell für die projektive Ebene ansehen. In diesem Modell können wir unsere Kurve $V(xyz + x^2y - y^3)$ visualisieren (siehe Abbildung 23). Die Kurve schneidet den Äquator in drei Punktepaaren, die den drei Schnittpunkten der Kurve mit der unendlich fernen Geraden entsprechen (vgl. Beispiel 3.16).

Man sollte auch das Bild in Abbildung 20 mit der oberen Hemisphäre der Abbildung 23 vergleichen. Beides sind Visualisierungen der gleichen affinen Kurve. In Abbildung 20 sieht man eine Gerade, die von den zwei Zweigen einer Hyperbel geschnitten wird. In Abbildung 23 sehen wir die Gerade als Großkreis auf der oberen Hemisphäre, und wir sehen auch die beiden Zweige der Hyperperbel. Wir sehen aber noch mehr. Die Enden des einen Hyperbelzweiges treffen die Enden des anderen Hyperperbelzweiges im Unendlichen. Die beiden Zweige der Hyperperbel sind also nicht mehr

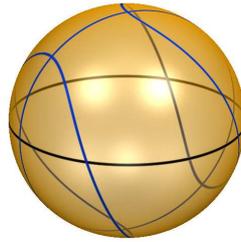


ABBILDUNG 23. Ein Modell des $\mathbb{P}_{\mathbb{R}}^2$ mit der Kurve $V(xyz + x^2y - y^3)$.

getrennt sondern bilden eine geschlossene Kurve! Dies gilt allgemein für projektive Kurven. Den Fall von Hyperbeln, oder allgemein von Kegelschnitten wollen wir am Ende dieses Kapitels aber noch mal etwas genauer betrachten.

Projektive Kurven sind immer geschlossen; sie haben keine Enden! Etwas präziser ausgedrückt, projektive Kurven sind kompakt!

D) Projektive Koordinatentransformationen

Wir haben schon bei der Betrachtung von affinen Kegelschnitten gesehen (siehe Kapitel 2), daß es hilfreich sein kann, die Koordinaten zu wechseln, um die strukturellen Merkmale einer affinen algebraischen Hyperfläche besser zu sehen. In der affinen Ebene lassen wir affine Koordinatentransformationen zu, das sind invertierbare lineare Abbildungen gefolgt von einer Verschiebung – hierbei ist es geschickter, Punkte (x, y) in der affinen Ebene $\mathbb{A}_{\mathbb{K}}^2$ als Spaltenvektoren

$$(x, y)^t = \begin{pmatrix} x \\ y \end{pmatrix}$$

zu schreiben:³

$$\mathbb{A}_{\mathbb{K}}^2 \longrightarrow \mathbb{A}_{\mathbb{K}}^2 : (x, y)^t \mapsto A \cdot (x, y)^t + v^t,$$

wobei

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \text{Gl}_2(\mathbb{K})$$

eine invertierbare 2×2 -Matrix⁴ mit Koeffizienten in \mathbb{K} ist und $v = (v_1, v_2) \in \mathbb{K}^2$ ein Verschiebungsvektor ist.

³Der Exponent t beim Vektor steht für *Transponieren*.

⁴Für eine positive ganze Zahl n bezeichnet $\text{Gl}_n(\mathbb{K})$ die Menge der invertierbaren $n \times n$ -Matrizen mit Einträgen aus \mathbb{K} . Diese Menge ist mit der Matrixmultiplikation eine Gruppe, im Englischen *general linear group* genannt – daher rührt das Kürzel *Gl*.

Bemerkung 3.19 (Projektive Koordinatentransformationen)

Welche Koordinatentransformationen wollen / können wir in der projektiven Ebene zulassen?

Wir müssen bedenken, daß die projektiven Koordinaten nur bis auf ein skalares Vielfaches eindeutig bestimmt sind. Die Transformationen, die wir zulassen, müssen dem Rechnung tragen.

Damit scheidet Verschiebungen der Koordinaten aus, denn $(2, 2, 2)$ ist ein Vielfaches von $(1, 1, 1)$, aber wenn wir zu beiden Vektoren den Vektor $(1, 2, 3)$ addieren, so erhalten wir die Vektoren $(3, 4, 5)$ bzw. $(4, 5, 6)$, die keine Vielfachen voneinander sind.

Transformationen mit invertierbaren 3×3 -Matrizen

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \text{Gl}_3(\mathbb{K})$$

sind hingegen zulässig, denn aus

$$(x', y', z') = \lambda \cdot (x, y, z)$$

folgt unmittelbar

$$A \cdot (x', y', z')^t = \lambda \cdot A \cdot (x, y, z)^t.$$

Dies liegt daran, daß die Multiplikation mit einer Matrix eine *lineare* Operation ist.

Die Koordinatentransformationen der projektiven Ebene sind also im Prinzip einfacher als die der affinen Ebene!

In der folgenden Definition beachten wir, daß

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_{11} \cdot x + a_{12} \cdot y + a_{13} \cdot z \\ a_{21} \cdot x + a_{22} \cdot y + a_{23} \cdot z \\ a_{31} \cdot x + a_{32} \cdot y + a_{33} \cdot z \end{pmatrix}.$$

Definition 3.20 (Projektive Koordinatentransformation)

Ist $A \in \text{Gl}_3(\mathbb{K})$ eine invertierbare 3×3 -Matrix, so nennen wir die Abbildung

$$\Phi_A : \mathbb{P}_{\mathbb{K}}^2 \longrightarrow \mathbb{P}_{\mathbb{K}}^2 : (x : y : z) \mapsto \Phi_A(x : y : z)$$

mit

$$\Phi_A(x : y : z) = (a_{11}x + a_{12}y + a_{13}z : a_{21}x + a_{22}y + a_{23}z : a_{31}x + a_{32}y + a_{33}z)$$

eine *projektive Koordinatentransformation* der projektiven Ebene.

Bemerkung 3.21 ($\text{PGL}_3(\mathbb{K})$)

Ist $A \in \text{Gl}_3(\mathbb{K})$ eine invertierbare Matrix und $0 \neq \lambda \in \mathbb{K}$, dann gilt

$$\Phi_A(x : y : z) = \Phi_{\lambda \cdot A}(x : y : z)$$

für alle $(x : y : z) \in \mathbb{P}_{\mathbb{K}}^2$. Zwei invertierbare Matrizen, die sich nur um ein skalares Vielfaches unterscheiden, definieren also die gleiche projektive Koordinatentransformation. Man kann die projektiven Koordinatentransformationen von $\mathbb{P}_{\mathbb{K}}^2$ deshalb auch mit der Faktorgruppe $\text{PGL}_3(\mathbb{K}) = \text{GL}_3(\mathbb{K})/\mathbb{D}$ identifizieren, wenn \mathbb{D} die Untergruppe

$$\mathbb{D} = \left\{ \left(\begin{array}{ccc} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{array} \right) \mid 0 \neq \lambda \in \mathbb{K} \right\}$$

der Diagonalmatrizen ist.

Bemerkung 3.22 (Affine Koordinatentransformationen im Projektiven)

Welche projektiven Koordinatentransformationen erhalten die affine Ebene und die unendlich ferne Gerade?

Etwas genauer formuliert, wann gilt

$$\Phi_A(V(z)) \subseteq V(z) \quad \text{und} \quad \Phi_A(E) \subseteq E?$$

Damit Φ_A die unendlich ferne Gerade $V(z)$ in sich selbst überführt, muß für das Polynom $F = z$ insbesondere

$$a_{31} = F(a_{11} : a_{21} : a_{31}) = F(\Phi_A(1 : 0 : 0)) = 0$$

und

$$a_{32} = F(a_{12} : a_{22} : a_{32}) = F(\Phi_A(0 : 1 : 0)) = 0$$

gelten. Also hat die Matrix A die Gestalt

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}.$$

Da A invertierbar ist, muß zudem $a_{33} \neq 0$ gelten. Da A und $\frac{1}{a_{33}} \cdot A$ die gleiche projektive Koordinatentransformation definieren, können wir $a_{33} = 1$ annehmen, so daß die Matrix die Gestalt

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{pmatrix}$$

hat. Setzen wir nun $v = (a_{13}, a_{23}) \in \mathbb{K}^2$ und

$$A' = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

dann hat A die Blockgestalt

$$A = \left(\begin{array}{cc|c} A' & v^t \\ \hline 0 & 0 & 1 \end{array} \right)$$

und wegen $\det(A') = \det(A) \neq 0$ ist $A' \in \text{Gl}_2(K)$ invertierbar. Multiplizieren wir A mit einem Vektor der Form $(x, y, 1)^t$, so erhalten wir

$$A \cdot (x, y, 1)^t = A' \cdot (x, y)^t + v^t.$$

Die von A induzierte projektive Abbildung Φ_A bildet also automatisch die affine Ebene E in sich selbst ab, und die Abbildung entspricht dabei der affinen Abbildung, die durch die Matrix A' und den Verschiebungsvektor v definiert wird!

Satz 3.23 (Standardkoordinaten)

Sind P, Q, R und S vier Punkte in der projektiven Ebene, von denen keine drei auf einer projektiven Geraden liegen, so gibt es eine invertierbare Matrix $A \in \text{Gl}_3(K)$, so daß

$$\begin{aligned}\Phi_A(P) &= (1 : 0 : 0), \\ \Phi_A(Q) &= (0 : 1 : 0), \\ \Phi_A(R) &= (0 : 0 : 1), \\ \Phi_A(S) &= (1 : 1 : 1).\end{aligned}$$

Beweis: Wir wählen zunächst Punkte $p, q, r, s \in \mathbb{R}^3 \setminus \{(0, 0, 0)\}$ auf den Ursprungsgeraden P, Q, R bzw. S . Daß keine drei der gegebenen Punkte auf einer projektiven Geraden liegen, bedeutet, daß je drei der vier Punkte p, q, r, s linear unabhängig sind. Insbesondere bilden die Punkte p, q, r eine Basis des K -Vektorraums K^3 . Damit ist s als eine Linearkombination in dieser Basis darstellbar, d.h. es gibt Koeffizienten $a, b, c \in K$, so daß

$$s = a \cdot p + b \cdot q + c \cdot r.$$

Da zudem s linear unabhängig von je zwei der drei Vektoren p, q, r ist, müssen alle drei Koeffizienten ungleich null sein.

Da die Vektoren p, q, r linear unabhängig sind, sind auch die Vektoren $a \cdot p, b \cdot q, c \cdot r$ linear unabhängig, und die Matrix B , deren Spalten diese Vektoren sind, ist invertierbar. Die Matrix $A = B^{-1} \in \text{Gl}_3(K)$ bildet $a \cdot p$ auf den ersten Einheitsvektor e_1 ab, $b \cdot q$ auf den zweiten Einheitsvektor e_2 , $c \cdot r$ auf den dritten Einheitsvektor e_3 und s auf den Vektor $(1, 1, 1)$. Da $a \cdot p$ aber auf der Ursprungsgeraden P liegt und $b \cdot q$ auf Q und $c \cdot r$ auf R , hat Φ_A die gewünschten Eigenschaften. \square

Bemerkung 3.24

Eine wichtige Frage ist, wie sich die Gleichung einer ebenen projektiven Kurve unter einer Koordinatentransformation ändert. Ist $A \in \text{Gl}_3(K)$ eine invertierbare 3×3 -Matrix und ist $F \in K[x, y, z]$ ein nicht-konstantes Polynom, so gilt

$$\Phi_A(V(F)) = V(F(A^{-1} \cdot (x, y, z)^t)),$$

wobei

$$F(A^{-1} \cdot (x, y, z)^t) = F(b_{11}x + b_{12}y + b_{13}z, b_{21}x + b_{22}y + b_{23}z, b_{31}x + b_{32}y + b_{33}z)$$

wenn die Inverse von A folgende Matrix ist:

$$A^{-1} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}.$$

Man sieht dies leicht daran, daß für einen Punkt $(a : b : c) \in \mathbb{P}_K^2$ gilt:

$$F(a, b, c) = F(A^{-1} \cdot A \cdot (a, b, c)^t).$$

Betrachten wir zum Beispiel die ebene projektive Kurve

$$V(x^3 - y^2z)$$

und die Matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in \text{Gl}_3(K),$$

dann ist

$$A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \in \text{Gl}_3(K),$$

und

$$F(A^{-1}(x, y, z)^t) = (x - y)^3 - (y - z)^2 \cdot z = x^3 - 3x^2y + 3xy^2 - y^3 - y^2z + 2yz^2 - z^3.$$

Also ist

$$\Phi_A(V(F)) = V(x^3 - 3x^2y + 3xy^2 - y^3 - y^2z + 2yz^2 - z^3).$$

Qualitativ hat sich nichts verändert (siehe Abbildung 24).

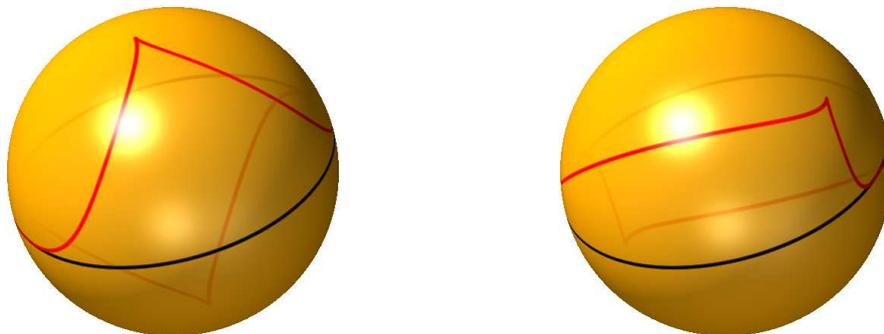


ABBILDUNG 24. $V(x^3 - y^2z)$ und $\Phi_A(V(x^3 - y^2z))$

E) Projektive Quadriken

Definition 3.25 (Projektive Quadriken)

Wir nennen eine ebene projektive Kurve vom Grad 2 auch eine *projektive Quadrik*.

Bemerkung 3.26 (Projektive Quadriken)

Eine projektive Quadrik wird von einem homogenen Polynom der Form

$$F = a \cdot x^2 + b \cdot y^2 + c \cdot z^2 + d \cdot xy + e \cdot xz + f \cdot yz$$

definiert, und dieses kann mit Hilfe von Matrixmultiplikation geschrieben werden als

$$F = (x, y, z) \cdot \begin{pmatrix} a & \frac{d}{2} & \frac{e}{2} \\ \frac{d}{2} & b & \frac{f}{2} \\ \frac{e}{2} & \frac{f}{2} & c \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Dabei ist die Matrix

$$Q = \begin{pmatrix} a & \frac{d}{2} & \frac{e}{2} \\ \frac{d}{2} & b & \frac{f}{2} \\ \frac{e}{2} & \frac{f}{2} & c \end{pmatrix} \in \text{Mat}_3(K)$$

eine *symmetrische* 3×3 -Matrix. Umgekehrt definiert jede symmetrische 3×3 -Matrix auf diese Weise ein homogenes Polynom vom Grad 2. Wenn wir projektive Quadriken studieren wollen, so können wir statt dessen auch symmetrische Matrizen studieren.

Wie wirkt sich eine projektive Koordinatentransformation Φ_A auf eine Quadrik, d.h. auf die definierende Gleichung oder alternativ auf die symmetrische Matrix aus?

Dazu sollen das homogene Polynom F und die symmetrische Matrix Q wie oben dargestellt zueinander in Beziehung stehen, und analog soll das Polynom G zur Matrix $Q' = (A^{-1})^t \cdot Q \cdot A^{-1}$ gehören. Man beachte dabei, daß diese Matrix wieder symmetrisch ist!

Für einen Punkt $P = (x : y : z) \in \mathbb{P}_K^2$ gilt dann:

$$\begin{aligned} P \in V(F) &\iff (x, y, z) \cdot Q \cdot (x, y, z)^t = 0 \\ &\iff (x, y, z) \cdot A^t \cdot (A^{-1})^t \cdot Q \cdot A^{-1} \cdot A \cdot (x, y, z)^t = 0 \\ &\iff ((x, y, z) \cdot A^t) \cdot \left((A^{-1})^t \cdot Q \cdot A^{-1} \right) \cdot A \cdot (x, y, z)^t = 0 \\ &\iff (A \cdot (x, y, z)^t)^t \cdot Q' \cdot (A \cdot (x, y, z)^t) = 0 \\ &\iff \Phi_A(P) \in V(G). \end{aligned}$$

Die zur Quadrik gehörende symmetrische Matrix Q transformiert sich unter der projektiven Koordinatentransformation Φ_A also zur symmetrischen Matrix

$$(A^{-1})^t \cdot Q \cdot A^{-1}.$$

Diese Überlegungen gelten soweit über jedem Körper K . Arbeiten wir über dem Grundkörper \mathbb{R} der reellen Zahlen, dann können wir jede ebene projektive Quadrik in eine besonders schöne Normalform überführen. Dieser Sachverhalt ist als *Hauptachsentransformation* bekannt.

Satz 3.27 (Hauptachsentransformation)

Ist $Q \in \text{Mat}_3(\mathbb{R})$ eine symmetrische 3×3 -Matrix, so existiert eine invertierbare Matrix A mit $A^{-1} = A^t$, so daß

$$A \cdot Q \cdot A^{-1} = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix},$$

wobei $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ die Eigenwerte der Matrix Q sind.

Bemerkung 3.28 (Hauptachsentransformation)

Eine invertierbare Matrix A mit der Eigenschaft $A^{-1} = A^t$ nennt man eine *orthogonale Matrix*. Ihre Spalten bilden eine Orthonormalbasis des \mathbb{R}^3 , d.h. die Spalten stehen paarweise senkrecht aufeinander und haben jeweils die Länge eins. Die Wahl einer solchen Matrix entspricht damit der Wahl eines geeigneten normierten orthogonalen Koordinatensystems.

Der Satz über die Hauptachsentransformation sagt nun, daß wir zu einer gegebenen Quadrik mit Matrix Q , eine Orthonormalbasis von Eigenvektoren der Matrix wählen können, so daß die Gleichung der Quadrik in diesen neuen Koordinaten die Form

$$\lambda_1 \cdot x^2 + \lambda_2 \cdot y^2 + \lambda_3 \cdot z^2 = 0$$

haben wird.

Wenn wir die Forderung bezüglich der Länge der Spaltenvektoren fallen lassen und Transformationen über den komplexen Zahlen \mathbb{C} zulassen, so können wir die Gleichung sogar noch weiter vereinfachen, indem wir die Basisvektoren strecken oder stauchen. Dies geschieht durch Multiplikation von $A \cdot Q \cdot A^t$ mit der Matrix

$$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix} \in \text{Gl}_3(\mathbb{C}),$$

wobei

$$d_i = \begin{cases} 1, & \text{falls } \lambda_i = 0, \\ \sqrt{\lambda_i}, & \text{falls } \lambda_i \neq 0. \end{cases}$$

Setzen wir

$$\delta_i = \begin{cases} 0, & \text{falls } \lambda_i = 0, \\ 1, & \text{falls } \lambda_i \neq 0, \end{cases}$$

so erhalten wir schließlich

$$(D \cdot A) \cdot Q \cdot (D \cdot A)^t = D \cdot A \cdot Q \cdot A^t \cdot D^t = \begin{pmatrix} \delta_1 & 0 & 0 \\ 0 & \delta_2 & 0 \\ 0 & 0 & \delta_3 \end{pmatrix}.$$

Unsere Quadrik wird in den neuen Koordinaten also eine der folgenden Normalformen haben:

$\det(Q)$	Normalform	Kegelschnitt
3	$x^2 + y^2 + z^2 = 0$	Kreis / Ellipse / Parabel / Hyperbel,
2	$x^2 + y^2 = 0$	zwei sich schneidende Geraden,
1	$x^2 = 0$	eine Doppelgerade.

Erlauben wir projektive Koordinatentransformationen über den komplexen Zahlen, so sind Kreise, Ellipsen, Parabeln und Hyperbeln nicht mehr zu unterscheiden. Dies sollte uns nicht verwundern, wenn wir uns die Visualisierungen projektiver Ellipsen, Hyperbeln und Parabeln in Abbildung 25 anschauen.

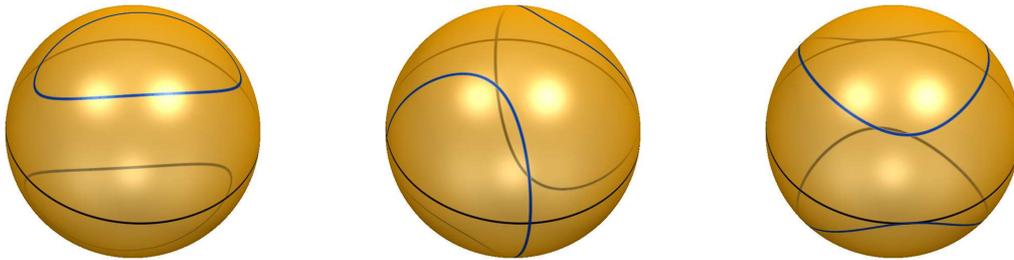


ABBILDUNG 25. Projektive Kegelschnitte: Ellipse, Hyperbel, Parabel

F) Die Boysche Fläche

Unsere Probleme, die projektive Ebene $\mathbb{P}_{\mathbb{R}}^2$ zu visualisieren, rühren daher, daß sie als *Fläche*, d.h. als *zweidimensionales* geometrisches Objekt, nicht im Anschauungsraum \mathbb{R}^3 enthalten ist. Wir haben uns damit beholfen, daß wir die Kugeloberfläche als Modell der projektiven Ebene angesehen haben, indem wir einander gegenüberliegende Punkte der Kugeloberfläche miteinander identifizieren. Das ist für unsere Zwecke die sinnvollste Art, die projektive Ebene graphisch zu darzustellen. Dennoch darf man sich fragen, ob es möglich ist, die projektive Ebene $\mathbb{P}_{\mathbb{R}}^2$ so in den Anschauungsraum einzubetten, daß keine Identifikation mehr nötig ist. Etwas mathematischer ausgedrückt suchen wir eine gute Abbildung

$$\iota : \mathbb{P}_{\mathbb{R}}^2 \longrightarrow \mathbb{A}_{\mathbb{R}}^3.$$

Wie gut sollte ι sein? Da wir algebraische Geometrie betreiben, würden wir uns wünschen, daß ι durch rationale Funktionen gegeben wird, wie wir das bei Parametrisierungen schon kennen gelernt haben; natürlich wünschen wir uns auch, daß die Abbildung injektiv ist; und es wäre schön, wenn die Ableitungen von ι sich gut verhielten, so daß keine höherdimensionalen Analoga von Hoch- und Tiefpunkten, Wendepunkten oder Sattelpunkten vorkommen. Dies alles zusammen ist leider nicht möglich. Es gibt überhaupt keine *sinnvolle* Abbildung von $\mathbb{P}_{\mathbb{R}}^2$ nach $\mathbb{A}_{\mathbb{R}}^3$, die injektiv ist. Schwächen wir diese Bedingung also etwas ab und fordern nur, daß ι *fast injektiv* ist, d.h. die Menge der Punkte, für die ι nicht injektiv ist, ist eine Kurve in der projektiven Ebene $\mathbb{P}_{\mathbb{R}}^2$. Dann läßt sich unser Ziel in der Tat realisieren, und

man nennt eine solche Abbildung ι eine *Immersion* der projektiven Ebene in den Anschauungsraum.

Die projektive Ebene $\mathbb{P}_{\mathbb{R}}^2$ kann so in den affinen dreidimensionalen Raum $\mathbb{A}_{\mathbb{R}}^3$ eingebettet werden, daß ihr Bild eine Fläche mit Selbstdurchdringung ist. Man nennt die Fläche dann eine Boysche Fläche.

Unser Ziel ist es nun, eine solche Abbildung und die Gleichung ihres Bildes anzugeben. Dazu wollen wir einige Vorüberlegungen anstellen.

Wenn die Komponentenfunktionen von ι durch rationale Funktionen $\frac{F}{G}$ gegeben sein sollen, dann muß für $(x, y, z) \in \mathbb{R}^3$ und für $0 \neq \lambda \in \mathbb{R}$ notwendigerweise

$$\frac{F}{G}(x, y, z) = \frac{F}{G}(\lambda \cdot x, \lambda \cdot y, \lambda \cdot z)$$

gelten. Das legt zunächst nahe, daß die Polynome F und G homogen sind, und wir fordern zudem, daß sie den gleichen Grad haben. Damit erhalten wir dann

$$\frac{F(\lambda \cdot x, \lambda \cdot y, \lambda \cdot z)}{G(\lambda \cdot x, \lambda \cdot y, \lambda \cdot z)} = \frac{\lambda^{\deg(F)} \cdot F(x, y, z)}{\lambda^{\deg(G)} \cdot G(x, y, z)} = \frac{F(x, y, z)}{G(x, y, z)},$$

d.h. der Wert der rationalen Funktion ist für jedes $\lambda \neq 0$ gleich. Damit induziert sie eine wohldefinierte Funktion auf der projektiven Ebene

$$\mathbb{P}_{\mathbb{R}}^2 \longrightarrow \mathbb{R} : (x : y : z) \mapsto \frac{F(x, y, z)}{G(x, y, z)}.$$

Die Komponentenfunktionen von ι sollen also Brüche von homogenen Polynomen des gleichen Grades sein. In unserem Fall werden es homogene Polynome vom Grad vier sein.

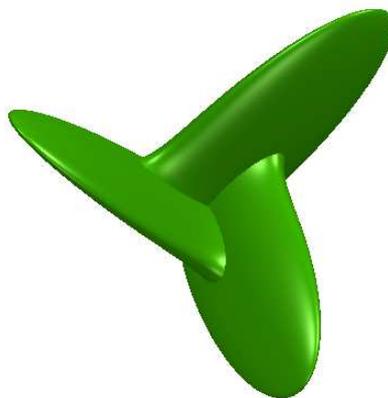


ABBILDUNG 26. Die Boysche Fläche aus Satz 3.29

Satz 3.29 (Boysche Fläche)

Die Abbildung $\iota : \mathbb{P}_{\mathbb{R}}^2 \longrightarrow \mathbb{A}_{\mathbb{R}}^3$ mit

$$\iota(x : y : z) = \begin{pmatrix} \frac{\sqrt{2} \cdot (x^2 + y^2) \cdot (x^2 - y^2 + \sqrt{2} \cdot xz)}{3 \cdot (x^2 + y^2 + z^2) \cdot (x^2 + y^2) - 3 \cdot \sqrt{2} \cdot y \cdot z \cdot (3x^2 - y^2)} \\ \frac{\sqrt{2} \cdot (x^2 + y^2) \cdot (2 \cdot x \cdot y - \sqrt{2} \cdot y \cdot z)}{3 \cdot (x^2 + y^2 + z^2) \cdot (x^2 + y^2) - 3 \cdot \sqrt{2} \cdot y \cdot z \cdot (3x^2 - y^2)} \\ \frac{(x^2 + y^2)^2}{(x^2 + y^2 + z^2) \cdot (x^2 + y^2) - \sqrt{2} \cdot y \cdot z \cdot (3x^2 - y^2)} \end{pmatrix}$$

ist eine stetig differenzierbare Immersion, und es gilt

$$\text{Im}(\iota) = V(F)$$

mit

$$\begin{aligned} F = & 64 \cdot (1 - z)^3 \cdot z^3 - 48 \cdot (1 - z)^2 \cdot z^2 \cdot (3 \cdot x^2 + 3 \cdot y^2 + 2 \cdot z^2) \\ & + 12 \cdot (1 - z) \cdot z \cdot (27 \cdot (x^2 + y^2)^2 - 24 \cdot z^2 \cdot (x^2 + y^2) + \\ & \quad 36 \cdot \sqrt{2} \cdot y \cdot z \cdot (y^2 - 3 \cdot x^2) + 4 \cdot z^4) \\ & + (9 \cdot x^2 + 9 \cdot y^2 - 2 \cdot z^2) \cdot (-81 \cdot (x^2 + y^2)^2 - \\ & \quad 72 \cdot z^2 \cdot (x^2 + y^2) + 108 \cdot \sqrt{2} \cdot x \cdot z \cdot (x^2 - 3 \cdot y^2) + 4 \cdot z^4). \end{aligned}$$

Das Bild von ι ist also eine Fläche vom Grad sechs, eine Boysche Fläche.

Bemerkung 3.30

Man kann leicht durch Einsetzen in SINGULAR überprüfen, daß das Bild von ι in der Fläche $V(F)$ enthalten ist. Aber wir wissen bereits, daß das Bild einer solchen Abbildung im allgemeinen nicht abgeschlossen ist, d.h. daß nicht unbedingt erwartet werden kann, daß jeder Punkt von $V(F)$ auch wirklich im Bild von ι liegt. Das Erstaunliche an ι ist, daß dies in der Tat der Fall ist; das Bild von ι ist die ganze Fläche $V(F)$. Für einen Beweis dieser Tatsache sowie für eine Darstellung von ι mit Hilfe trigonometrischer Funktionen mittels Kugelkoordinaten, verweisen wir auf [Apé87, Kap. 2.4, Prop. 2]. Im Prinzip kann man die Gleichung der Fläche mit Hilfe von Elimination aus der Abbildungsvorschrift für ι berechnen. Die Rechnungen in SINGULAR werden aber recht komplex. Die Fläche ist dargestellt in Abbildung 26, und man kann dort die Selbstdurchdringung der Fläche sehr gut erkennen. Das Bild wurde mit Surfex erzeugt.

G) Der projektive Raum**Bemerkung 3.31** (Der projektive Raum $\mathbb{P}_{\mathbb{K}}^n$)

Analog zur projektiven Ebene $\mathbb{P}_{\mathbb{K}}^2$ kann man den n -dimensionalen projektiven Raum $\mathbb{P}_{\mathbb{K}}^n$ als die Menge der Ursprungsgeraden im \mathbb{K}^{n+1} definieren und man führt analog projektive Koordinaten

$$(x_0 : x_1 : \dots : x_n) = \{\lambda \cdot (x_0, x_1, \dots, x_n) \mid \lambda \in \mathbb{K}\}$$

ein. Dann kann man zu einem gegebenen homogenen Polynom $F \in \mathbb{K}[x_0, x_1, \dots, x_n]$ die *projektive Hyperfläche*

$$V(F) = \{(x_0 : x_1 : \dots : x_n) \in \mathbb{P}_{\mathbb{K}}^n \mid F(x_0, x_1, \dots, x_n) = 0\}$$

definieren.

H) Aufgaben

Aufgabe 3.32

Welche der folgenden Punkte der projektiven Ebene stimmen überein?

- a. $P_1 = (2 : 3 : 1)$
- b. $P_2 = (-1 : 1 : 1)$
- c. $P_3 = (3 : -3 : 3)$
- d. $P_4 = (4 : 1 : 1)$
- e. $P_5 = (6 : 9 : 3)$
- f. $P_6 = (-4 : -6 : -2)$

Aufgabe 3.33

Beweisen Sie, daß man die Homogenisierung eines Polynoms $f \in \mathbb{K}[x, y]$ dadurch erhält, daß man alle Monome $x^i y^j$ von f durch $x^i y^j z^{\deg(f) - i - j}$ ersetzt.

Aufgabe 3.34

Berechnen Sie die Schnittpunkte der projektiven Kurve $V(x^3 z + 2xy z^2 - 3xz^3 + x^4 - x^3 y)$ mit der unendlich fernen Geraden $V(z)$.

Aufgabe 3.35

Visualisieren Sie mit **Surfex** ein Modell der projektiven Ebene mit den drei Koordinatenachsen $V(x)$, $V(y)$ und $V(z)$.

Aufgabe 3.36

Bilden Sie den projektiven Abschluß von drei parallelen affinen Geraden und visualisieren Sie diese dann mit **Surfex**.

Aufgabe 3.37

Reproduzieren Sie das Bild in Abbildung 27 mit **Surfex**. Es vereinigt die affine und die projektive Ansicht einer Geraden.

Aufgabe 3.38

Visualisieren Sie die ebene projektive Kurve $V(x^2 z - y^3)$ mit **Surfex**.

Aufgabe 3.39

Homogenisieren Sie die folgenden Polynome und visualisieren Sie die zugehörigen ebenen affinen und projektiven Kurven mit **Surf** bzw. mit **Surfex**:

- a. $x^2 - y^3$.

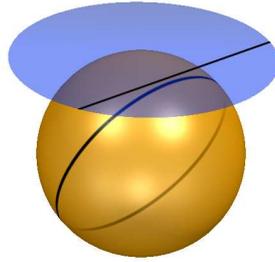


ABBILDUNG 27. Affine und projektive Ansicht einer Geraden

- b. $xy - 1$.
- c. $x^2 - y^4$.
- d. $y^2 - x \cdot (x - 1) \cdot (x - 2)$.

Aufgabe 3.40

Dehomogenisieren Sie die folgenden homogenen Polynome und visualisieren Sie die zugehörigen ebenen affinen und projektiven Kurven mit **Surf** bzw. mit **Surfex** :

- a. $x^2z - 3xyz + y^3$.
- b. $xz + yz + z^2$.

Aufgabe 3.41

Berechnen Sie das Bild des projektiven Abschlusses des Einheitskreises in der affinen Ebene unter der projektiven Koordinatentransformation, die durch die Matrix

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

gegeben wird.

Aufgabe 3.42

Bestimmen Sie die Normalform der Quadrik $V(5x^2 + 4xy + 4xz + 2y^2 - 8yz + 2z^2)$ über \mathbb{C} und berechnen Sie die Matrix A einer Koordinatentransformation, die die Quadrik auf die gewünschte Normalform bringt.

4 DER SATZ VON BÉZOUT

(VON THOMAS MARKWIG)

Wir haben die projektive Ebene eingeführt, weil wir der parallelen Geraden überdrüssig waren, weil das *Schnittverhalten* von Geraden in der projektiven Ebene weit besser ist als in der affinen. In diesem Kapitel werden wir nun sehen, daß das nicht nur auf Geraden zutrifft. In der projektiven Ebene existiert für allgemeine Kurven eine vernünftige Schnitttheorie. Dieser Aussage, dem Satz von Bézout, wollen wir uns schrittweise nähern.

A) Nullstellen und ihre Vielfachheit

Dazu betrachten wir zunächst einmal Polynome in einer Veränderlichen und deren Nullstellen.

Satz 4.1

Ist $f \in K[x]$ ein Polynom und ist $\alpha \in K$ eine Nullstelle von f , so hat f die Form

$$f = (x - \alpha) \cdot g$$

für ein geeignetes Polynom $g \in K[x]$. Wir sagen, daß wir die Nullstelle α von f als *Linearfaktor* abspalten können.

Beweisidee: Im Polynomring kann man wie in den ganzen Zahlen Division mit Rest durchführen (vgl. Aufgabe 4.26). Dividieren wir f durch $x - \alpha$ mit Rest, so schreibt sich f als

$$f = (x - \alpha) \cdot g + r \tag{4}$$

für Polynome g und r in $K[x]$, wobei der Grad von r echt kleiner als der Grad von $x - \alpha$ ist. Letzteres bedeutet aber, daß r ein konstantes Polynom ist. Lösen wir die Gleichung (4) nach r auf, so erhalten wir

$$r = f - (x - \alpha) \cdot g.$$

Setzen wir in diese Gleichung auf beiden Seiten den Wert α ein, so bleibt auf der linken Seite r stehen, da r ein konstantes Polynom ist. Wir erhalten damit

$$r = f(\alpha) - (\alpha - \alpha) \cdot g(\alpha) = 0,$$

d.h. das konstante Polynom r ist das Nullpolynom und wir haben insgesamt $f = (x - \alpha) \cdot g$. □

Bemerkung 4.2

Wie viele Nullstellen haben die folgenden Polynome?

- a. $f_1 = x^2 - 1$,
- b. $f_2 = x^3 - x$,
- c. $f_3 = (x - 2) \cdot (x - 1) \cdot x \cdot (x + 1) \cdot (x + 2)$,

d. $f_4 = x^2 - 2x + 1,$

e. $f_5 = x^2 + 1?$

Das Polynom $f_1 = (x-1) \cdot (x+1)$ hat die beiden Nullstellen 1 und -1 , das Polynom $f_2 = x \cdot (x-1) \cdot (x+1)$ die drei Nullstellen $-1, 0$ und 1 , und das Polynom f_3 hat die fünf Nullstellen $-2, -1, 0, 1$ und 2 . Die Zahl der Nullstellen stimmt in diesen Beispielen mit dem Grad des Polynoms überein.

Dagegen hat das Polynom $f_4 = (x-1)^2$ nur die eine Nullstelle eins. Spalten wir sie als Linearfaktor ab, so bleibt ein Polynom übrig, das die gleiche Nullstelle hat. Der Linearfaktor zur Nullstelle 1 kommt doppelt in der Primfaktorzerlegung von f vor. Wir sagen deshalb auch, daß 1 eine *Nullstelle der Vielfachheit 2* ist. Zählen wir die Nullstellen von f_4 mit ihrer Vielfachheit, so ist das Ergebnis wieder der Grad des Polynoms. Dies gibt Anlaß zur Vermutung, daß der Grad eines Polynoms mit der Anzahl seiner Nullstellen übereinstimmt, solange man sie mit ihrer Vielfachheit zählt. Dabei definieren wir die Vielfachheit von f allgemein wie folgt:

Eine Nullstelle a eines Polynoms f hat die Vielfachheit k , wenn $(x-a)^k$ die höchste Potenz des Linearfaktors $x-a$ ist, die das Polynom f teilt. D.h. $f = (x-a)^k \cdot g$ mit $g(a) \neq 0$.

Das Polynom f_5 macht unsere Hoffnung dann aber zunichte, denn f_5 hat in \mathbb{R} überhaupt keine Nullstelle! Das ist eindeutig zu wenig. Betrachten wir f_5 aber als Polynom in $\mathbb{C}[x]$, dann hat $f_5 = (x-i) \cdot (x+i)$ die beiden Nullstellen i und $-i$, wobei i die imaginäre Einheit bezeichnet. Unsere Vermutung ist also wieder erfüllt, und für Polynome in $\mathbb{C}[x]$ ist dies in der Tat stets der Fall. Das ist die Aussage des *Hauptsatzes der Algebra* (vgl. Satz 1.26), und man nennt den Körper der komplexen Zahlen deshalb auch *algebraisch abgeschlossen*. Diese Eigenschaft ist der wesentliche Grund, weshalb die komplexen Zahlen für die algebraische Geometrie weit besser geeignet sind, als die reellen Zahlen.

Die Zahl der Nullstellen eines nicht-konstanten Polynoms $f \in \mathbb{C}[x]$ mit komplexen Koeffizienten ist der Grad $\deg(f)$ des Polynoms, wenn man die Nullstellen mit ihrer Vielfachheit zählt.

B) Schnittpunkte und ihre Vielfachheit

Wir wollen diese Aussage nun am Beispiel des Polynoms

$$f = x^4 - 4 \cdot x^2 = x^2 \cdot (x-2) \cdot (x+2)$$

geometrisch interpretieren.

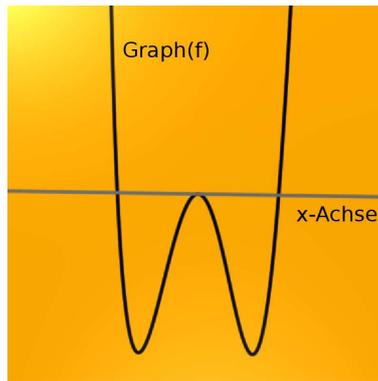


ABBILDUNG 28. Nullstellen des Polynoms $f = x^4 - 4x^2$.

Eine Nullstelle ist die x -Koordinate eines Schnittpunktes des Graphen von f mit der x -Achse (vgl. Abbildung 28). Daß eine Nullstelle doppelte Vielfachheit hat, wie die Nullstelle 0 in unserem Beispiel, bedeutet, daß die x -Achse im zugehörigen Punkt des Graphen die Tangente an den Graphen ist (vgl. Bemerkung 4.4). In diesem Sinne treffen wir eine Aussage über die Anzahl der Schnittpunkte der beiden algebraischen Kurven

$$\text{Graph}(f) = V(\mathbf{y} - x^4 + 4x^2)$$

und

$$V(\mathbf{y}) = x - \text{Achse},$$

und die Zahl der Schnittpunkte ist gleich

$$4 = \deg(\mathbf{y} - x^4 + 4x^2) \cdot \deg(\mathbf{y}),$$

wenn wir sie mit der richtigen Vielfachheit zählen, d.h. wenn wir den tangentialen Schnittpunkt doppelt zählen.

Sinnvollerweise sollte man diese Rechnung im Projektiven durchführen, indem man die beiden Gleichungen homogenisiert. Das liefert aber keinen weiteren Schnittpunkt, so daß die Aussage korrekt bleibt.

Beispiel 4.3

Schauen wir uns die Quadriken

$$C_t = V(x^2 + t \cdot y^2 - z^2) \subset \mathbb{P}_{\mathbb{R}}^2$$

und

$$C' = V(4xy - z^2) \subset \mathbb{P}_{\mathbb{R}}^2$$

an, wobei wir den Parameter t im Intervall $[1, 4]$ wählen. Um die Schnittpunkte von C_t und C' zu berechnen, lösen wir die Gleichung $4xy - z^2 = 0$ nach z^2 auf und setzen sie in $x^2 + t \cdot y^2 - z^2 = 0$ ein. Wir erhalten die Gleichung

$$x^2 + t \cdot y^2 - 4xy = 0,$$

oder alternativ

$$(x - 2y)^2 = (4 - t) \cdot y^2.$$

Durch Wurzelziehen auf beiden Seiten erhalten wir die zwei Lösungen

$$x = (2 \pm \sqrt{4-t}) \cdot y.$$

Setzen wir diese in die Gleichung $4xy - z^2 = 0$ ein, so erhalten wir

$$z^2 = (8 \pm 4 \cdot \sqrt{4-t}) \cdot y^2,$$

und Wurzelziehen auf beiden Seiten liefert dann die vier Lösungen

$$z = \pm \sqrt{8 \pm 4\sqrt{4-t}} \cdot y.$$

Um die projektiven Koordinaten der vier Schnittpunkte zu bestimmen, können wir $y = 1$ wählen und erhalten als Schnittpunkte somit

$$P_1 = \left(2 - \sqrt{4-t} : 1 : \sqrt{8 - 4 \cdot \sqrt{4-t}} \right),$$

$$P_2 = \left(2 + \sqrt{4-t} : 1 : \sqrt{8 + 4 \cdot \sqrt{4-t}} \right),$$

$$P_3 = \left(2 - \sqrt{4-t} : 1 : -\sqrt{8 - 4 \cdot \sqrt{4-t}} \right),$$

$$P_4 = \left(2 + \sqrt{4-t} : 1 : -\sqrt{8 + 4 \cdot \sqrt{4-t}} \right).$$

Verschieden sind die Punkte aber nur für $t < 4$. Im Fall $t = 4$ fallen die Punkte P_1 und P_2 zusammen sowie die Punkte P_3 und P_4 . Wir haben dann also nur zwei Schnittpunkte. In diesem Fall stimmen die Tangenten an C_4 und C' in P_1 aber überein, und gleiches gilt in P_3 . Die gemeinsame Tangente an C_4 und C' in P_1 ist gegeben durch $V(4x + 8y - 16z)$. Man sollte die Schnittpunkte P_1 und P_3 von C_4 und C' deshalb mit doppelter Vielfachheit zählen. (Vgl. Abbildung 29.)

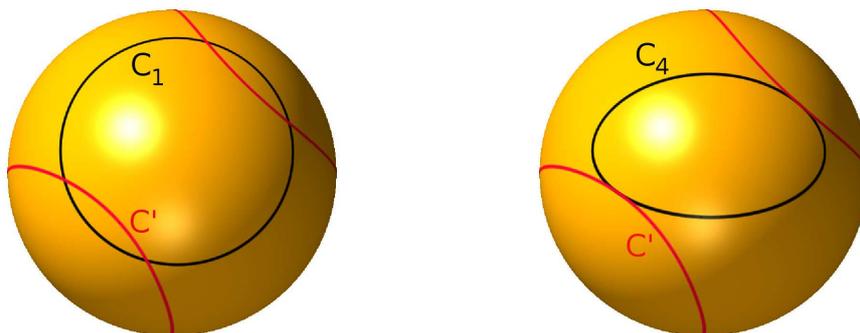


ABBILDUNG 29. $C_1 \cap C'$ und $C_4 \cap C'$

Unter dieser Prämisse erhalten wir wieder, daß die Anzahl der Schnittpunkte mit Vielfachheit gezählt gleich dem Produkt der Grade der definierenden Polynome ist. Dies ist kein Zufall – zumindest nicht, wenn wir den Grundkörper \mathbb{R} durch den Körper \mathbb{C} ersetzen!

Bemerkung 4.4 (Tangenten)

Wie bestimmt man die Tangente an eine ebene projektive Kurve $V(F)$? Dazu macht man sich zunutze, daß man statt der projektiven Kurve auch ihren Kegel

$$C(F) = \{(x, y, z) \in \mathbb{A}_K^3 \mid F(x, y, z) = 0\} \subset \mathbb{A}_K^3$$

im affinen Raum \mathbb{A}_K^3 betrachten kann. Dies ist eine Hyperfläche und der *Gradient* des Polynoms F in einem Punkt (a, b, c) ist der Normalenvektor der *Tangentialebene* an $C(F)$ im Punkt (a, b, c) . Diese Ebene ist eine Ursprungsebene und definiert mithin eine Gerade in der projektiven Ebene, die *Tangente* an $V(F)$ im Punkt $(a : b : c)$. D.h. die Tangente hat die Gleichung

$$\frac{\partial F}{\partial x}(a : b : c) \cdot x + \frac{\partial F}{\partial y}(a : b : c) \cdot y + \frac{\partial F}{\partial z}(a : b : c) \cdot z = 0.$$

Das angegebene Verfahren funktioniert natürlich nur, wenn der Gradient von F im Punkt $(a : b : c)$ nicht $(0 : 0 : 0)$ ist! Ansonsten ist der Begriff der Tangente in $(a : b : c)$ nicht definiert und wir nennen den Punkt $(a : b : c)$ einen *singulären Punkt* von $V(F)$ (siehe Kapitel 5).

Im obigen Beispiel war die Gleichung $F = 4xy - z^2$ gegeben, und wir wollen die Tangente an $V(F)$ im Punkte $P = (2 : 1 : 8) \in V(F)$ bestimmen. Der Gradient von F ist dann

$$\left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z} \right) = (4y, 4x, -2z).$$

Werten wir ihn am Punkt $(2, 1, 8)$ aus, so erhalten wir den Punkt $(4, 8, -16)$ und damit die Tangentialgleichung

$$4x + 8y - 16z = 0.$$

C) Der Satz von Bézout in der Ebene

Wenn wir die *Vielfachheit*, mit der sich zwei ebene projektive Kurven $V(F)$ und $V(G)$ in einem Punkt P schneiden mit $\text{mult}_P(F \cap G)$ bezeichnen, so berechnet sich die mit der Vielfachheit gewichtete Anzahl der Schnittpunkte von $V(F)$ und $V(G)$ aus den Graden der Polynome F und G . Dabei sollte die Vielfachheit eines Schnittpunktes eins sein, wenn die beiden Kurven in dem Schnittpunkt verschiedene Tangenten haben, und sonst sollte sie größer als eins sein.

Natürlich ist es wichtig, daß die Kurven $V(F)$ und $V(G)$ keine gemeinsame Komponente haben, da die Anzahl der Schnittpunkte sonst nicht endlich wäre. Algebraisch bedeutet dies, daß die Polynome F und G keinen gemeinsamen Teiler besitzen.

Satz 4.5 (Satz von Bézout über \mathbb{C})

Sind $F, G \in \mathbb{C}[x, y, z]$ nicht-konstante homogene Polynome, die keinen gemeinsamen Teiler haben, so ist die Anzahl der mit Vielfachheit gezählten Schnittpunkte von $V(F)$ und $V(G)$ in $\mathbb{P}_{\mathbb{C}}^2$ das Produkt der Grade von F und G , d.h.

$$\sum_{P \in V(F) \cap V(G)} \text{mult}_P(F \cap G) = \deg(F) \cdot \deg(G).$$

Bemerkung 4.6

Für zwei verschiedene projektive Geraden sagt der Satz von Bézout aus, daß sie sich in genau einem Punkt schneiden!

Für die Gleichheit im Satz von Bézout ist es wesentlich, daß in den komplexen Zahlen der *Hauptsatz der Algebra* gilt, d.h. daß jedes nicht-konstante Polynom in einer Veränderlichen auch eine Nullstelle besitzt. Über den reellen Zahlen erhält man nur eine Ungleichung, die für viele Anwendungen aber bereits hinreichend ist (siehe etwa den Beweis des Satzes von Pappos 6.7). Die folgende Version des Satzes von Bézout über den reellen Zahlen folgt unmittelbar aus Satz 4.5, da die Nullstellenmengen von F und G in $\mathbb{P}_{\mathbb{R}}^2$ als Teilmengen der Nullstellenmengen von F und G in $\mathbb{P}_{\mathbb{C}}^2$ aufgefaßt werden können, und da dann jeder Schnittpunkt in $\mathbb{P}_{\mathbb{R}}^2$ auch ein Schnittpunkt in $\mathbb{P}_{\mathbb{C}}^2$ ist.

Korollar 4.7 (Satz von Bézout über \mathbb{R})

Sind $F, G \in \mathbb{R}[x, y, z]$ nicht-konstante homogene Polynome, die keinen gemeinsamen Teiler haben, so besitzen $V(F)$ und $V(G)$ in $\mathbb{P}_{\mathbb{R}}^2$ höchstens $\deg(F) \cdot \deg(G)$ Schnittpunkte.

D) Schnittvielfachheit mittels Resultanten

Wenn wir Satz 4.5 beweisen oder auch nur wirklich verstehen wollen, müssen wir den Begriff der *Vielfachheit eines Schnittpunktes* exakter fassen. Sonst können wir nicht einmal wirklich Beispiele rechnen. Wir geben im Folgenden eine Definition mit Hilfe von Resultanten. Es ist auf den ersten Blick vollkommen unklar, weshalb dies eine sinnvolle Definition sein sollte. Wir werden aber in Beispielen sehen, daß es eine gute Wahl ist.

Prinzip: Die Vielfachheit, mit welcher sich zwei Kurven in einem Punkt schneiden, sollte nur vom Verhalten der Kurven in einer kleinen Umgebung des Punktes bestimmt werden. Wie die Kurven global, d.h. in den übrigen Punkten, aussehen, sollte dafür ohne Belang sein!

Wir können deshalb zunächst die Schnittvielfachheit zweier affiner Kurven im Ursprung definieren.

Definition 4.8 (Resultante und Schnittvielfachheit)

Sind $f = \sum_{i=0}^m a_i \cdot y^i, g = \sum_{j=0}^n b_j \cdot y^j \in \mathbb{C}[x, y]$ mit $a_i, b_j \in \mathbb{C}[x]$ zwei Polynome in den Veränderlichen x und y , die nicht nur von x abhängen, so nennen wir die Determinante

$$\text{Res}_{f,g} = \det(S_{f,g}) \in \mathbb{C}[x]$$

der $(n + m) \times (n + m)$ -Matrix

$$S_{f,g} = \begin{pmatrix} a_0 & \dots & \dots & \dots & a_m & & \\ & \ddots & & & & \ddots & \\ & & a_0 & \dots & \dots & \dots & a_m \\ b_0 & \dots & \dots & b_n & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & b_0 & \dots & \dots & b_n \end{pmatrix}$$

die *Resultante* von f und g . Die Matrix hat n Zeilen mit Einträgen a_i und m Zeilen mit Einträgen b_j , und sie wird die *Sylvestermatrix* von f und g genannt. Die Resultante $R_{f,g}$ ist ein Polynom in der Veränderlichen x .

Ferner definieren wir die *Schnittvielfachheit* der ebenen affinen Kurven $V(f)$ und $V(g)$ im Punkt $p = (0, 0)$ als die Ordnung

$$\text{mult}_p(f \cap g) = \text{ord}_x(\text{Res}_{f,g})$$

der Resultante von f und g als Polynom in x . Dabei ist die *Ordnung* eines Polynoms der *minimale* Grad eines Monoms des Polynoms. Wir nennen $\text{mult}_p(f \cap g)$ auch die *Vielfachheit* von p als Schnittpunkt von $V(f) \cap V(g)$.

Bemerkung 4.9

Da man die Sylvestermatrix $S_{f,g}$ durch Zeilenvertauschungen in die Sylvestermatrix $S_{g,f}$ überführen kann und dies die Determinante bestenfalls um das Vorzeichen ändert, erhalten wir aus der Definition unmittelbar, daß

$$\text{mult}_p(f \cap g) = \text{mult}_p(g \cap f)$$

gilt. Würde dies nicht gelten, dann wäre unsere Definition offensichtlich unsinnig.

Beispiel 4.10

a. Sind $f = y - x^4 + 4x^2$ und $g = y$, dann hat die Resultante

$$\text{Res}_{f,g} = \det \begin{pmatrix} (-x^4 + 4x^2) & 1 \\ 0 & 1 \end{pmatrix} = -x^4 + 4x^2$$

von f und g die Ordnung 2. Dies entspricht der doppelten Nullstelle 0 in Abbildung 28.

b. Sind $f = y - x^2$ und $g = y - x^4$, dann hat die Resultante

$$\text{Res}_{f,g} = \det \begin{pmatrix} -x^2 & 1 \\ -x^4 & 1 \end{pmatrix} = x^4 - x^2$$

von f und g ebenfalls die Ordnung 2. Dies trägt dem Umstand Rechnung, daß die beiden Kurven sich im Ursprung tangential berühren (vgl. Abbildung 30).

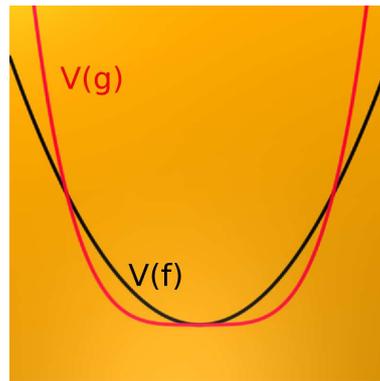


ABBILDUNG 30. Tangentialer Schnitt im Ursprung

c. Sind $f = x^3 - y^2$ und $g = x + y$, dann hat die Resultante

$$\text{Res}_{f,g} = \det \begin{pmatrix} x^3 & 0 & -1 \\ x & 1 & 0 \\ 0 & x & 1 \end{pmatrix} = x^3 - x^2$$

von f und g wiederum die Ordnung 2. Dies trägt dem Umstand Rechnung, daß die von f definierte Kurve im Ursprung singulär ist (vgl. Abbildung 31).

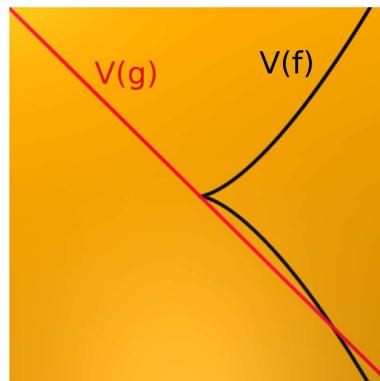


ABBILDUNG 31. Nicht-tangentialer Schnitt eines singulären Punktes

d. Sind $f = x^3 - y^2$ und $g = y$, dann hat die Resultante

$$\text{Res}_{f,g} = \det \begin{pmatrix} x^3 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = x^3$$

von f und g diesmal die Ordnung 3. Dies trägt dem Umstand Rechnung, daß die von f definierte Kurve im Ursprung singulär ist und daß sie von der durch g definierten Geraden zusätzlich tangential geschnitten wird (vgl. Abbildung 32).

Bemerkung 4.11

Man kann die Berechnung einer Resultante natürlich auch mit Hilfe von SINGULAR durchführen.

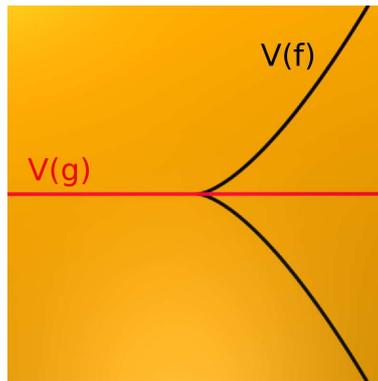


ABBILDUNG 32. Tangentialer Schnitt eines singulären Punktes

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0,(x,y),ds;
> poly f=x^3-y^2;
> poly g=x+y;
> resultant(f,g,y);
-x2+x3
> ord(resultant(f,g,y));
2

```

In diesem Beispiel haben wir die Resultante von f und g sowie die Ordnung der Resultante ausgerechnet. Man beachte dabei, daß in der Ringdefinition `ring r=0,(x,y),ds`; am Ende diesmal `ds` und nicht etwa `lp` oder `dp` steht. Das `s` sorgt dafür, daß die Monome mit dem kleinsten Grad nach vorne sortiert werden, d.h. wir erhalten $-x^2 + x^3$ statt $x^3 - x^2$. Dies ist nur wichtig, wenn wir die Funktion `ord` verwenden wollen!

Definition 4.12 (Schnittvielfachheit)

Sind F und G zwei nicht-konstante homogene Polynome in $\mathbb{C}[x, y, z]$, die keine gemeinsamen Teiler haben, und ist $P \in V(F) \cap V(G)$ ein Punkt im Schnitt der beiden zugehörigen Kurven, so wählen wir eine invertierbare Matrix $A \in GL_3(\mathbb{C})$ derart, daß die zugehörige projektive Koordinatentransformation den Punkt P auf den Punkt $(0 : 0 : 1)$ abbildet, d.h.

$$\Phi_A(P) = (0 : 0 : 1),$$

und derart, daß in den transformierten Polynomen

$$F' = F(A^{-1} \cdot (x, y, z)^t) \quad \text{und} \quad G' = G(A^{-1} \cdot (x, y, z)^t)$$

die Variable y noch vorkommt.⁵ Dann dehomogenisieren wir diese beiden Polynome zu

$$f = F'(x, y, 1) \quad \text{und} \quad g = G'(x, y, 1).$$

Die *Vielfachheit* von P als Schnittpunkt von $V(F)$ mit $V(G)$ definieren wir dann als die Ordnung

$$\text{mult}_P(F \cap G) = \text{mult}_{(0,0)}(f \cap g) = \text{ord}_x(\text{Res}_{f,g})$$

der Resultante von f und g als Polynom in x . Wir nennen $\text{mult}_P(F \cap G)$ auch die *Schnittvielfachheit* von $V(F)$ und $V(G)$ in P .

Bemerkung 4.13

Damit diese Definition sinnvoll ist, muß man natürlich zeigen, daß eine solche Transformation immer möglich ist und daß sie nicht von der Wahl der Matrix A abhängt. Das wollen wir hier nicht tun.

E) Der Beweis des Satzes von Bézout

Wir wollen den Satz von Bézout nun in dem Spezialfall beweisen, daß $V(G)$ eine Gerade ist.

Beweis des Satzes von Bézout 4.5 für eine Gerade $V(G)$: In der Definition der Vielfachheit von Schnittpunkten haben wir bereits verwendet, daß diese invariant unter projektiven Koordinatentransformationen ist. Selbiges trifft auf den Grad von F und G zu. Wir können also eine Koordinatentransformation durchführen, die die Gerade $V(G)$ auf $V(y)$ abbildet und zudem sicherstellt, daß kein Schnittpunkt von $V(F)$ und $V(G)$ auf den Punkt $(1 : 0 : 0)$ auf der unendlich fernen Geraden abgebildet wird. D.h. wir können ohne Einschränkung annehmen, daß $G = y$ und $(1 : 0 : 0) \notin V(F) \cap V(G)$.

Wegen des Hauptsatzes der Algebra zerfällt das Polynom

$$a_0 = F(x, 0, 1) \in \mathbb{C}[x]$$

in Linearfaktoren, d.h. es hat die Form

$$a_0 = d \cdot (x - c_1)^{k_1} \cdots (x - c_l)^{k_l}$$

für paarweise verschiedene komplexe Zahlen $c_1, \dots, c_l \in \mathbb{C}$, positive ganze Zahlen $k_1, \dots, k_l \in \mathbb{Z}_{>0}$ und eine Konstante $0 \neq d \in \mathbb{C}$.

Liegt ein Punkt $P = (x : y : 1) \in V(F) \cap V(G) = V(F) \cap V(y)$ und hat die Dehomogenisierung von $F(x, y, 1)$ die Gestalt

$$F(x, y, 1) = \sum_{i=0}^m a_i \cdot y^i \in \mathbb{C}[x, y]$$

⁵Geometrisch bedeutet die Bedingung, daß y in dem Polynom F' noch vorkommt, daß $V(F')$ keine Vereinigung von Geraden ist, die alle $V(x)$ im Punkt $(0 : 1 : 0)$ auf der unendlich fernen Geraden schneiden, oder alternativ, daß die Dehomogenisierung $F'(x, y, 1)$ keine Vereinigung von Geraden definiert, die parallel zur y -Achse sind.

mit $\mathbf{a}_i \in \mathbb{C}[x]$, so gilt $\mathbf{y} = \mathbf{0}$ und

$$\mathbf{a}_0(x) = F(x, 0, 1) = F(P) = 0.$$

Die Zahl x muß also eines der c_i sein, d.h. $P = (c_i : 0 : 1)$.

Wir führen nun die Koordinatentransformation mit der Matrix

$$A = \begin{pmatrix} 1 & 0 & -c_i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

durch. Diese bildet den Punkt P auf den Punkt $(0 : 0 : 1)$ ab, sie läßt das Polynom $G = \mathbf{y}$ unverändert und bildet F auf das Polynom $F(x + c_i z, \mathbf{y}, z)$ ab, dessen Dehomogenisierung durch

$$f = F(x + c_i, \mathbf{y}, 1) = \sum_{i=0}^m \mathbf{a}_i(x + c_i) \cdot \mathbf{y}^i$$

gegeben ist. Die Vielfachheit von $V(F)$ und $V(G)$ im Punkt P errechnet sich nun als die x -Ordnung der Resultante

$$\text{Res}_{f,\mathbf{y}} = \det \begin{pmatrix} \mathbf{a}_0(x + c_i) & \mathbf{a}_1(x + c_i) & \dots & \mathbf{a}_m(x + c_i) \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = \mathbf{a}_0(x + c_i)$$

von f und \mathbf{y} , d.h. die x -Ordnung von

$$\text{Res}_{f,\mathbf{y}} = \mathbf{d} \cdot x^{k_i} \cdot \prod_{j \neq i} (x + c_i - c_j)^{k_j}.$$

Diese Ordnung ist aber gerade k_i , da die c_j paarweise verschieden sind.

Wir erhalten also

$$\sum_{P \in V(F) \cap V(G)} \text{mult}_P(F \cap G) = k_1 + \dots + k_l = \deg(F(x, 0, 1)) = \deg(F),$$

wobei die letzte Gleichheit der Grade durch $(1 : 0 : 0) \notin V(F)$ sichergestellt wird. \square

F) Alternative Möglichkeiten zur Berechnung von Schnittvielfachheiten

Es gibt noch zwei alternative Möglichkeiten die Schnittvielfachheit von affinen Kurven $V(f)$ und $V(g)$ im Punkt $p = (0, 0)$ auszurechnen.

Bemerkung 4.14

Die Schnittvielfachheit von $V(f)$ und $V(g)$ in $p = (0, 0)$ kann als Vektorraumdimension eines \mathbb{C} -Vektorraumes berechnet werden. Es gilt nämlich

$$\text{mult}_{(0,0)}(f \cap g) = \dim_{\mathbb{C}}(\mathbb{C}\{x, y\}/\langle f, g \rangle),$$

d.h. die Schnittvielfachheit von $V(f)$ und $V(g)$ in p ist die Dimension des \mathbb{C} -Vektorraumes, den wir erhalten, wenn wir den Potenzreihenring modulo dem Ideal betrachten, das von f und g erzeugt wird. Diese Dimension kann man wieder mit

Hilfe von Singular ausrechnen, was wir im Beispiel $f = x^3 - y^2$ und $g = x + y$ tun wollen.

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0,(x,y),ds;
> ideal I=x^3-y^2,x+y;
> vdim(std(I));
2

```

Man beachte, daß auch diesmal in der Definition des Ringes r am Ende ein ds statt des üblichen dp steht. Dies ist wichtig, da wir mit Potenzreihen rechnen wollen – das s steht dabei für das englische Wort *series*, gleich Reihe. Der Befehl `vdim` berechnet die Vektorraumdimension des Quotienten, und der Befehl `std` sorgt dafür, daß das Erzeugendensystem f und g zunächst in ein *besseres* überführt wird. Genauer gesagt, es wird ein *Standardbasis* berechnet. Diese Rechnungen sind das Herzstück von SINGULAR.

Wir können mit Hilfe von SINGULAR Schnittvielfachheiten berechnen, ohne Resultanten ausrechnen zu müssen, auch wenn dies für den Rechner der schnellere Weg ist.

Eine zweite Alternative bietet der nächste Satz, der es uns erlaubt, Schnittvielfachheiten mit Hilfe von Parametrisierungen auszurechnen.

Satz 4.15 (Schnittvielfachheit mittels Parametrisierung)

Sind $f, g \in \mathbb{C}[x, y]$ zwei Polynome mit $p = (0, 0) \in V(f) \cap V(g)$ und ist $t \mapsto (x(t), y(t))$ eine primitive polynomiale Parametrisierung von $V(g)$, dann gilt

$$\text{mult}_p(f \cap g) = \text{ord}_t(f(x(t), y(t))).$$

Dabei heißt die Parametrisierung primitiv, wenn sich $x(t)$ und $y(t)$ nicht schreiben lassen als

$$x(t) = a(t^k) \quad \text{und} \quad y(t) = b(t^k)$$

für Polynome $a, b \in \mathbb{C}[t]$ und $k > 0$.

Beweis für Geraden: Wir beweisen nur den Fall, daß $g = ax + by$ ein lineares Polynom mit $b \neq 0$ ist, so daß $V(g)$ eine Gerade durch den Ursprung ist, die nicht parallel zur y -Achse ist. Das Polynom f können wir wieder in der Form $f =$

$\sum_{i=0}^m \mathbf{a}_i \cdot \mathbf{y}^i$ mit $\mathbf{a}_i \in \mathbb{C}[\mathbf{x}]$ schreiben. Die Sylvestermatrix von f und g hat dann die Gestalt

$$S_{f,g} = \begin{pmatrix} \mathbf{a}_0 & \mathbf{a}_1 & \dots & \dots & \mathbf{a}_n \\ \mathbf{ax} & -\mathbf{b} & & & 0 \\ & \mathbf{ax} & -\mathbf{b} & & \vdots \\ & & \ddots & \ddots & 0 \\ & & & \mathbf{ax} & -\mathbf{b} \end{pmatrix}.$$

Die Determinante einer Matrix ändert sich nicht, wenn zu einer Spalte das Vielfache einer anderen Spalte addiert. Wir addieren zur $m-1$ -ten Spalte das $\frac{\mathbf{ax}}{\mathbf{b}}$ -fache der m -ten Spalte, dann zur $m-2$ -ten Spalte das $\frac{\mathbf{ax}}{\mathbf{b}}$ -fache der $m-3$ -ten Spalte, usw. — dadurch überführen wir die Sylvestermatrix in die Form

$$A = \begin{pmatrix} \mathbf{a}_0 + \frac{\mathbf{ax}}{\mathbf{b}} \cdot \mathbf{a}_1 + \dots + \left(\frac{\mathbf{ax}}{\mathbf{b}}\right)^{m-1} \cdot \mathbf{a}_{m-1} + \left(\frac{\mathbf{ax}}{\mathbf{b}}\right)^m \cdot \mathbf{a}_m & \dots & \dots & \dots & \mathbf{a}_m \\ & 0 & & & -\mathbf{b} & & \vdots \\ & & & & 0 & -\mathbf{b} & \vdots \\ & & & & & \ddots & \ddots & \vdots \\ & & & & & & 0 & -\mathbf{b} \end{pmatrix}.$$

Da $S_{f,g}$ und A die gleiche Determinante haben, gilt

$$\begin{aligned} \text{Res}_{f,g} &= \det(S_{f,g}) = \det(A) \\ &= (-\mathbf{b})^m \cdot \left(\mathbf{a}_0 + \frac{\mathbf{ax}}{\mathbf{b}} \cdot \mathbf{a}_1 + \dots + \left(\frac{\mathbf{ax}}{\mathbf{b}}\right)^{m-1} \cdot \mathbf{a}_{m-1} + \left(\frac{\mathbf{ax}}{\mathbf{b}}\right)^m \cdot \mathbf{a}_m \right) \\ &= (-\mathbf{b})^m \cdot f\left(\mathbf{x}, \frac{-\mathbf{bx}}{\mathbf{a}}\right). \end{aligned}$$

Zugleich ist die Abbildung

$$\mathbb{R} \longrightarrow \mathbb{R}^2 : \mathbf{t} \mapsto (\mathbf{x}(\mathbf{t}), \mathbf{y}(\mathbf{t}))$$

mit

$$\mathbf{x}(\mathbf{t}) = \mathbf{t} \quad \text{und} \quad \mathbf{y}(\mathbf{t}) = \frac{-\mathbf{b}}{\mathbf{a}} \cdot \mathbf{t}$$

eine primitive Parametrisierung der Geraden. Deshalb stimmen die Ordnung von $\text{Res}_{f,g}$ bezüglich \mathbf{x} und die Ordnung von $f(\mathbf{x}(\mathbf{t}), \mathbf{y}(\mathbf{t}))$ bezüglich \mathbf{t} überein. \square

Bemerkung 4.16

Das Verfahren mit der Parametrisierung ist sehr effizient, wenn man eine primitive *polynomiale* Parametrisierung einer der beiden Kurven besitzt. Nun besitzen aber die wenigsten Kurven global eine solche Parametrisierung, so daß der Satz in dieser Form nur sehr selten anwendbar ist. Allerdings kann man globale polynomiale Parametrisierungen durch *lokale Puiseux Parametrisierungen* ersetzen, bei denen die Komponentenfunktionen Potenzreihen mit rationalen Exponenten sind. Der Satz gilt dann immer noch, und für jede affine algebraische Kurve durch den Ursprung gilt, daß man jeden Zweig der Kurve lokal auf diese Weise parametrisieren kann.

G) Schnittvielfachheiten und Vielfachheiten

Bemerkung 4.17

Statt Schnittvielfachheiten exakt auszurechnen, können wir sie aber auch einfach abschätzen. Dazu führen wir für eine Kurve $V(F)$ den Begriff der *Vielfachheit* der Kurve $V(F)$ im Punkt P ein. Wir transformieren wie oben P in den Punkt $(0 : 0 : 1)$ und berechnen das dehomogenisierte transformierte Polynom f . Dann ist die *Vielfachheit*

$$\text{mult}_P(F) = \text{ord}(f)$$

von F im Punkt P als die Ordnung von f definiert, d.h. als das Minimum der Grade der Monome von f .

Satz 4.18 (Schnittvielfachheit)

Sind $F, G \in \mathbb{C}[x, y, z]$ nicht-konstante homogene Polynome, die keinen gemeinsamen Teiler haben, so gilt die Abschätzung

$$\text{mult}_P(F \cap G) \geq \text{mult}_P(F) \cdot \text{mult}_P(G).$$

Dabei gilt die Gleichheit genau dann, wenn $V(F)$ und $V(G)$ keine gemeinsame Tangente in P besitzen.

Beweis für den Fall einer Geraden $V(G)$: Es reicht, den Beweis für den Fall $P = (0 : 0 : 1)$ und $G = y$ führen, da wir uns durch Koordinatentransformation auf diesen Fall zurück ziehen können. Mit den Notationen des Beweises des Satzes von Bézout gilt dann aber

$$\begin{aligned} \text{mult}_P(F \cap G) &= \text{ord}_x(\mathbf{a}_0) \geq \min\{\text{ord}(\mathbf{a}_i \cdot \mathbf{y}^i) \mid i = 0, \dots, n\} \\ &= \text{mult}_P(F) = \text{mult}_P(F) \cdot \text{mult}_P(G). \end{aligned}$$

Die Gleichheit gilt genau dann, wenn $\text{ord}(\mathbf{a}_i \cdot \mathbf{y}^i) \geq \text{ord}(\mathbf{a}_0)$ für alle $i = 1, \dots, n$. Das ist aber gleichbedeutend dazu, daß \mathbf{y} nicht den homogenen Anteil kleinsten Grades teilt, sprich, \mathbf{y} ist keine Tangente von F in P .⁶ □

Bemerkung 4.19 (Schnittvielfachheit)

Die Schnittvielfachheit zweier Kurven ist eine lokale Eigenschaft der Kurven, so daß wir genauso für ebene affine Kurven $V(f)$ und $V(g)$ mit $\mathbf{p} = (0, 0) \in V(f) \cap V(g)$ die Ungleichheit

$$\text{mult}_P(f \cap g) \geq \text{ord}(f) \cdot \text{ord}(g)$$

erhalten. Die Gleichheit gilt wieder genau dann, wenn die beiden Kurven im Punkt \mathbf{p} keine gemeinsame Tangente haben.

⁶Für genaueres zu Tangenten an affine ebene Kurven verweisen wir auf das Kapitel zu Singularitäten.

H) Der allgemeine Satz von Bézout

Der Satz von Bézout gilt nicht nur in der projektiven Ebene. Er gilt allgemeiner für projektive Varietäten im $\mathbb{P}_{\mathbb{C}}^n$ in der folgenden Version.

Satz 4.20 (Allgemeiner Satz von Bézout)

Sind $V, W \subseteq \mathbb{P}_{\mathbb{C}}^n$ zwei rein-dimensionale projektive Varietäten, so daß keine Komponente von V in W enthalten ist und keine Komponente von W in V .

a. Ist $\dim(V) + \dim(W) = n$, so ist $V \cap W$ eine endliche Menge und es gilt

$$\sum_{P \in V \cap W} \text{mult}_P(V \cap W) = \deg(V) \cdot \deg(W).$$

b. Ist $\dim(V) + \dim(W) = n + 1$, dann ist $V \cap W$ eine Kurve vom Grad

$$\deg(V \cap W) = \deg(V) \cdot \deg(W).$$

Bemerkung 4.21

Wir wollen an dieser Stelle den Begriffe der Schnittvielfachheit nicht für allgemeine projektive Varietäten einführen. Dazu reichen unsere technischen Mittel nicht aus. Auch den Grad einer Kurve im $\mathbb{P}_{\mathbb{C}}^n$ wollen wir nicht algebraisch definieren. Man kann einen Spezialfall des Satzes von Bézout ggf. als Definition verwenden: der Grad einer Kurve $C \subset \mathbb{P}_{\mathbb{C}}^n$ ist die Anzahl an Schnittpunkten von C mit einer allgemeinen Hyperebene $H \subset \mathbb{P}_{\mathbb{C}}^n$.

Wir werden den Satz nun noch einmal für einen Spezialfall formulieren, den wir im Zusammenhang mit enumerativer Geometrie anwenden wollen.

Korollar 4.22 (Satz von Bézout für Hyperflächen und Geraden)

Ist $F \in \mathbb{C}[x_0, \dots, x_n]$ ein nicht-konstantes homogenes Polynom vom Grad d , $V = V(F) \subset \mathbb{P}_{\mathbb{C}}^n$ und ist $W \subset \mathbb{P}_{\mathbb{C}}^n$ eine Gerade, die nicht in V enthalten ist, dann gilt

$$\sum_{P \in V \cap W} \text{mult}_P(V \cap W) = d.$$

Für die meisten Geraden W gilt zudem $\text{mult}_P(V \cap W) = 1$ für alle $P \in V \cap W$.

Der letzte Zusatz, daß die Schnittvielfachheit für Geraden fast immer eins ist, liegt daran, daß die wenigsten Geraden Tangenten an eine gegebene Varietät sind.

I) Rationale Parametrisierungen mittels Bézout

Bemerkung 4.23 (Parametrisierungen von Kurven)

Wir können uns den Satz von Bézout zunutze machen, um Parametrisierungen von speziellen Kurven zu konstruieren. Es sei $f \in \mathbb{C}[x, y]$ ein Polynom vom Grad d und von Ordnung $d - 1$, d.h.

$$\deg(f) = \text{ord}(f) + 1.$$

Satz 4.18 stellt sicher, daß die Schnittvielfachheit der meisten Ursprungsgeraden $V(y - tx)$, $t \in \mathbb{C}$, mit der Kurve $V(f^h)$ im Ursprung gleich $\text{ord}(f)$ ist. Der Satz von

Bézout sichert dann aber, daß die Gerade $V(\mathbf{y} - t\mathbf{x})$ die Kurve noch in genau einem weiteren Punkt P_t schneiden muß. Die Koordinaten dieses Punktes können wir in Abhängigkeit von t ausrechnen und erhalten so eine Parametrisierung der Kurve.

Ist z.B. $f = (x^2 + y^2)^2 + 3x^2y - y^3$ das definierende Polynom des dreiblättrigen Kleeblattknotens, so ist $\deg(f) = 4 = \text{ord}(f) + 1$. Setzen wir die Gleichung der Geraden $y = tx$ in die Gleichung von f ein, so erhalten wir die Gleichung

$$0 = (x^2 + t^2x^2)^2 + 3tx^3 - t^3x^3 = x^3 \cdot ((1 + t^2)^2 \cdot x + (3t - t^3)).$$

Der Fall $x = 0$ ist unwesentlich, da dann auch $y = 0$ gilt und wir den Ursprung als Lösung finden. Uns interessiert aber der zusätzliche Punkt, so daß wir $x \neq 0$ annehmen dürfen. Dann gilt also

$$x = \frac{3t - t^3}{(1 + t^2)^2}$$

und somit

$$y = \frac{3t^2 - t^4}{(1 + t^2)^2}.$$

Wir erhalten die Parametrisierung des Kleeblattknotens von Seite 5. Abbildung 33

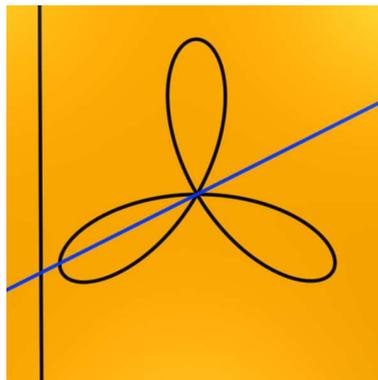


ABBILDUNG 33. Parametrisierung des Kleeblattknotens

ist der Versuch, diese Parametrisierung zu visualisieren. Die blaue Gerade schneidet den Kleeblattknoten im Ursprung und in genau einem weiteren Punkt. Ihre Steigung ist der Parameter t , den man als reelle Zahl mit dem Schnittpunkt mit der zweiten, schwarzen Geraden identifizieren kann. Man erhält auf diese Weise eine Abbildung von der schwarzen Geraden auf den Kleeblattknoten, eine Parametrisierung.

J) Diskriminanten

Bemerkung 4.24 (Resultanten und Diskriminanten)

Wir haben Resultanten oben verwendet, um Schnittvielfachheiten zu definieren. Bekannter ist eine andere Eigenschaft der Resultanten. Sind $f = \sum_{i=0}^m a_i \cdot y^i$ und $g = \sum_{j=0}^n b_j \cdot y^j$ zwei Polynome, deren Koeffizienten aus einem Ring R stammen – z.B. $R = \mathbb{Z}$ oder $R = \mathbb{C}$ oder $R = K[x]$. Wir bilden die Sylvestermatrix $S_{f,g}$ und

die Resultante $\text{Res}_{f,g}$ von f und g wie in Definition 4.8. Die Resultante ist dann ein Element des Ringes \mathbf{R} . Dabei gilt:

f und g haben genau dann einen gemeinsamen Faktor vom Grad mindestens eins, wenn $\text{Res}_{f,g}$ in \mathbf{R} null ist.

Ist $\mathbf{R} = \mathbb{C}$ der Körper der komplexen Zahlen, so ist die Resultante einfach eine komplexe Zahl und es gilt:

f und g haben genau dann eine gemeinsame Nullstelle, wenn $\text{Res}_{f,g} = 0$.

Einen elementaren Beweis der Aussage findet man in [Fis94, Anhang A].

Ist $f \in \mathbb{C}[y]$ und $g = \frac{\partial f}{\partial y}$ die Ableitung von f , dann nennt man die Resultante von f und g auch die *Diskriminante* von f und schreibt

$$D_f = \text{Res}_{f, \frac{\partial f}{\partial y}}.$$

Da f und $\frac{\partial f}{\partial y}$ genau dann eine gemeinsame Nullstelle haben, wenn f eine mehrfache Nullstelle hat, erhalten wir die Aussage:

f hat genau dann eine mehrfache Nullstelle, wenn $D_f = 0$.

Wir können mit Hilfe von Resultanten und Diskriminanten feststellen, ob zwei Polynome gemeinsame Nullstellen haben bzw. ob ein Polynom eine mehrfache Nullstelle hat, *ohne* die Nullstellen von f bzw. g kennen zu müssen!

Beispiel 4.25 (Der Schwalbenschwanz)

In diesem Beispiel wollen wir Polynome der Form

$$f_{a,b,c} = x^4 + ax^2 + bx + c$$

für reelle Zahlen $a, b, c \in \mathbb{R}$ untersuchen. Betrachten wir die Zahlen a, b, c als Parameter, so bilden die Polynome eine dreidimensionale Familie

$$(f_{a,b,c})_{a,b,c \in \mathbb{R}}.$$

Uns interessiert die Frage, für welche Parameterwerte (a, b, c) das Polynom eine mehrfache Nullstelle hat.

Wir betrachten den vierdimensionalen affinen Raum $\mathbb{A}_{\mathbb{R}}^4$ mit Koordinaten x, a, b, c sowie die Projektion

$$\pi : \mathbb{A}_{\mathbb{R}}^4 \longrightarrow \mathbb{A}_{\mathbb{R}}^3 : (x, a, b, c) \mapsto (a, b, c)$$

auf die letzten drei Koordinaten. Für einen festen Punkt $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathbb{A}_{\mathbb{R}}^3$ nennen wir die Menge

$$\pi^{-1}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \mathbb{R} \times \{(\mathbf{a}, \mathbf{b}, \mathbf{c})\} = \{(x, \mathbf{a}, \mathbf{b}, \mathbf{c}) \mid x \in \mathbb{R}\}$$

die *Faser* von π über dem Punkt $(\mathbf{a}, \mathbf{b}, \mathbf{c})$. Sie ist eine Kopie der reellen Zahlenachse.

$$W = V\left(f_{\mathbf{a}, \mathbf{b}, \mathbf{c}}, \frac{\partial f_{\mathbf{a}, \mathbf{b}, \mathbf{c}}}{\partial y}\right) \subset \mathbb{A}_{\mathbb{R}}^4$$

ist eine zweidimensionale Varietät im $\mathbb{A}_{\mathbb{R}}^4$. Halten wir einen Punkt $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in \mathbb{A}_{\mathbb{R}}^3$ fest, so gilt:

$$W \cap \{(x, \mathbf{a}, \mathbf{b}, \mathbf{c}) \mid x \in \mathbb{R}\} \neq \emptyset \iff f_{\mathbf{a}, \mathbf{b}, \mathbf{c}} \text{ hat eine mehrfache Nullstelle.}$$

Wenn wir also die Parameterwerte $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ bestimmen wollen, für die $f_{\mathbf{a}, \mathbf{b}, \mathbf{c}}$ eine mehrfache Nullstelle hat, so müssen wir das Bild $\pi(W)$ der Varietät W unter Projektion π bestimmen. Dies können wir durch Variablenelementation mittels SINGULAR machen.

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0,(x,a,b,c),dp;
> poly f=x^4+a*x^2+b*x+c;
> ideal I=f,diff(f,x);
> eliminate(I,x);
_[1]=4*a^3*b^2-16*a^4*c+27*b^4-144*a*b^2*c+128*a^2*c^2-256*c^3

```

Also ist das Polynom

$$D_{f_{\mathbf{a}, \mathbf{b}, \mathbf{c}}} = 4 \cdot a^3 \cdot b^2 - 16 \cdot a^4 \cdot c + 27 \cdot b^4 - 144 \cdot a \cdot b^2 \cdot c + 128 \cdot a^2 \cdot c^2 - 256 \cdot c^3$$

die Diskriminante der Familie und das Bild von W unter der Projektion π ist gegeben als

$$\pi(W) = V(4a^3b^2 - 16a^4c + 27b^4 - 144ab^2c + 128a^2c^2 - 256c^3).$$

Die Gleichung ist genau die Diskriminante von $f_{\mathbf{a}, \mathbf{b}, \mathbf{c}}$, wenn wir f als Polynom mit Koeffizienten im Ring $R = \mathbb{C}[a, b, c]$ auffassen. Wir hätten sie deshalb in SINGULAR auch mit Resultantenmethoden ausrechnen können. Dazu können wir in obiger SINGULAR -Sitzung folgendes Kommando eingeben:

```

> resultant(f,diff(f,x),x);
-4*a^3*b^2+16*a^4*c-27*b^4+144*a*b^2*c-128*a^2*c^2+256*c^3

```

Visualisieren wir die Varietät $\pi(W)$, so erhalten wir das Bild in Abbildung 34, das als *Schwalbenschwanz* bekannt ist. Für die meisten Punkte $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ auf der Fläche wird das Polynom $f_{\mathbf{a}, \mathbf{b}, \mathbf{c}}$ eine doppelte Nullstelle und zwei einfache Nullstellen haben. Die Punkte auf der schwarz eingezeichneten Kurve sind die Punkte, für die das Polynom gar eine dreifache oder vierfache Nullstelle hat, wobei letzteres nur

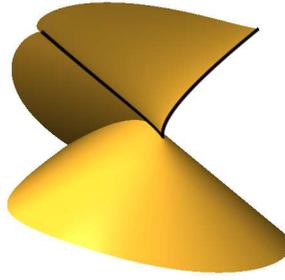


ABBILDUNG 34. Schwalbenschwanz

für den Punkt $(0,0,0)$, d.h. die Spitze der schwarzen Kurve, gilt. Dies kann man wieder mittels Elimination berechnen, denn $f_{a,b,c}$ hat genau dann eine Nullstelle von Vielfachheit mindestens 3, wenn das Polynom $f_{a,b,c}$ sowie seine ersten beiden Ableitungen verschwinden, d.h. wir müssen die Varietät

$$V\left(f_{a,b,c}, \frac{\partial f_{a,b,c}}{\partial x}, \frac{\partial^2 f_{a,b,c}}{\partial x^2}\right)$$

mittels π projizieren. Dies können wir in obiger SINGULAR -Sitzung wie folgt realisieren:

```
> ideal J=f,diff(f,x),diff(diff(f,x),x);
> eliminate(J,x);
_[1]=9*b^2-32*a*c
_[2]=a^2+12*c
```

Wir sehen, daß diese Raumkurve in $\mathbb{A}_{\mathbb{R}}^3$ durch die beiden Gleichungen

$$9 \cdot b^2 - 32 \cdot a \cdot c = 0 \quad \text{und} \quad a^2 + 12 \cdot c = 0$$

gegeben wird.

Wenn Sie das Verhalten der Nullstellen von f – sprich ihre Vielfachheiten, ihre Lage zueinander und ob sie reell oder komplex sind – genauer sehen wollen, dann schauen Sie sich die mit **Surf** erstellte Animation für den 15. Dezember in folgendem Adventskalender an:

<http://www.calendar.algebraicsurface.net>

K) Aufgaben

Aufgabe 4.26 (Division mit Rest)

Beweisen Sie, daß es im Polynomring $K[x]$ in einer Veränderlichen über einem Körper eine *Division mit Rest* gibt. D.h. für je zwei Polynome $f, g \in K[x]$ mit $g \neq 0$ gibt es zwei eindeutig bestimmte Polynome $q, r \in K[x]$ mit

$$f = q \cdot g + r$$

und

$$\deg(\mathbf{r}) < \deg(\mathbf{g}).$$

Hinweis: man führe den Beweis mittels Induktion nach dem Grad von f .

Aufgabe 4.27

Berechnen Sie für folgende ebenen projektiven Kurven $V(F)$ die Tangente in dem angegebenen Punkt P , sofern dies möglich ist:

a. $F = x^2 + y^2 - z^2$, $P = (0 : 1 : 1)$.

b. $F = x^2 + y^2 - z^2$, $P = (3 : 4 : 5)$.

c. $F = x^2z + y^3$, $P = (0 : 0 : 1)$.

d. $F = x^2z + y^3$, $P = (1 : 0 : 0)$.

e. $F = x^2y - y^3$, $P = (0 : 0 : 1)$.

f. $F = x^2y - y^3$, $P = (1 : 1 : 1)$.

Welche der Punkte sind singuläre Punkte der gegebenen Kurve?

Aufgabe 4.28

Wir betrachten die ebenen affinen Kurven $V(f)$ und $V(g)$ mit

$$f = x^2 - y^3$$

und

$$g = y^2 - x^2 - x^3,$$

d.h. die Kuspel und den Newtonschen Knoten. $V(f)$ besitzt die polynomiale Parametrisierung

$$t \mapsto (t^3, t^2).$$

Zeigen Sie, daß die Schnittvielfachheit von $V(f)$ und $V(g)$ im Punkt $p = (0, 0)$ die Gleichung

$$\text{mult}_p(f \cap g) = \text{ord}_t(g(t^3, t^2)),$$

erfüllt, wobei die Ordnung ord_t eines Polynoms in t der niedrigste Grad eines Monoms des Polynoms ist.

Aufgabe 4.29

Berechnen Sie in Beispiel 4.3 die Schnittvielfachheit von C_t und C' im Punkt P_1 für $t = 1$ und $t = 4$ mittels der Resultanten.

Aufgabe 4.30

Berechnen Sie für folgende Polynome f und g die Schnittvielfachheit von $V(f)$ und $V(g)$ im Punkt $(0, 0)$:

a. $f = x^3 + 4xy^4$ und $g = x + y$.

b. $f = (x^2 + y^2)^2 + 3x^2y - y^3$ und $g = x + 2y$.

c. $f = (x^2 + y^2)^2 + 3x^2y - y^3$ und $g = y$.

- d. $f = (x^2 + y^2)^2 + 3x^2y - y^3$ und $g = y - x^2$.
 e. $f = (x^2 + y^2)^2 + 3x^2y - y^3$ und $g = y^2 - x$.
 f. $f = (x^2 + y^2)^2 + 3x^2y - y^3$ und $g = y^2 - x^2$.

In welchen Fällen gilt die Gleichheit

$$\text{mult}_p(f \cap g) = \text{mult}_p(f) \cdot \text{mult}_p(g)?$$

Visualisieren Sie $V(f)$ und $V(g)$ im Punkt $p = (0, 0)$.

Aufgabe 4.31

Überprüfen Sie den Satz von Bézout für die ebenen projektiven Kurven $V(F)$ und $V(G)$ mit

$$F = y^2z - x \cdot (x - z) \cdot (x - 2z)$$

und

$$G = y^2 + 2x^2 - 2xz.$$

Visualisieren Sie auch die beiden Kurven und ihren Schnitt in der projektiven Ebene.

Aufgabe 4.32

Berechnen Sie eine rationale Parametrisierung der ebenen affinen Kurve

$$V(x^3 - 3x^2y + 3xy^2 - y^3 + 4x^2y^2)$$

und visualisieren Sie den projektiven Abschluß der Kurve in $\mathbb{P}_{\mathbb{R}}^2$.

Aufgabe 4.33

Geben Sie sich weitere Polynome $f \in \mathbb{R}[x, y]$ mit $\deg(f) = \text{ord}(f) + 1$ vor, berechnen Sie eine zugehörige Parametrisierung und visualisieren Sie den projektiven Abschluß der Kurve im $\mathbb{P}_{\mathbb{R}}^2$.

Aufgabe 4.34

Berechnen Sie die Diskriminante der Familie $(f_{a,b,c})_{a,b,c \in \mathbb{R}}$ mit

$$f_{a,b,c} = ax^2 + bx + c$$

und visualisieren Sie diese mit **Surfex**. Schneiden sie die Fläche mit der Ebene, die durch $\mathbf{a} = \mathbf{0}$ definiert wird. Was erhalten Sie als Schnitt, und wie ist das Ergebnis algebraisch zu interpretieren, d.h. in Bezug auf mehrfache Nullstellen des Polynoms $f_{a,b,c}$.

Aufgabe 4.35

Berechnen Sie die Diskriminante der Familie $(f_{a,b,c})_{a,b,c \in \mathbb{R}}$ mit

$$f_{a,b,c} = x^3 + ax^2 + bx + c$$

und visualisieren Sie diese mit **Surfex**. Berechnen Sie dann die Gleichungen, denen die Parameter $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ genügen, für die das Polynom $f_{a,b,c}$ eine dreifache Nullstelle hat und zeichnen sie die zugehörige Kurve auf der Fläche der Diskriminanten ein.

5 SINGULARITÄTEN

(VON OLIVER LABS)

Siehe Olivers Skript.

6 ENUMERATIVE GEOMETRIE

(VON THOMAS MARKWIG)

A) Was ist enumerative Geometrie?

In der enumerativen Geometrie werden geometrische Objekte gezählt, die vorgegebenen Bedingungen genügen. Ein Beispiel dieser Art haben wir mit dem Satz von Bézout schon kennen gelernt. Die geometrischen Objekte, die wir dort zählen wollen, sind Punkte und die vorgegebene Bedingung ist, daß sie Schnittpunkt zweier gegebener Kurven $V(F)$ und $V(G)$ sind.

Die Anzahl der Schnittpunkte zweier ebener projektiver Kurven $V(F)$ und $V(G)$ ist $\deg(F) \cdot \deg(G)$.

Das Beispiel zeigt auch schon ein weiteres Charakteristikum enumerativer Fragen in der algebraischen Geometrie. *Es ist nicht immer korrekt!* Haben F und G einen gemeinsamen Faktor, z.B. $F = x \cdot (x^2 - yz)$ und $G = x \cdot (x^3 - y^3)$, so ist die Anzahl der Schnittpunkte in $\mathbb{P}_{\mathbb{C}}^2$ unendlich. Wählt man die beiden Polynome F und G aber zufällig, so werden sie keinen gemeinsamen Faktor haben. Die obige Aussage ist *im allgemeinen* also richtig!

Wir möchten die Aussage, daß die Polynome bei *zufälliger Wahl* keinen gemeinsamen Faktor haben werden, genauer erläutern und beschränken uns dabei auf den Fall, daß $\deg(F) = 2$ und $\deg(G) = 1$. Die Polynome haben dann die Form

$$F = a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}xz + a_{01}yz + a_{00}z^2$$

und

$$G = b_0x + b_1y + b_2z$$

mit $a_{ij}, b_k \in \mathbb{C}$. Dabei können wir die a_{ij} und b_k in den komplexen Zahlen frei wählen, so daß wir für F sechs und für G drei freie Parameter haben. In der am Ende von Kapitel 1 eingeführten Sprache bilden die Tupel von Polynomen (F, G) eine Familie

$$\left(\text{big}(a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}xz + a_{01}yz + a_{00}z^2, b_0x + b_1y + b_2z) \right)_{a_{ij}, b_k \in \mathbb{C}}$$

der Dimension $6 + 3 = 9$ und der Parameterraum der Familie ist der Raum \mathbb{C}^9 mit den Koordinaten

$$(a_{20}, a_{11}, a_{02}, a_{10}, a_{01}, a_{00}, b_0, b_1, b_2).$$

Verlangen wir nun, daß G und F einen Teiler gemeinsam haben, so ist G ein Teiler von F und F hat die Form

$$F = G \cdot (c_0x + c_1y + c_2z) = (b_0x + b_1y + b_2z) \cdot (c_0x + c_1y + c_2z)$$

für irgendwelche komplexen Zahlen $c_0, c_1, c_2 \in \mathbb{C}$. Wir haben für ein Tupel

$$(F, G) = \left((b_0x + b_1y + b_2z) \cdot (c_0x + c_1y + c_2z), (b_0x + b_1y + b_2z) \right)$$

dieser Form also nur noch sechs Parameter, so daß diese Polynome eine höchstens sechsdimensionale Teilmenge in der Familie aller Polynompaare (F, G) bilden. Wenn man in einem neundimensionalen Raum einen Punkt zufällig auswählt, dann ist die Wahrscheinlichkeit, daß er auf einer vorher festgelegten sechsdimensionalen Teilmenge liegt, aber sehr gering, nämlich null. Die sechsdimensionale Teilmenge ist übrigens eine algebraische Varietät, deren Gleichungen man mit SINGULAR ausrechnen kann. Dazu führt man einen Koeffizientenvergleich der beiden Darstellungen von F durch

$$a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}xz + a_{01}yz + a_{00}z^2 = (b_0x + b_1y + b_2z) \cdot (c_0x + c_1y + c_2z) \quad (5)$$

und erhält damit sechs Gleichungen in den Variablen a_{ij}, b_k, c_l . Diese definieren eine algebraische Varietät in einem zwölfdimensionalen Raum, deren Projektion auf den neundimensionalen Raum mit den Koordinaten a_{ij} und b_k uns interessiert. Denn zu einem Punkt $(a_{ij}, b_k \mid 0 \leq i + j \leq 2, k = 0, 1, 2)$ in dieser Projektion gehört ein Tripel (c_0, c_1, c_2) , so daß die Gleichung (5) erfüllt ist. Wie wir die Gleichungen einer Varietät unter einer Projektion mit Hilfe von Elimination ausrechnen, wissen wir aber.

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0, (a00,a01,a10,a20,a11,a02,b0,b1,b2,c0,c1,c2), dp;
> ideal I=a20-b0*c0,a11-b0*c1-b1*c0,a10-b0*c2-b2*c0,a02-b1*c1,
a01-b1*c2-b2*c1,a00-b2*c2;
> ideal J=eliminate(I,c0*c1*c2);
> J;
[1]=a20*b1^2-a11*b0*b1+a02*b0^2
[2]=a01*b0*b1-a10*b1^2+a11*b1*b2-2*a02*b0*b2
[3]=a01*b0^2-a10*b0*b1+2*a20*b1*b2-a11*b0*b2
[4]=2*a01*a20*b1-a01*a11*b0-a10*a11*b1+2*a10*a02*b0-4*a20*a02*b2+a11^2*b2
[5]=a00*b1^2-a01*b1*b2+a02*b2^2
[6]=2*a00*b0*b1-a01*b0*b2-a10*b1*b2+a11*b2^2
[7]=a00*b0^2-a10*b0*b2+a20*b2^2
[8]=2*a00*a11*b1-4*a00*a02*b0+a01^2*b0-a01*a10*b1-a01*a11*b2+2*a10*a02*b2
[9]=4*a00*a20*b1-2*a00*a11*b0+a01*a10*b0-2*a01*a20*b2-a10^2*b1+a10*a11*b2
[10]=4*a00*a20*a02-a00*a11^2-a01^2*a20+a01*a10*a11-a10^2*a02

```

Wir erhalten also zehn Gleichungen in den neun Veränderlichen. Dabei haben wir doch eine sechsdimensionalen Varietät erwartet. Sind da nicht zehn Gleichungen etwas zu viel? Wir können die Dimension dieser Varietät ebenfalls mit SINGULAR berechnen. Dabei müssen wir berücksichtigen, daß wir drei Parameter eliminiert haben!

```
> dim(std(J))-3;
6
```

Die Dimension ist also sechs, wie wir erwartet haben.

Das Beispiel erläutert den Zusatz *im allgemeinen* in folgendem Grundprinzip der enumerativen Geometrie:

Die Bedingungen müssen von der Art sein, daß im allgemeinen nur eine endliche Anzahl an Elementen aus der Grundmenge der zugelassenen geometrischen Objekte diese erfüllen!

B) Kurven durch vorgegebene Punkte

Für die Überlegungen in diesem Abschnitt wechseln wir wieder vom Körper \mathbb{C} der komplexen Zahlen zu einem beliebigen Körper K .

Unser erstes Beispiel für enumerative Fragestellungen in der algebraischen Geometrie war schon recht komplex – der Beweis des Satzes von Bézout ist anspruchsvoll und die Menge der Ausnahmebedingungen hat eine komplizierte Beschreibung —, obwohl wir nur Punkte zählen wollten. In diesem Abschnitt wollen wir Kurven zählen, und überraschenderweise wird das Leben damit einfacher. Der Grund dafür ist, daß wir uns zunächst nur einfache Bedingungen vorgeben: *die Kurven sollen durch einige fest vorgegebene Punkte gehen.*

Das grundlegendste Beispiel dieser Art ist:

Durch je zwei Punkte der projektiven Ebene geht genau eine Gerade.

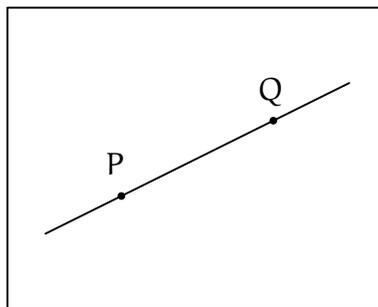


ABBILDUNG 35. Die Gerade durch P und Q

Die Grundmenge der geometrischen Objekte ist die Menge der Geraden in der projektiven Ebene, d.h. die Menge

$$\{V(ax + by + cz) \mid (0, 0, 0) \neq (a, b, c) \in K^3\},$$

und als Bedingung halten wir zwei Punkte P und Q in \mathbb{P}_K^2 fest, deren Koordinaten die Geradengleichung erfüllen sollen. Die Bedingung entspricht also der Wahl eines Punktpaares

$$(P, Q) \in \mathbb{P}_K^2 \times \mathbb{P}_K^2.$$

Damit die Anzahl an Geraden endlich ist, müssen wir nur fordern, daß die Punkte P und Q nicht gleich sind. Aber der Parameterraum der Bedingungen ist vierdimensional, und daß die Punkte gleich sind, liefert die zweidimensionalen Teilmenge $\{(P, P) \mid P \in \mathbb{P}_K^2\}$. Im allgemeinen wird die Anzahl also endlich sein, nämlich eins.

Wie kann man diese Aussage eigentlich beweisen?

Dazu beachten wir zunächst, daß zwei Geraden $V(ax + by + cz)$ und $V(a'x + b'y + c'z)$ genau dann gleich sind, wenn sich die beiden Polynome nur um ein skalares Vielfaches unterscheiden, d.h.

$$\begin{aligned} V(ax + by + cz) &= V(a'x + b'y + c'z) \\ \iff \exists \lambda \in K \setminus \{0\} : ax + by + cz &= \lambda \cdot (a'x + b'y + c'z) \\ \iff (a : b : c) &= (a' : b' : c'). \end{aligned}$$

Wir können eine Gerade $V(ax + by + cz)$ mithin mit einem Punkt $(a : b : c)$ der sogenannten *dualen* projektiven Ebene identifizieren, d.h. die Abbildung

$$\Phi : \mathbb{P}_K^2 \longrightarrow \{V(ax+by+cz) \mid (0,0,0) \neq (a,b,c) \in K^3\} : (a : b : c) \mapsto V(ax+by+cz)$$

ist *bijektiv*. Wir unterscheiden deshalb nicht zwischen den beiden Mengen und sagen, daß die Menge der Geraden in der projektiven Ebene selbst wieder eine projektive Ebene ist. Sie ist damit eine algebraische Varietät.

Ein Punkt $P = (p_0 : p_1 : p_2)$ liegt genau dann auf der Geraden $V(ax + by + cz)$, wenn er der Geradengleichung genügt, d.h.

$$P = (p_0 : p_1 : p_2) \in V(ax + by + cz) \iff p_0 \cdot a + p_1 \cdot b + p_2 \cdot c = 0.$$

Erinnern wir uns an unser Eingangsproblem. Uns sind zwei verschiedene Punkte $P = (p_0 : p_1 : p_2)$ und $Q = (q_0 : q_1 : q_2)$ in der projektiven Ebene gegeben und wir *suchen* einen Punkt $(a : b : c)$ in der dualen projektiven Ebene, so daß die beiden Gleichungen

$$\begin{aligned} p_0 \cdot a + p_1 \cdot b + p_2 \cdot c &= 0 \\ q_0 \cdot a + q_1 \cdot b + q_2 \cdot c &= 0 \end{aligned}$$

gelten. Die p_i und q_i sind bekannte Zahlen, a, b, c sind gesuchte Unbekannte! Daß die beiden Punkte P und Q verschieden sind, bedeutet, daß die beiden Gleichungen linear unabhängig sind. Mithin ist die Lösungsmenge des Gleichungssystems eindimensional, da wir zwei unabhängige Gleichungen bei drei Unbekannten haben. Da das Gleichungssystem homogen ist, ist die Lösungsmenge damit eine Ursprungsgerade im K^3 , also ein Punkt in der projektiven Ebene. Wir finden also *genau* einen

Punkt $(a : b : c)$, der unser Problem löst, d.h. genau eine Gerade $V(ax + by + cz)$ auf der die beiden Punkte P und Q liegen.

Bei der Beschreibung des enumerativen Problems der Anzahl an Geraden durch zwei Punkte ist die Menge der zugelassenen geometrischen Objekte ein projektiver Raum, die Gesamtheit der Bedingungen wird durch eine algebraische Varietät beschrieben und die Menge der Ausnahmebedingungen hat niedere Dimension.

Wir wollen nun den Grad der Kurven, die wir zählen, erhöhen.

Wie viele Punkte müssen wir festlegen, damit die Anzahl an ebenen projektiven Quadriken durch diese Punkte endlich wird?

Eine ebene projektive Quadrik ist durch eine Gleichung der Form

$$a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}xz + a_{01}yz + a_{00}z^2 = 0 \quad (6)$$

gegeben. Dabei ist die Gleichung wieder nur bis auf ein skalares Vielfaches eindeutig bestimmt. Wir erhalten analog zum Beispiel der Geraden die Identifikation der Menge der Quadriken mit dem projektiven Raum $\mathbb{P}_{\mathbb{K}}^5$ mit den Koordinaten

$$(a_{20} : a_{11} : a_{02} : a_{10} : a_{01} : a_{00}).$$

Daß ein Punkt $P = (p_0 : p_1 : p_2)$ auf der Quadrik in Gleichung (6) liegt, bedeutet, daß die lineare Gleichung

$$p_0^2 \cdot a_{20} + p_0 \cdot p_1 \cdot a_{11} + p_1^2 \cdot a_{02} + p_0 \cdot p_2 \cdot a_{10} + p_1 \cdot p_2 \cdot a_{01} + p_2^2 \cdot a_{00} = 0$$

erfüllt ist. Dabei sind die p_i wieder bekannt und die a_{ij} sind gesucht. Die Gleichung ist eine *lineare* Gleichung in sechs Unbekannten. Wir müssen fünf solcher Gleichungen haben, damit der Lösungsraum eindimensional wird, d.h. eine Ursprungsgerade und damit ein Punkt im $\mathbb{P}_{\mathbb{K}}^5$. Damit erhalten wir, daß fünf Punkte eine Quadrik eindeutig festlegen. Die Bedingungen an die Quadriken sind also durch die Menge

$$\mathbb{P}_{\mathbb{K}}^2 \times \mathbb{P}_{\mathbb{K}}^2 \times \mathbb{P}_{\mathbb{K}}^2 \times \mathbb{P}_{\mathbb{K}}^2 \times \mathbb{P}_{\mathbb{K}}^2$$

gegeben.

Bei unserer Argumentation sind wir aber davon ausgegangen, daß fünf lineare Gleichungen in sechs Unbekannten einen Lösungsraum der Dimension fünf ergeben. Das ist nur dann richtig, wenn die Gleichungen linear unabhängig sind. Bezeichnen wir

die Punkte mit $P_i = (p_{i0} : p_{i1} : p_{i2})$, $i = 1, \dots, 5$, dann ist die Matrix des linearen Gleichungssystems

$$\begin{pmatrix} p_{10}^2 & p_{10} \cdot p_{11} & p_{11}^2 & p_{10} \cdot p_{12} & p_{11} \cdot p_{12} & p_{12}^2 \\ p_{20}^2 & p_{20} \cdot p_{21} & p_{21}^2 & p_{20} \cdot p_{22} & p_{21} \cdot p_{22} & p_{22}^2 \\ p_{30}^2 & p_{30} \cdot p_{31} & p_{31}^2 & p_{30} \cdot p_{32} & p_{31} \cdot p_{32} & p_{32}^2 \\ p_{40}^2 & p_{40} \cdot p_{41} & p_{41}^2 & p_{40} \cdot p_{42} & p_{41} \cdot p_{42} & p_{42}^2 \\ p_{50}^2 & p_{50} \cdot p_{51} & p_{51}^2 & p_{50} \cdot p_{52} & p_{51} \cdot p_{52} & p_{52}^2 \end{pmatrix}. \quad (7)$$

Die Zeilen dieser Matrix sind genau dann linear abhängig, wenn alle sechs 5×5 -Minoren der Matrix null sind. Dabei ist ein 5×5 -Minor die Determinante der Matrix, die entsteht, wenn man aus obiger Matrix eine Spalte streicht. Ein solcher Minor ist aber ein Polynom in den Einträgen der Matrix. Wir erhalten also sechs Gleichungen in den Koordinaten p_{ij} des Parameterraums der Bedingungen und diese Gleichungen beschreiben genau die Ausnahmebedingungen. Mithin ist die Menge der Ausnahmebedingungen niederdimensional und wir haben folgende Aussage bewiesen.

Durch fünf Punkte in der projektiven Ebene geht im allgemeinen genau eine Quadrik.

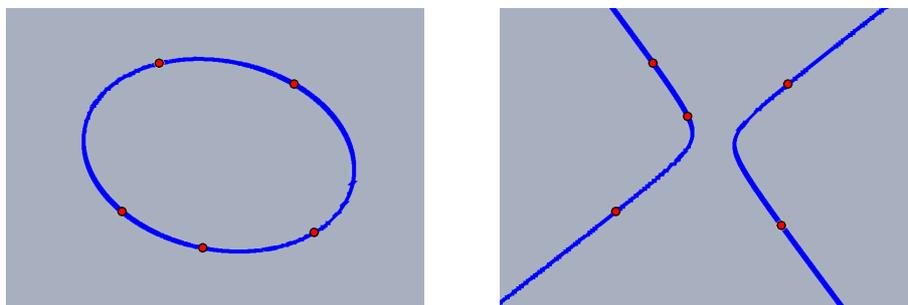


ABBILDUNG 36. Quadriken durch fünf Punkte

Die Bilder in Abbildung 36 wurden mit der dynamischen Geometriesoftware *Cinderella* erstellt (siehe [HRG08]).

Man kann die Bedingung, die die Punkte P_1, \dots, P_5 erfüllen müssen, damit die es genau eine Quadrik durch die fünf Punkte gibt, auch geometrisch sehr schön formulieren. Wir wollen dies hier tun, weil wir das Ergebnis später noch benötigen.

Proposition 6.1

Es seien $P_1, \dots, P_5 \in \mathbb{P}_K^2$ fünf Punkte, von denen keine vier auf einer Geraden liegen, dann gibt es genau eine Quadrik durch diese fünf Punkte.

Beweis: Wenn keine vier der Punkte auf einer Geraden liegen, dann können nicht je drei der P_i kollinear sein. Wir können also ohne Einschränkung annehmen, daß die drei Punkte P_1, P_2 und P_3 nicht auf einer Geraden liegen. Da die Fragestellung

invariant unter linearen Koordinatentransformationen ist, und da wir mit einer linearen Koordinatentransformation die Punkte P_1 auf $(1 : 0 : 0)$, P_2 auf $(0 : 1 : 0)$ und P_3 auf $(0 : 0 : 1)$ abbilden können, können wir ohne Einschränkung annehmen, daß bereits

$$P_1 = (1 : 0 : 0), \quad P_2 = (0 : 1 : 0) \quad \text{und} \quad P_3 = (0 : 0 : 1)$$

gilt. Wir setzen nun zur Vereinfachung der Notation

$$P_4 = (u : v : w) \quad \text{und} \quad P_5 = (x : y : z).$$

Die Matrix in (7) nimmt dann die Gestalt

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ u^2 & uv & v^2 & uw & vw & w^2 \\ x^2 & xy & y^2 & xz & yz & z^2 \end{pmatrix}$$

an. Von den sechs 5×5 -Minoren sind nur die folgenden drei nicht automatisch null:

$$vy \cdot (wx - uz), \quad wz \cdot (vx - uy) \quad \text{und} \quad ux \cdot (wy - vz).$$

Die Koordinaten der Punkte P_4 und P_5 , für die es mehr als eine Quadrik durch die Punkte P_1, \dots, P_5 gibt, sind also genau die Lösungsmenge der drei Gleichungen:

$$\begin{aligned} vy \cdot (wx - uz) &= 0, \\ wz \cdot (vx - uy) &= 0, \\ ux \cdot (wy - vz) &= 0. \end{aligned}$$

Dabei müssen wir beachten, daß die fünf Punkte paarweise verschieden sind und daß es sich um homogene Koordinaten handelt, d.h. in jedem Punkt muß mindestens eine Koordinate ungleich null sein und wir können eine der Koordinaten, die nicht null ist, stets auf eins setzen. Wir betrachten nun verschiedene Fälle.

- 1. Fall:** $u = 0$. Da $P_4 \neq P_2$ und $P_4 \neq P_3$, muß dann $v \neq 0$ und $w \neq 0$ gelten. Unsere drei Gleichungen reduzieren sich dann zu den zwei Gleichungen

$$v \cdot y \cdot w \cdot x = 0 \quad \text{und} \quad w \cdot z \cdot v \cdot x = 0$$

und damit zu

$$y \cdot x = 0 \quad \text{und} \quad z \cdot x = 0.$$

Falls $x = 0$ gilt, gilt

$$P_2 = (0 : 1 : 0), \quad P_3 = (0 : 0 : 1), \quad P_4 = (0 : u : v), \quad P_5 = (0 : y : z) \in \overline{P_1 P_2},$$

im Widerspruch dazu, daß keine vier der Punkte auf einer Geraden liegen. Falls $x \neq 0$, dann muß $y = z = 0$ gelten, d.h. $P_5 = P_1$, was nach Voraussetzung ebenfalls ausgeschlossen ist.

- 2.-6. Fall:** Die Fälle $v = 0$ oder $w = 0$ oder $x = 0$ oder $y = 0$ oder $z = 0$ schließt man ganz analog aus.

7. Fall: Es bleibt also der Fall zu betrachten, daß alle sechs Koordinaten u, v, w, x, y, z ungleich null sind. Dann können wir ohne Einschränkung $u = 1 = x$ annehmen. Die erste und zweite unserer Gleichungen liefern uns dann

$$w = z \quad \text{und} \quad v = y,$$

d.h.

$$P_4 = (1 : v : w) = (1 : y : z) = P_5,$$

was nach Voraussetzung ausgeschlossen ist.

Damit hat die Matrix M vollen Rang, und dies ist, wie wir uns weiter oben überlegt haben, gleichwertig dazu, daß es genau eine Quadrik gibt, die durch die fünf Punkte geht. \square

Wir können das Verfahren nun leicht auf Kurven beliebigen Grades verallgemeinern. Ein homogenes Polynom vom Grad d in drei Veränderlichen hat

$$\binom{d+2}{2} = \frac{(d+2) \cdot (d+1)}{2} = \frac{d \cdot (d+3)}{2} + 1$$

Koeffizienten. Damit zeigt sich die folgende Aussage analog zu obiger Betrachtung.

Die ebenen Kurven vom Grad d bilden einen projektiven Raum der Dimension $\frac{d \cdot (d+3)}{2}$ und durch $\frac{d \cdot (d+3)}{2}$ Punkte in der projektiven Ebene geht im allgemeinen genau eine Kurve vom Grad d .

C) Rationale Kurven durch vorgegebene Punkte

Für die Betrachtungen dieses Abschnitts beschränken wir uns wieder auf den Körper der komplexen Zahlen.

Definition 6.2

Projektive Kurven C , die eine Parametrisierung

$$\varphi : \mathbb{P}_{\mathbb{C}}^1 \longrightarrow C$$

durch die projektive Gerade besitzen, werden *rational* genannt.

Beispiel 6.3

a. Jede Gerade ist rational. Z.B. besitzt die Gerade $V(x+y-z)$ die Parametrisierung

$$\varphi : \mathbb{P}_{\mathbb{C}}^1 \longrightarrow V(x+y-z) : (s:t) \mapsto (s:t:s+t).$$

b. Jede glatte Quadrik ist rational. Z.B. besitzt die Quadrik $V(xz - y^2)$ die Parametrisierung

$$\varphi : \mathbb{P}_{\mathbb{C}}^1 \longrightarrow V(xz - y^2) : (s:t) \mapsto (s^2 : st : t^2).$$

c. Der *Newtonsche Knoten* ist rational mit der Parametrisierung

$$\varphi : \mathbb{P}_{\mathbb{C}}^1 \longrightarrow V(y^2z - x^2z - x^3) : (s:t) \mapsto (st^2 - s^3 : t^3 - s^2t : s^3).$$

d. Die *Neilsche Parabel* ist rational mit der Parametrisierung

$$\varphi : \mathbb{P}_{\mathbb{C}}^1 \longrightarrow V(y^2z - x^3) : (s : t) \mapsto (st^2 : t^3).$$

Satz 6.4 (Rationale Kubiken)

Eine irreduzible Kurve vom Grad drei hat höchstens einen singulären Punkt, und eine sie ist genau dann singulär, wenn sie rational ist.

Beweis: Nehmen wir an, es gäbe ein homogenes Polynom F vom Grad drei in $\mathbb{C}[x, y, z]$, so daß die Kurve $V(F)$ zwei singuläre Punkte P und Q hätte. Es gibt eine Gerade $V(G)$ durch die beiden Punkte P und Q . Die Vielfachheit einer Kurve in einem singulären Punkt ist mindestens zwei. Nach Satz 4.18 ist die Schnittvielfachheit von $V(F)$ mit der Geraden $V(G)$ in einem Punkt aber mindestens gleich der Vielfachheit von F in diesem Punkt. Da F irreduzibel ist, haben F und G keinen gemeinsamen Faktor und wir erhalten mit dem Satz von Bézout 4.5 die Ungleichung

$$3 = \deg(F) \cdot \deg(G) \geq \text{mult}_P(F \cap G) + \text{mult}_Q(F \cap G) \geq 2 + 2 = 4.$$

Damit haben wir einen Widerspruch hergeleitet und somit kann es keine irreduzible Kurve vom Grad drei mit zwei singulären Punkten geben.

Ist P ein singulärer Punkt einer irreduziblen Kubik $V(F)$, so können wir nach einer Koordinatentransformation annehmen, daß $P = (0 : 0 : 1)$ ist. Dann hat das Polynom $f = F(x, y, 1)$ vom Grad drei im Ursprung $(0, 0)$ die Ordnung zwei. Wir können also eine rationale Parametrisierung von $V(f)$ wie in Bemerkung 4.23 berechnen und anschließend homogenisieren, um eine Parametrisierung von $V(F)$ zu finden. Auf diese Weise sind wir auch zu den beiden Parametrisierungen in Beispiel 6.3 gekommen, die die beiden wesentlichen Beispiele darstellen. Andere Singularitätstypen als den gewöhnlichen Doppelpunkt oder die Kuspel gibt es auf Kurven vom Grad drei nicht.

Es bleibt noch zu zeigen, daß eine irreduzible Kubik, die nicht singulär ist, auch nicht rational sein kann. Für diesen Teil des Beweises wollen wir nur die Idee angeben. Nach einer Koordinatentransformation können wir annehmen, daß

$$f = F(x, y, 1) = y^2 - x \cdot (x - 1) \cdot (x - \lambda)$$

mit $\lambda \in \mathbb{C} \setminus \{0, 1\}$ gilt. Man nennt f die *Legendreform* der Kubik. Für eine solche haben wir bereits in Beispiel 1.22 gesehen, daß die zugehörige affine Kurve keine rationale Parametrisierung besitzt (siehe auch Beispiel 1.22). Dann kann $V(F)$ aber auch keine besitzen. \square

Der Satz läßt sich wie folgt verallgemeinern, wobei die Zahl $\frac{(d-1) \cdot (d-2)}{2}$ das *geometrische Geschlecht* einer ebenen projektiven Kurve vom Grad d ist.

Satz 6.5 (Rationale ebene projektive Kurven)

Die maximale Anzahl von gewöhnlichen Doppelpunkten auf einer ebenen projektiven Kurve vom Grad d ist $\frac{(d-1) \cdot (d-2)}{2}$. Eine solche Kurve ist rational.

Eine zentrale Frage der enumerativen algebraischen Geometrie ist die nach der Anzahl rationaler Kurven mit bestimmten Zusatzbedingungen. Diese Frage haben Physiker im Rahmen der Stringtheorie gestellt, einem Versuch, die allgemeine Relativitätstheorie und die Quantenmechanik in einem allgemeineren Ansatz zu vereinen. Die Physiker haben die Zahlen auch berechnet, ohne daß jemand zu diesem Zeitpunkt in der Lage gewesen wäre, zu beweisen, daß oder weshalb ihr Ergebnis korrekt sein sollte. Dies hat zur Entwicklung einer völlig neuen Theorie innerhalb der Mathematik geführt, in der die Begriffe Gromov-Witten Invarianten und Mirrorsymmetrie eine wesentliche Rolle spielen. Für unsere Belange handelt es sich bei den Gromov-Witten Invarianten genau um die Anzahl an rationalen Kurven. Für Kurven vom Grad drei in der Ebene können wir sie beantworten.

Eine ebene projektive Kurve vom Grad drei hat eine Gleichung der Form

$$F = \sum_{0 \leq i+j \leq 3} a_{ij} x^i y^j z^{3-i-j} = 0$$

mit zehn Parametern a_{ij} . Wie oben gesehen können wir die Familie aller ebenen projektiven Kurven vom Grad drei deshalb mit dem projektiven Raum $\mathbb{P}_{\mathbb{C}}^9$ identifizieren, wobei unsere Koordinaten durch

$$(a_{ij} \mid 0 \leq i + j \leq 3)$$

gegeben sind. Ein Punkt $P = (a : b : c)$ ist nun genau dann ein singulärer Punkt von $V(F)$, wenn

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

Aus der Euler-Formel (vgl. Aufgabe 6.12)

$$3 \cdot F = x \cdot \frac{\partial F}{\partial x}(P) + y \cdot \frac{\partial F}{\partial y}(P) + z \cdot \frac{\partial F}{\partial z}(P)$$

ergibt sich dabei automatisch, daß dann auch $F(P) = 0$ gilt. Fassen wir die Parameter a_{ij} wieder als Veränderliche auf, so beschreiben uns die drei Gleichungen

$$\begin{aligned} \frac{\partial F}{\partial x}(x, y, z) &= 0, \\ \frac{\partial F}{\partial y}(x, y, z) &= 0, \\ \frac{\partial F}{\partial z}(x, y, z) &= 0. \end{aligned}$$

eine algebraische Varietät im $\mathbb{P}_{\mathbb{C}}^2 \times \mathbb{P}_{\mathbb{C}}^9$ mit den Koordinaten

$$((x : y : z), (a_{ij} \mid 0 \leq i + j \leq 3)).$$

Projizieren wir diese Varietät auf die letzten zehn Koordinaten, d.h. eliminieren wir die Variablen x, y, z , so erhalten wir eine Teilvarietät W des Parameterraumes $\mathbb{P}_{\mathbb{C}}^9$. Dabei liegt ein Punkt $(a_{ij} \mid 0 \leq i + j \leq 3)$ genau dann auf dieser Varietät, wenn die zugehörige Kurve F einen singulären Punkt besitzt.

Wir können die notwendige Elimination mit SINGULAR durchführen und erhalten binnen weniger Sekunden das Ergebnis. Die Elimination liefert uns in diesem Fall ein einziges homogenes Polynom Δ , das die *Diskriminante* der Familie von Kubiken genannt wird, da es genau die Kubiken beschreibt, die singulär sind. Das Polynom hat 2040 Summanden und in kleiner Schriftart füllt es etwa 27 Seiten. Dennoch hilft es uns ohne weiteres Zutun, unsere Eingangsfrage zu beantworten. Dazu müssen wir nur wissen, daß dieses Polynom den Grad 12 besitzt!

Wie wir oben bereits gesehen haben, liefert die Bedingung, daß eine Kurve F durch einen Punkt P geht, eine lineare Bedingung, d.h. eine *Hyperebene* in unserem Raum $\mathbb{P}_{\mathbb{C}}^2$ der Kurven. Legen wir acht Punkte fest, so erhalten wir acht Hyperebenen im $\mathbb{P}_{\mathbb{C}}^2$ und diese scheiden sich in einer projektiven Geraden – algebraisch heißt dies, wir haben acht Gleichungen bei zehn Unbekannten und erhalten eine Ursprungsebene. Eine Gerade schneidet nach dem allgemeinen Satz von Bézout 4.22 die Hyperfläche vom Grad 12 aber genau in 12 Punkten. Dies beweist die folgende Aussage.

Durch acht Punkte in der projektiven Ebene gehen im allgemeinen genau zwölf rationale Kurven vom Grad drei.

Example 6.6

Wir wollen nun ein Beispiel mit Singular rechnen. Wir geben uns hierfür die folgenden acht Punkte vor:

$$P_1 = (-1 : 0 : 1), \quad P_2 = \left(\frac{21}{100} : \frac{231}{1000} : 1\right), \quad P_3 = \left(\frac{62}{100} : -\frac{897}{1000} : 1\right), \quad P_4 = \left(\frac{7}{9} : \frac{28}{27} : 1\right), \\ P_5 = \left(\frac{5}{4} : -\frac{15}{8} : 1\right), \quad P_6 = (3 : 6 : 1), \quad P_7 = (8 : -24 : 1), \quad P_8 = (80 : 720 : 1).$$

Für unsere Rechnungen können wir bezüglich z dehomogenisieren, da alle Punkte in der affinen Karte $\{z = 1\}$ liegen. D.h. wir setzen in allen Rechnungen $z = 1$.

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
// Wir laden zunaechst zwei Bibliotheken, die wir benoetigen.
LIB "poly.lib"; // stellt den Befehl substitute zur Verfuegung
LIB "solve.lib"; // stellt den Befehl solve zur Verfuegung
// Dann sorgen wir dafuer, dass Singular die Variablen x und y
// sowie die Parameter aij fuer 0<=i+j<=3 kennt.
ring r=0,(x,y,a00,a10,a01,a20,a11,a02,a30,a21,a12,a03),dp;
// Nun definieren wir das allgemeine Polynom vom Grad 3 in x und y.
poly f=a00+a10*x+a01*y+a20*x2+a11*xy+a02*y2+a30*x3+a21*x2y+a12*xy2+a03*y3;
// Das Ideal I enthaelt f und seine beiden partiellen Ableitungen.
ideal I=f,diff(f,x),diff(f,y);
// Wir eliminieren die Variablen x und y aus dem Ideal I und erhalten ein

```

```

// Ideal, das von einem Polynom erzeugt wird, von der Diskriminante Delta.
ideal J=eliminate(I,xy);
// Setzen wir nun in f fuer x und y nacheinander die vorgegebenen acht
// Punkte ein, so erhalten wir acht lineare Gleichungen in den aij.
poly g1=substitute(f,x,-1,y,0);
poly g2=substitute(f,x,21/100,y,231/1000);
poly g3=substitute(f,x,69/100,y,-897/1000);
poly g4=substitute(f,x,7/9,y,28/27);
poly g5=substitute(f,x,5/4,y,-15/8);
poly g6=substitute(f,x,3,y,6);
poly g7=substitute(f,x,8,y,-24);
poly g8=substitute(f,x,80,y,720);
// Die Diskriminante und die acht linearen Gleichungen stecken wir
// in ein Ideal. Darin kommen die Variablen x und y nicht mehr vor.
ideal II=J[1],g1,g2,g3,g4,g5,g6,g7,g8;
// Dann teilen wir Singular mit, dass wir kuenftig
// x und y nicht mehr benoetigen.
ring R=0,(a00,a10,a01,a20,a11,a02,a30,a21,a12,a03),dp;
// Aber wir benoetigen das Ideal II weiterhin.
ideal II=imap(r,II);
// Wir suchen konkrete Werte fuer die aij, so dass die gegebenen acht
// Punkte auf den zugehoerigen Kurven V(f) liegen und dass diese
// einen Doppelpunkt besitzen. Die Kurve V(f) legt das Polynom f nur
// bis auf ein Vielfaches fest. Um es eindeutig zu machen, verlangen
// wir, dass a00+a10+a01+a20+a11+a02+a30+a21+a12+a03=1 gelten soll.
// Wir muessen deshalb das Polynom
// a00+a10+a01+a20+a11+a02+a30+a21+a12+a03-1 zum Ideal II hinzufuegen.
II=II,a00+a10+a01+a20+a11+a02+a30+a21+a12+a03-1;
// Dann berechnen wir die Loesungen mit Hilfe der Prozedur solve.
// Es wird eine Liste mit zweielf Eintraegen angezeigt, bei der jeder
// Listeneintrag aus einer Liste mit zehn komplexen Zahlen besteht.
// Setzen wir diese fuer die aij ein (in der Reihenfolge
// a00,a10,a01,a20,a11,a02,a30,a21,a12,a03), so gibt uns jeder der
// zweielf Listeneintraege ein Polynom f und eine dazugehoerige Kurve.
// Man beachte, dass die Koeffizienten hier nur naeherungsweise
// berechnet wurden und dass einige der Kurven nicht ueber den reellen
// Zahlen definiert sind, d.h. dass die Koeffizienten nicht alle
// reelle Zahlen sind. -- In der Tat sind es nur die ersten acht,
// und die vierte hat sogar rationale Koeffizienten.
solve(II);
[1]:
  [1]:
    -1.63080386
  [2]:
    4.43203885

```

[3]:
 4.9211745
 [4]:
 3.641077
 [5]:
 -9.10592967
 [6]:
 -3.37535922
 [7]:
 -2.42176574
 [8]:
 3.6495001
 [9]:
 1.04150386
 [10]:
 -0.15143581

[2]:

.
 .
 .

[4]:

[1]:
 0
 [2]:
 0
 [3]:
 0
 [4]:
 1
 [5]:
 0
 [6]:
 -1
 [7]:
 1
 [8]:
 0
 [9]:
 0
 [10]:
 0

.
 .
 .

[8]:

[1]:
4.16239888

[2]:
-11.31216

[3]:
-12.56061

[4]:
-5.74097979

[5]:
23.24161258

[6]:
5.06277236

[7]:
9.73357872

[8]:
-9.31483885

[9]:
-2.658293

[10]:
0.38651873

[9]:

[1]:
(-0.054163506+i*0.072090806)

.

.

.

[12]:

[1]:
(1.11803594-i*0.38217008)

[2]:
(-3.03848848+i*1.03862438)

[3]:
(-3.37382693+i*1.15325068)

[4]:
(-0.81065244+i*0.61892213)

[5]:
(6.24278426-i*2.13392547)

[6]:
(0.62848338-i*0.55665261)

[7]:
(3.345872-i*0.80187233)

[8]:
(-2.50200063+i*0.85524065)

[9]:
(-0.71402747+i*0.24407081)

[10]:

(0.10382038-i*0.035488164)

Die Singularrechnung liefert uns acht Kubiken mit reellen Koeffizienten, die durch die vorgegebenen Punkte P_1, \dots, P_8 gehen und singularär sind. Die Koeffizienten sind nur näherungsweise gegeben, aber für unsere Zwecke der Visualisierung reicht das aus. Die Gleichung der ersten Kubik lautet näherungsweise:

$$\begin{aligned} f_1 = & -1.63080386 \cdot z^3 + 4.43203885 \cdot xz^2 + 4.9211745 \cdot yz^2 \\ & + 3.641077 \cdot x^2z - 9.10592967 \cdot xyz - 3.37535922 \cdot y^2z - 2.42176574 \cdot x^3 \\ & + 3.6495001 \cdot x^2y + 1.04150386 \cdot xy^2 - 0.15143581 \cdot y^3 \end{aligned}$$

Das Polynom der vierten Kurve hat rationale Koeffizienten und lautet:

$$f_4 = x^2z - y^2z + x^3.$$

Die beiden Kurven sind in Abbildung 37 zu sehen. Die schwarze Kurve ist $V(f_4)$ und ist ein Newtonscher Knoten; die rote Kurve ist $V(f_1)$. Der Satz von Bézout sagt, daß sie den Newtonschen Knoten in insgesamt neun Punkten schneiden muß. Acht der Punkte sind die Punkte P_1, \dots, P_8 , und acht Schnittpunkte kann man in der Abbildung bei genauem Hinsehen auch finden. Der neunte ist verdeckt. Wir können

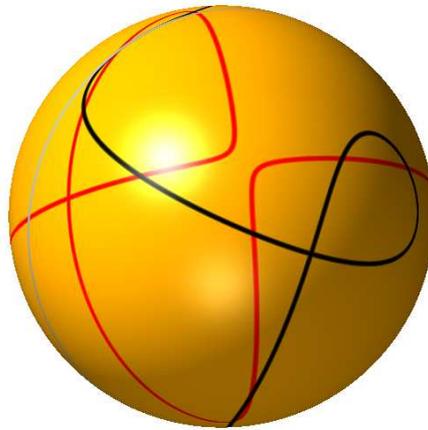


ABBILDUNG 37. Der Schnitt der Kubiken $V(f_1)$ und $V(f_4)$

in dieses Bild auch die achte Kurve einzeichnen:

$$\begin{aligned} f_8 = & 4.16239888 \cdot z^3 - 11.31216 \cdot xz^2 - 12.56061 \cdot yz^2 \\ & - 5.74097979 \cdot x^2z + 23.24161258 \cdot xyz + 5.06277236 \cdot y^2z + 9.73357872 \cdot x^3 \\ & - 9.31483885x^2y - 2.658293 \cdot xy^2 + 0.38651873 \cdot y^3. \end{aligned}$$

Dann erhalten wir Abbildung 38. Man beachte, daß die drei Kubiken in der Tat nur gemeinsame Schnittpunkte haben.

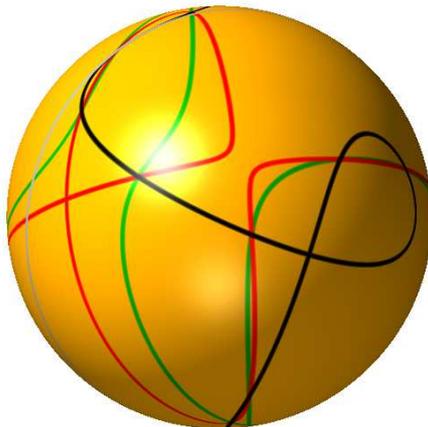


ABBILDUNG 38. Der Schnitt der Kubiken $V(f_1)$, $V(f_4)$ und $V(f_8)$

Die zwölf Kubiken, die wir in unserem Beispiel konstruiert haben, sind irreduzibel, und damit sind sie rational, wie wir aus Satz 6.4 wissen.

Wenn man sich acht Punkte vorgibt und die singulären Kubiken, die durch diese acht Punkte gehen, mit der richtigen Vielfachheit zählt, so ist ihre Anzahl immer zwölf. Geben wir uns etwa die Punkte

$$\begin{aligned} P_1 &= (3 : 6 : 1), & P_2 &= (3 : -6 : 1), & P_3 &= (8 : 24 : 1), & P_4 &= (8 : -24 : 1), \\ P_5 &= (15 : 60 : 1), & P_6 &= (15 : -60 : 1), & P_7 &= (24 : 120 : 1), & P_8 &= (24 : -120 : 1) \end{aligned}$$

vor, so kann man auf die gleiche Weise feststellen, daß es nur sieben singuläre Kubiken durch diese acht Punkte gibt. Eine besitzt jedoch die Vielfachheit drei, drei besitzen die Vielfachheit zwei und drei müssen einfach gezählt werden. Insgesamt ergeben sich also

$$1 \cdot 3 + 3 \cdot 2 + 3 \cdot 1 = 12$$

Kubiken. Die Vielfachheiten kommen letztlich aus dem Satz von Bézout. Es empfiehlt sich, das Beispiel zu rechnen, denn die sieben Gleichungen, die man erhält haben sämtlich reelle Koeffizienten, ja, bis auf zwei haben sie sogar alle rationale Koeffizienten.

Ein weiteres Beispiel von drei singulären Kubiken durch acht vorgegebene Punkte ist in Abbildung 39 zu sehen. Dieses Beispiel kommt aus Aufgabe 6.13. Hier sind die Kubiken nicht irreduzibel, sondern zerfallen jeweils in eine Quadrik und eine Gerade. Die Kubiken sind nicht rational! Die Punkte in diesem Beispiel sind nicht hinreichend allgemein gewählt, sonst müßten die Kubiken irreduzibel sein — hinreichend allgemein würde in diesem Zusammenhang bedeuten, daß keine vier auf einer Geraden und keine sieben auf einer Quadrik liegen dürfen (vgl. auch Lemma 6.8).

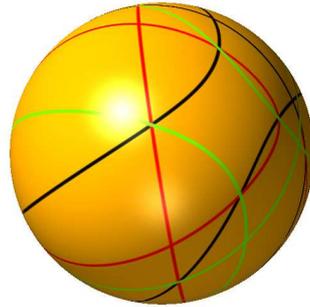


ABBILDUNG 39. Drei singuläre Kubiken durch acht vorgegebene Punkte

D) Kubische Flächen mit 27 Geraden

In diesem Abschnitt arbeiten wir wieder über dem Körper der komplexen Zahlen \mathbb{C} , um den Satz von Bézout in seiner vollen Allgemeinheit anwenden zu können.

Bislang haben wir nur Punkte gezählt, die wir als Schnittpunkte von Kurven erhalten haben, sowie Kurven die durch vorgegebene Punkte gingen. Die geometrischen Objekte und Bedingungen waren also stets null- oder eindimensional. Ein klassisches Ergebnis der algebraischen Geometrie des neunzehnten Jahrhunderts wählt eine zweidimensionale Bedingung.

Eine Fläche $V \subset \mathbb{P}_{\mathbb{C}}^3$ vom Grad drei enthält im allgemeinen genau 27 Geraden, wenn man sie mit Vielfachheit zählt.

Die Aussage ist auf den ersten Blick überraschend. Die projektive Ebene enthält unendlich viele Geraden. Und schauen wir uns etwa die Fläche

$$V(xw - zy) \subset \mathbb{P}_{\mathbb{C}}^3$$

vom Grad zwei mit Koordinaten w, x, y, z an, dann enthält diese zwei Scharen paralleler Geraden⁷ (siehe Abbildung 40). Es darf also verwundern, daß es im Grad drei nur noch endlich viele solcher Geraden geben soll.

⁷Eine Gerade im $\mathbb{P}_{\mathbb{C}}^3$ ist durch zwei lineare Gleichungen gegeben. Wählen wir eine Zahl k , so liefern die zwei Gleichungen

$$x = k \cdot y \quad \text{und} \quad z = k \cdot w$$

eine Gerade, und zwei verschiedene Werte für k liefern zwei parallele Geraden. Wir erhalten also eine Parallelschar von Geraden. Die Gleichungen

$$x = k \cdot z \quad \text{und} \quad y = k \cdot w$$

für $k \in \mathbb{C}$ definieren analog eine zweite Parallelschar von Geraden. Außerdem liegen diese Geraden offensichtlich alle auf der Fläche $V(xw - yz)$, da ihre Punkte die Gleichung $xw - yz = 0$ erfüllen. Um die Fläche zu visualisieren und ein schönes Bild zu erhalten, wenden wir zunächst

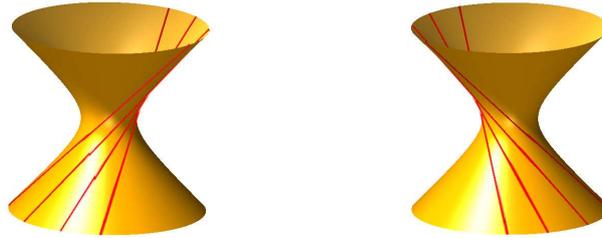


ABBILDUNG 40. Eine Quadrik mit zwei Parallelenscharen von Geraden

Alfred Clebsch hat 1861 (siehe [Cle61]) zu gegebener Fläche $V(F) \subset \mathbb{P}_{\mathbb{C}}^3$ vom Grad drei ein homogenes Polynom G vom Grad 9 in den Koordinaten w, x, y, z mit der Eigenschaft gefunden, daß der Schnitt von $V(F)$ und $V(G)$ genau aus den Geraden auf $V(F)$ besteht. Der allgemeine Satz von Bézout 4.20 sagt dann aber, daß der Schnitt $V(F) \cap V(G)$ eine Kurve vom Grad $\deg(F) \cdot \deg(G) = 3 \cdot 9 = 27$ ist. Wenn sie nur aus Geraden besteht, so müssen es 27 Geraden sein.

Eine Fläche vom Grad drei im $\mathbb{P}_{\mathbb{C}}^3$ ist durch ein Polynom mit fünfzehn Koeffizienten gegeben, so daß der Parameterraum der Bedingungen ein projektiver Raum der Dimension fünfzehn ist. Die Menge der Parameter, für die manche der Geraden auf der Fläche mehrfach gezählt werden müssen, hat niedrigere Dimension. Das Polynom G , das Clebsch gefunden hat, kann man in Abhängigkeit der Parameter angeben, so daß es für alle Flächen zugleich funktioniert.

Es ist eine Menge über die möglichen Lagen der Geraden zueinander bekannt, etwa daß keine vier der Geraden durch einen Punkte gehen können. Für mehr Information

eine Koordinatentransformation an, die durch die Matrix

$$A = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

gegeben wird, d.h. durch

$$w \mapsto x - w, \quad x \mapsto x + w, \quad y \mapsto z - y, \quad z \mapsto z + y.$$

Die Gleichung der Fläche wird dann

$$x^2 + y^2 - z^2 - w^2 = 0$$

und die Parallelenscharen von Geraden werden gegeben durch

$$x + w = k \cdot (z - y) \quad \text{und} \quad z + y = k \cdot (x - w)$$

bzw. durch

$$x + w = k \cdot (z + y) \quad \text{und} \quad z - y = k \cdot (x - w).$$

Nach dieser Koordinatentransformation können wir die Fläche in der affinen Karte betrachten, die durch $w = 1$ gegeben wird. Das linke Bild in Abbildung 40 zeigt die Fläche $V(x^2 + y^2 - z^2 - 1)$ mit einigen Geraden der ersten Parallelenschar, das rechte Bild zeigt die Fläche mit einigen Geraden der zweiten Parallelenschar.

hierzu sowie einen alternativen Beweis sei auf die Diplomarbeit von Oliver Labs [Lab01] verwiesen.

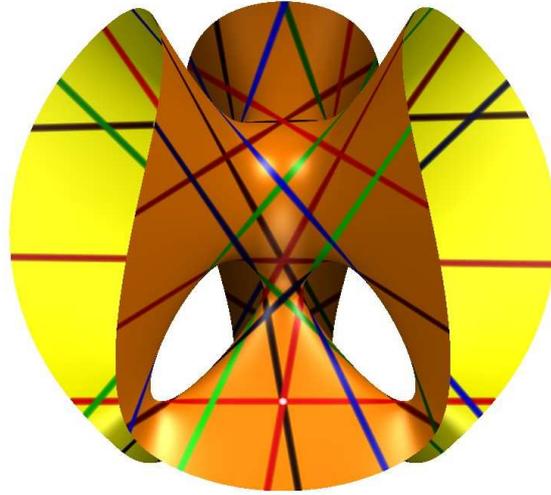


ABBILDUNG 41. Die Kubik von Clebsch mit ihren 27 Geraden:

$$x^3 + y^3 + z^3 + w^3 - (x + y + z + w)^3 = 0$$

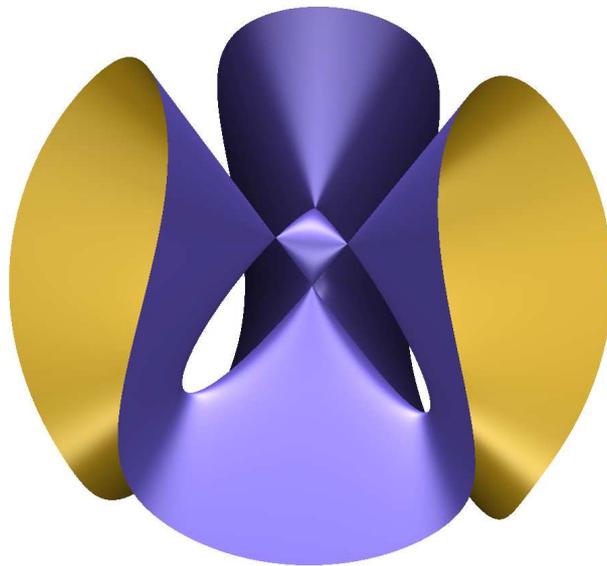


ABBILDUNG 42. Die Kubik von Cayley mit vier Doppelpunkten und 9 Geraden, von denen 6 mit Vielfachheit 4 gezählt werden:

$$x^3 + y^3 + z^3 + w^3 - \frac{1}{4} \cdot (x + y + z + w)^3 = 0$$

Zum Abschluß dieses Abschnitts wollen wir eine Definition der Covariante von Clebsch angeben sowie eine SINGULAR -Prozedur, mit deren Hilfe man die Covariante für ein gegebenes Polynom F ausrechnen kann. Wir folgen dabei der Beschreibung in [LvS03]. Um angenehmere Formeln zu haben, verwenden wir für die Variablen die Bezeichnungen x_1, x_2, x_3, x_4 anstatt w, x, y, z . Sei also $F \in \mathbb{C}[x_1, x_2, x_3, x_4]$ ein homogenes Polynom vom Grad drei. Die 4×4 -Matrix

$$H_F = \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{i,j=1,\dots,4}$$

heißt *Hesse-Matrix* des Polynoms F und hat als Einträge die zweiten partiellen Ableitungen von F . Mithin sind die Einträge der Hesse-Matrix homogene Polynome vom Grad eins. Wir setzen

$$\Delta_F = \det(H_F),$$

die Determinante der Hesse-Matrix. Sie ist ein homogenes Polynom vom Grad vier. Ferner wollen wir für die ersten und zweiten partiellen Ableitungen von Δ_F eine Bezeichnung einführen:

$$\Delta_{F,i} = \frac{\partial \Delta_F}{\partial x_i}$$

und

$$\Delta_{F,i,j} = \frac{\partial^2 \Delta_F}{\partial x_i \partial x_j}.$$

Damit sind $\Delta_{F,i}$ und $\Delta_{F,i,j}$ homogene Polynome vom Grad drei bzw. vom Grad zwei. Schließlich benötigen wir noch die Adjunkte von H_F . Es handelt sich dabei um eine 4×4 -Matrix A_F , deren Eintrag an der Stelle (i, j) sich errechnet als

$$A_{F,i,j} = (-1)^{i+j} \cdot \det(S(H_F, j, i)),$$

wobei die Matrix $S(H_F, j, i)$ aus der Matrix H_F durch die Streichung der j -ten Zeile und der i -ten Spalte entsteht. Die Adjunkte ist aus der linearen Algebra bekannt, wo sie im Zusammenhang mit dem *Determinanten-Entwicklungssatz* und mit der *Cramerschen Regel* zum Lösen linearer Gleichungssysteme auftritt. Die Einträge der Adjunkten A_F sind also homogene Polynome vom Grad drei.

Mit diesen Bezeichnungen erhalten wir die Covariante von Clebsch als

$$G = \sum_{i=1}^4 \sum_{j=1}^4 A_{F,i,j} \cdot (\Delta_{F,i} \cdot \Delta_{F,j} - 4 \cdot \Delta_F \cdot \Delta_{F,i,j}).$$

Damit ist G wie oben erwähnt ein homogenes Polynom vom Grad neun.

Die folgende SINGULAR -Prozedur nimmt ein homogenes Polynom F vom Grad drei als Eingabe und berechnet für dieses die Covariante von Clebsch. Will man die Prozedur anwenden, so muß man zunächst die Bibliothek `linalg.lib` laden, da diese zum Berechnen der Adjunkten benötigt wird. Die Variablen dürfen aber beliebige Namen haben, und wir empfehlen der Einfachheit halber die Namen w, x, y, z . Dann kann man sich anschließend durch Substitution von $w = 1$ auch eine affine Gleichung

der Covariante in der affinen Karte $\{w = 1\}$ beschaffen, die mit Hilfe von `Surfex` visualisiert werden kann.

```
LIB "linalg.lib";
proc covariante (poly F)
{
  matrix H=jacob(jacob(F)); // die Hesse-Matrix
  poly D=det(H);           // die Determinante der Hesse-Matrix
  int i,j;
  matrix A=adjoint(H);     // die Adjunkte der Hesse-Matrix
  poly G;
  for (i=1;i<=4;i++)
  {
    for (j=1;j<=4;j++)
    {
      G=G+A[i,j]*(diff(D,var(i))*diff(D,var(j))
                  -4*D*diff(diff(D,var(i)),var(j)));
    }
  }
  G=G/content(G); // teile die Koeffizienten von G durch ihren ggT
  return(G);
}
```

Ein Beispiel zur Anwendung der Prozedur zwecks Berechnung der Covariante für die Cayley-Kubik sieht wie folgt aus.

```
> LIB "linalg.lib";
> ring r=0,(w,x,y,z),dp;
> poly F=x^3+y^3+z^3+w^3-1/4*(x+y+z+w)^3;
> poly G=covariante(F); // berechne die Covariante
> short=0;             // Ausgabe soll * und ^ enthalten
> subst(G,w,1);        // substituiere w=1 in G
x^6*y^2*z-2*x^4*y^4*z+x^2*y^6*z+x^6*y*z^2+4*x^5*y^2*z^2+7*x^4*
y^3*z^2+7*x^3*y^4*z^2+4*x^2*y^5*z^2+x*y^6*z^2+7*x^4*y^2*z^3+14
*x^3*y^3*z^3+7*x^2*y^4*z^3-2*x^4*y*z^4+7*x^3*y^2*z^4+7*x^2*y^3
*z^4-2*x*y^4*z^4+4*x^2*y^2*z^5+x^2*y*z^6+x*y^2*z^6+x^6*y^2-2*x
^4*y^4+x^2*y^6+2*x^6*y*z+8*x^5*y^2*z+14*x^4*y^3*z+14*x^3*y^4*z
+8*x^2*y^5*z+2*x*y^6*z+x^6*z^2+8*x^5*y*z^2+20*x^4*y^2*z^2+26*x
^3*y^3*z^2+20*x^2*y^4*z^2+8*x*y^5*z^2+y^6*z^2+14*x^4*y*z^3+26*
x^3*y^2*z^3+26*x^2*y^3*z^3+14*x*y^4*z^3-2*x^4*z^4+14*x^3*y*z^4
+20*x^2*y^2*z^4+14*x*y^3*z^4-2*y^4*z^4+8*x^2*y*z^5+8*x*y^2*z^5
+x^2*z^6+2*x*y*z^6+y^2*z^6+x^6*y+4*x^5*y^2+7*x^4*y^3+7*x^3*y^4
+4*x^2*y^5+x*y^6+x^6*z+8*x^5*y*z+20*x^4*y^2*z+26*x^3*y^3*z+20*
x^2*y^4*z+8*x*y^5*z+y^6*z+4*x^5*z^2+20*x^4*y*z^2+46*x^3*y^2*z^
2+46*x^2*y^3*z^2+20*x*y^4*z^2+4*y^5*z^2+7*x^4*z^3+26*x^3*y*z^3
+46*x^2*y^2*z^3+26*x*y^3*z^3+7*y^4*z^3+7*x^3*z^4+20*x^2*y*z^4+
```

$$\begin{aligned}
&20*x*y^2*z^4+7*y^3*z^4+4*x^2*z^5+8*x*y*z^5+4*y^2*z^5+x*z^6+y*z \\
&^6+7*x^4*y^2+14*x^3*y^3+7*x^2*y^4+14*x^4*y*z+26*x^3*y^2*z+26*x \\
&^2*y^3*z+14*x*y^4*z+7*x^4*z^2+26*x^3*y*z^2+46*x^2*y^2*z^2+26*x \\
&*y^3*z^2+7*y^4*z^2+14*x^3*z^3+26*x^2*y*z^3+26*x*y^2*z^3+14*y^3 \\
&*z^3+7*x^2*z^4+14*x*y*z^4+7*y^2*z^4-2*x^4*y+7*x^3*y^2+7*x^2*y^ \\
&3-2*x*y^4-2*x^4*z+14*x^3*y*z+20*x^2*y^2*z+14*x*y^3*z-2*y^4*z+7 \\
&*x^3*z^2+20*x^2*y*z^2+20*x*y^2*z^2+7*y^3*z^2+7*x^2*z^3+14*x*y* \\
&z^3+7*y^2*z^3-2*x*z^4-2*y*z^4+4*x^2*y^2+8*x^2*y*z+8*x*y^2*z+4* \\
&x^2*z^2+8*x*y*z^2+4*y^2*z^2+x^2*y+x*y^2+x^2*z+2*x*y*z+y^2*z+x* \\
&z^2+y*z^2
\end{aligned}$$

Dieses Polynom kann man `Surfex` übergeben und den Schnitt mit der Kubik zeichnen lassen. Man beachte, daß man in `SINGULAR` die obige Prozedur zunächst definieren muß, d.h. den obigen Quelltext der Prozedur eingeben muß, bevor man sie aufrufen kann!

Das Ergebnis (siehe Abbildung 43) ist allerdings nicht sehr zufriedenstellend. Der

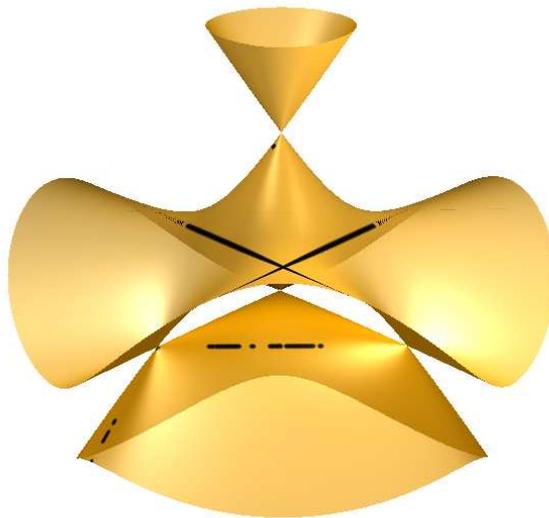


ABBILDUNG 43. Cayley-Kubik geschnitten mit der Covariante von Clebsch

Schnitt einer Kubik mit einer Kurve vom Grad neun ist für die Visualisierung eine schwierige Angelegenheit. Man kann das Ergebnis dadurch verbessern, daß man die Gleichungen für die Geraden ausrechnet und sie einzeln einzeichnen läßt. Eine Gerade im dreidimensionalen Raum ist durch zwei lineare Gleichungen gegeben. Man kann diese durch *Primärzerlegung* ausrechnen lassen.

```

> LIB "primdec.lib";
> poly F=x^3+y^3+z^3+w^3-1/4*(x+y+z+w)^3;
> poly G=covariante(G);
> ideal I=F,G;
> list PD=primdecGTZ(I);

```

```

> size(I); // gibt an, wie viele Komponenten gefunden wurden
9
> for (int i=1;i<=size(PD);i++)
. {
.   string(i)+"-te Komponente";
.   PD[i][2];           // gibt die ite Komponente aus
.   "Vielfachheit: ",
.   deg(std(PD[i][1])); // berechnet die Vielfachheit der iten Komponente
. }
1-te Komponente
_[1]=x+y
_[2]=w+z
Vielfachheit: 1
2-te Komponente
_[1]=x-y
_[2]=w+z
Vielfachheit: 4
3-te Komponente
_[1]=y+z
_[2]=w+x
Vielfachheit: 1
4-te Komponente
_[1]=y-z
_[2]=w+x
Vielfachheit: 4
5-te Komponente
_[1]=x+y
_[2]=w-z
Vielfachheit: 4
6-te Komponente
_[1]=y+z
_[2]=w-x
Vielfachheit: 4
7-te Komponente
_[1]=x-z
_[2]=w+y
Vielfachheit: 4
8-te Komponente
_[1]=x+z
_[2]=w+y
Vielfachheit: 1
9-te Komponente
_[1]=x+z
_[2]=w-y
Vielfachheit: 4

```

Die Primärzerlegung liefert uns die Gleichungen der neun Geraden und gibt uns für jede der neun Geraden an, mit welcher Vielfachheit sie gezählt werden muß. Die erste Gerade erhalten wir etwa als Lösungsmenge des Gleichungssystems

$$x + y = 0 \quad \text{und} \quad w + z = 0$$

und sie hat Vielfachheit eins. Wenn wir sie in der Karte $\{w = 1\}$ mit **Surfex** zeichnen, so erhalten wir Abbildung 44.

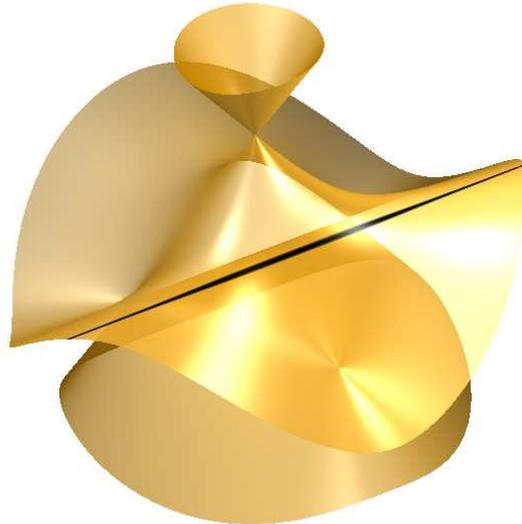


ABBILDUNG 44. Cayley-Kubik geschnitten mit der Covariante von Clebsch

Das Primärzerlegung wird im allgemeinen nicht so problemlos funktionieren. Für die Cayley-Kubik haben die Gleichungen der Geraden rationale Koeffizienten, was im allgemeinen nicht mehr der Fall ist. Dann muß man den Befehl `primdecGTZ` durch `absPrimdecGTZ` ersetzen und erhält Koeffizienten, die von einem Parameter abhängen. Bei diesem Parameter handelt es sich um eine algebraische Zahl, d.h. um die Nullstelle eines Polynoms in einer Veränderlichen. Das Polynom wird ebenfalls angegeben. Man kann eine numerische Approximation an die Nullstelle ausrechnen, z.B. mit `solve` aus `solve.lib`. Das sollte für die Visualisierung mit **Surfex** hinreichend sein. Die Rechnungen werden dann allerdings recht komplex und man muß etwas Geduld mitbringen.

E) Satz von Pappos

In diesem Abschnitt arbeiten wir über dem Körper der reellen Zahlen \mathbb{R} .

Der Satz von Pappos ist eine bereits in der Antike bekannte Aussage der Elementargeometrie der Ebene. Wir folgen in unserer Darstellung im wesentlichen [Rei92]. Um parallele Geraden und sich schneidende Geraden gleichzeitig behandeln zu können,

formuliert man sie sinnvollerweise gleich in der projektiven Ebene. In der Formulierung des folgenden Satzes soll für Punkte A und B in \mathbb{P}_R^2 mit \overline{AB} die Gerade bezeichnet sein, auf der A und B liegen.

Satz 6.7 (Satz von Pappos)

Es seien g und g' zwei Geraden in der projektiven Ebene, $A, B, C \in \mathbb{P}_R^2 \setminus (g \cap g')$ seien drei Punkte, die auf der Geraden g liegen, und $A', B', C' \in \mathbb{P}_R^2 \setminus (g \cap g')$ seien drei weitere Punkte, die auf einer Geraden g' liegen. Wir bilden die drei Schnittpunkte

$$P = \overline{AB'} \cap \overline{A'B}, \quad Q = \overline{BC'} \cap \overline{B'C}, \quad \text{und} \quad R = \overline{CA'} \cap \overline{C'A}.$$

Dann liegen die drei Punkte P, Q und R auf einer Geraden.

Die Voraussetzungen des Satzes sowie seine Aussage werden in den Abbildungen 45–49 veranschaulicht.

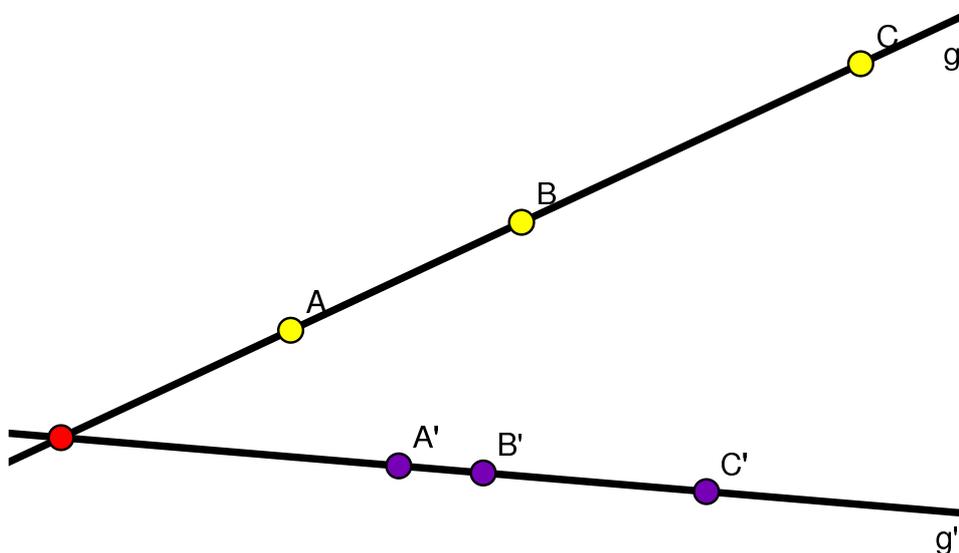


ABBILDUNG 45. g und g' mit den Punkten A, B, C sowie A', B', C'

Wir wollen in diesem Abschnitt den Satz von Pappos beweisen. Dabei werden wir die Begriffe *Quadrik* und *Kubik* immer wieder verwenden, so daß wir sie noch einmal ins Gedächtnis rufen wollen. Eine Kurve in der projektiven Ebene wird als Nullstellenmenge eines homogenen Polynoms gegeben. Hat das Polynom Grad eins, so handelt es sich um eine *Gerade*; hat es Grad zwei, so nennen wir die Kurve eine *Quadrik*; hat es Grad drei, sprechen wir von einer *Kubik*. Außerdem wollen wir uns daran erinnern, daß für die Nullstellenmenge zweier homogener Polynome F und G folgende Regel gilt:

$$V(F) \cup V(G) = V(F \cdot G).$$

Insbesondere ist also die Vereinigung dreier Geraden eine Kubik.

Die Vereinigung der drei grünen Geraden in Abbildung 47 ist also eine Kubik C , und die Vereinigung der drei roten Geraden dort ist eine weitere Kubik C' . Diese können

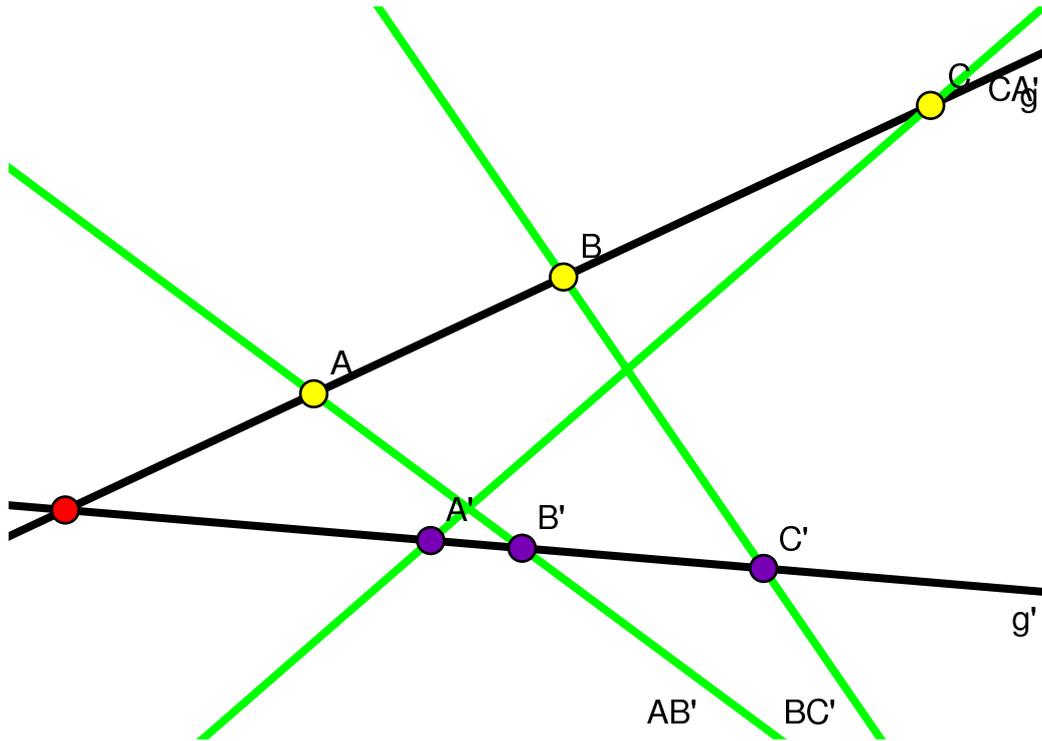


ABBILDUNG 46. Die Geraden $\overline{A B'}$, $\overline{B C'}$ und $\overline{C A'}$

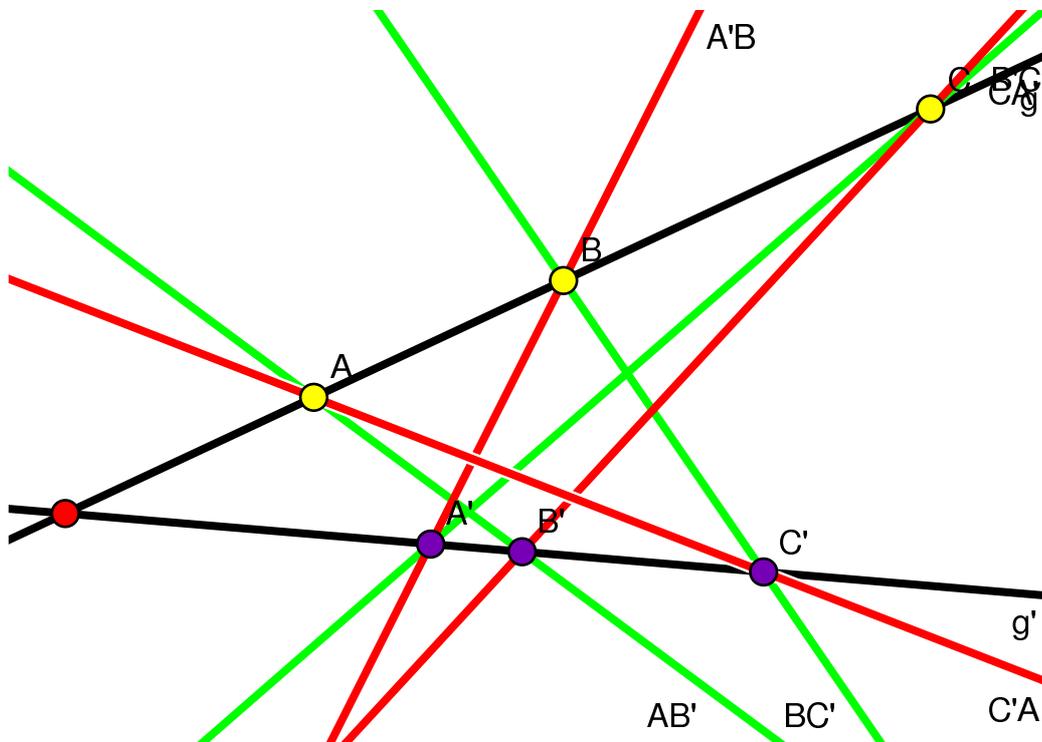


ABBILDUNG 47. Die Geraden $\overline{A B'}$, $\overline{B C'}$, $\overline{C A'}$ und $\overline{A' B}$, $\overline{B' C}$, $\overline{C' A}$

sich wegen des Satzes von Bézout 4.7 in höchstens $3 \cdot 3 = 9$ Punkten schneiden, und

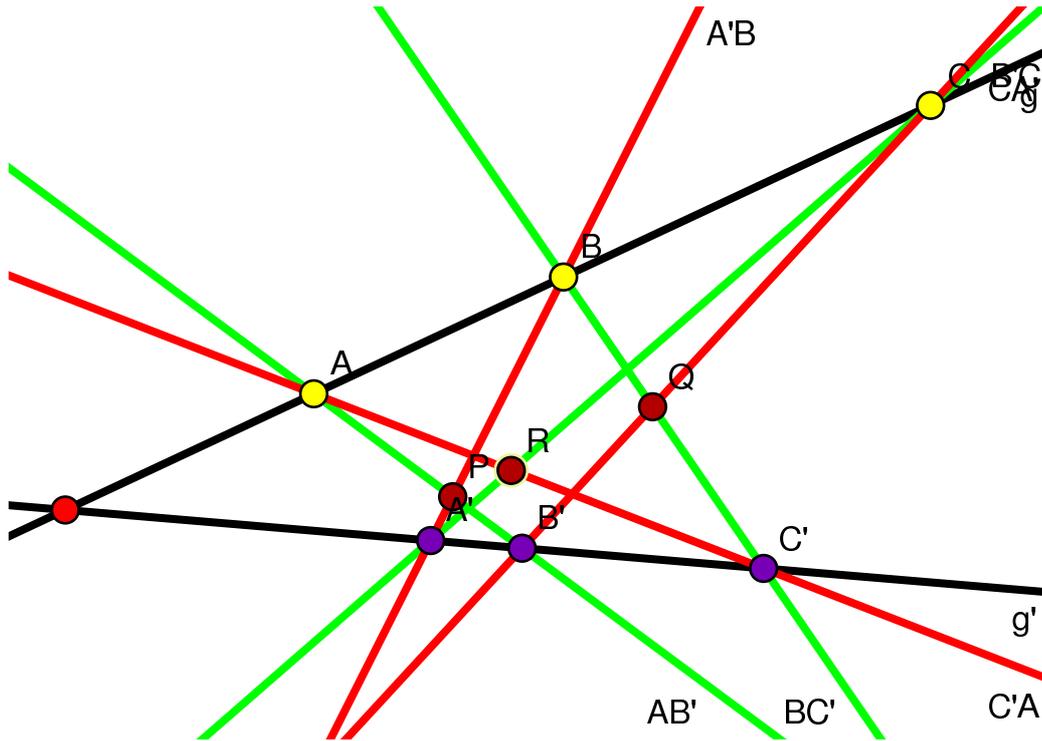


ABBILDUNG 48. Die Schnittpunkte P, Q und R.

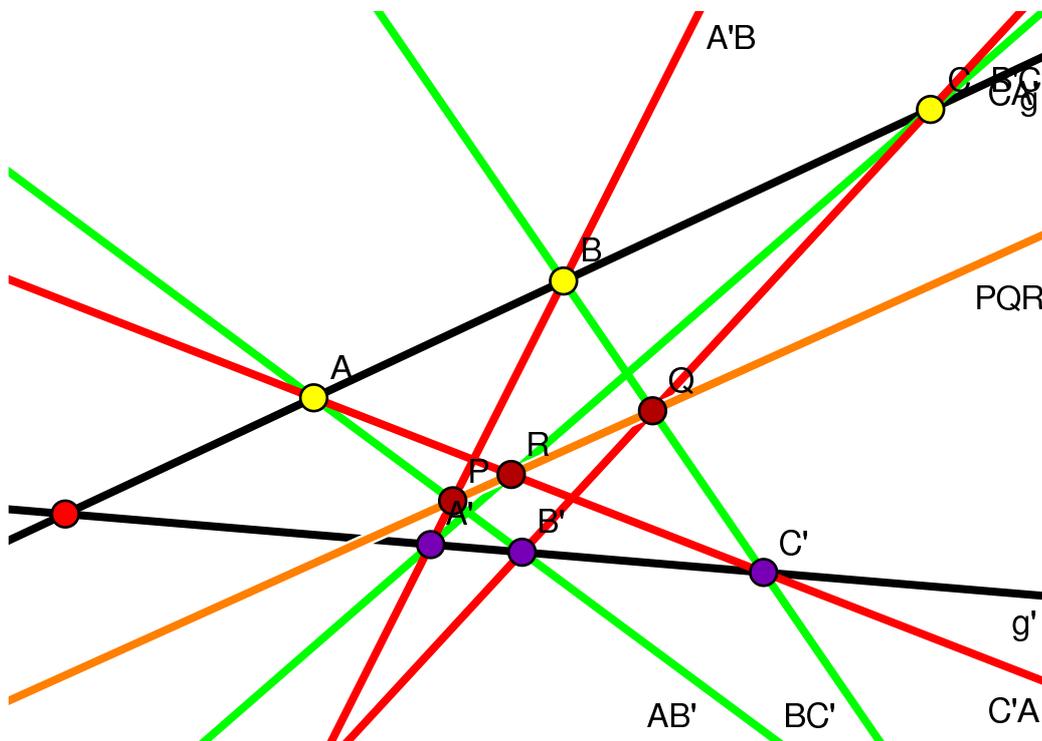


ABBILDUNG 49. P, Q und R liegen auf einer Geraden

wir sehen die Schnittpunkte in Abbildung 48:

$A, B, C, A', B', C', P, Q$ und R .

Vergessen wir für einen Augenblick, daß die orangefarbene Gerade in 49 neben P und Q auch R enthält, und betrachten wir sie nur als die durch P und Q gegebene Gerade \overline{PQ} . Dann ist die Vereinigung von g , g' und \overline{PQ} eine dritte Kubik, die mit den beiden Kubiken C und C' zumindest die acht Punkte

$$A, B, C, A', B', C', P \quad \text{und} \quad Q$$

gemeinsam hat. Wir wollen nun zeigen, daß eine Kubik, die mit zwei anderen Kubiken acht ihrer neun Schnittpunkte gemeinsam hat, automatisch auch den neunten mit ihr teilen muß. Damit ist dann der Satz von Pappos im wesentlichen ebenfalls bewiesen!

Um die Aussage zu den Kubiken beweisen zu können, schauen wir uns zunächst die Gesamtheit aller Kubiken an, die durch gegebene acht Punkte verlaufen. Dabei sollen die acht Punkte nicht zu speziell liegen, d.h. nicht zu viele sollen auf einer Geraden oder einer Quadrik liegen. Wir erinnern uns, daß für drei zufällig gewählte Punkte in der Ebene keine Gerade durch alle drei existiert und daß sich durch sechs Punkte im allgemeinen auch keine Quadrik mehr findet (siehe Seite 82).

Für das folgende Lemma wollen wir zudem dem \mathbb{R} -Vektorraum aller homogenen Polynome vom Grad drei einen Namen geben:

$$\mathbb{R}[x, y, z]_3 = \{F \in \mathbb{R}[x, y, z] \mid F \text{ ist homogen vom Grad } 3\}.$$

Wir kennen seine Dimension,

$$\dim_{\mathbb{R}} (\mathbb{R}[x, y, z]_3) = 10,$$

da ein homogenes Polynom vom Grad drei die Form

$$F = \sum_{i+j+k=3} a_{ijk} \cdot x^i \cdot y^j \cdot z^k$$

hat und es genau zehn solcher Tripel (i, j, k) gibt.

Wir werden im Beweis des Lemmas immer wieder zwischen homogenen Polynomen und den durch sie definierten Kurven wechseln müssen. Wir wollen uns deshalb daran erinnern, daß zwei homogene Polynome vom gleichen Grad genau dann die gleiche Kurve definieren, wenn sie sich nur um ein skalares Vielfaches unterscheiden. Betrachten wir also einen \mathbb{R} -Vektorraum W von homogenen Polynomen vom gleichen Grad, dann definieren diese Polynome genau dann die gleiche Kurve, wenn die Dimension von W eins ist. Ist sie echt größer als eins, dann definieren sie bereits unendlich viele verschiedene Kurven.

Ein weiteres Argument, das wir im Beweis des öfteren verwenden, kommt aus der linearen Algebra. Die Lösungsmenge eines homogenen linearen Gleichungssystems, d.h. eines Systems linearer Terme, die alle gleich null gesetzt werden, ist immer ein Vektorraum, und die Dimension des umgebenden Raumes sinkt mit jeder Gleichung um höchstens eins.

Lemma 6.8

Es seien $P_1, \dots, P_8 \in \mathbb{P}_{\mathbb{R}}^2$ acht Punkte, von denen keine vier auf einer Geraden liegen und keine sieben auf einer Quadrik. Dann hat der \mathbb{R} -Vektorraum

$$V = \{F \in \mathbb{R}[x, y, z]_3 \mid F(P_1) = \dots = F(P_8) = 0\}$$

die Dimension zwei.

Beweis: Der Vektorraum V ist als Teilmenge von $\mathbb{R}[x, y, z]_3$ durch acht homogene lineare Gleichungen beschrieben. Mithin gilt sicher

$$\dim_{\mathbb{R}}(V) \geq \dim_{\mathbb{R}}(\mathbb{R}[x, y, z]_3) - 8 = 2,$$

da jede der Gleichungen die Dimension um höchstens eins erniedrigt.

Wir nehmen nun an, die Dimension sei echt größer als zwei, und leiten einen Widerspruch her, indem wir verschiedene Fälle untersuchen.

1. Fall: Keine drei der P_i liegen auf einer Geraden und keine sechs auf einer Quadrik.

Wir betrachten die Gerade $\overline{P_1 P_2}$ und wählen zwei weitere Punkte P und R auf der Geraden. Der Vektorraum

$$W = \{F \in V \mid F(P) = F(R) = 0\}$$

ist die Lösungsmenge eines linearen Gleichungssystems mit zwei homogenen linearen Gleichungen. Mithin sinkt die Dimension von V um höchstens zwei, d.h.

$$\dim_{\mathbb{R}}(W) \geq \dim_{\mathbb{R}}(V) - 2 \geq 3 - 2 = 1.$$

Es gibt also ein homogenes Polynom F vom Grad drei mit der Eigenschaft, daß

$$F(P_1) = F(P_2) = F(P) = F(R) = 0.$$

Ist $C = V(F)$ die zugehörige Kubik, dann haben C und $\overline{P_1 P_2}$ vier Punkte gemeinsam. Wegen des Satzes von Bézout 4.7 geht das nur, wenn die Gerade $\overline{P_1 P_2}$ ganz in der Kubik C enthalten ist, d.h. es gibt eine Quadrik Q , so daß

$$C = \overline{P_1 P_2} \cup Q.$$

Da die Gerade $\overline{P_1 P_2}$ nach Voraussetzung keine drei der P_i enthält, müssen die Punkte P_3, \dots, P_8 auf Q liegen. Dies ist aber wiederum im Widerspruch zur Voraussetzung, diesmal dazu, daß keine sechs auf einer Quadrik liegen sollen.

2. Fall: Drei der P_i liegen auf einer Geraden. Wir können ohne Einschränkung annehmen, daß die Punkte P_1, P_2 und P_3 auf einer Geraden liegen, d.h. $P_3 \in \overline{P_1 P_2}$. Wählen wir nun einen weiteren Punkt P auf dieser Geraden und betrachten wir den \mathbb{R} -Vektorraum

$$W = \{F \in V \mid F(P) = 0\},$$

so gilt wie oben

$$\dim_{\mathbb{R}}(W) \geq \dim_{\mathbb{R}}(V) - 1 \geq 2,$$

da die Bedingung $F(P) = 0$ einer homogenen linearen Gleichung entspricht, die die Elemente in W erfüllen müssen. Ist F ein Polynom in W , dann schneidet die zugehörige Kurve $C = V(F)$ die Gerade $\overline{P_1 P_2}$ in den vier Punkten P_1, P_2, P_3 und P . Da C ein Kubik ist, impliziert der Satz von Bézout 4.7, daß die Gerade $\overline{P_1 P_2}$ in C enthalten ist. Es gibt also eine Quadrik Q , so daß $C = Q \cup \overline{P_1 P_2}$. Da nach Voraussetzung keine vier der Punkte P_i auf der Kubik C liegen, muß $P_4, \dots, P_8 \in Q$ gelten. Die Quadrik Q geht also durch fünf vorgegebene Punkte. Drücken wir diese Überlegungen auf der Ebene der definierenden Polynome aus und ist H ein homogenes Polynom vom Grad eins mit $V(H) = \overline{P_1 P_2}$, dann gibt es also ein homogenes Polynom G vom Grad zwei, so daß

$$F = G \cdot H,$$

und es gilt $G(P_i) = 0$ für $i = 4, \dots, 8$. Damit ist

$$W' = \left\{ \frac{F}{H} \mid F \in W \right\}$$

ein mindestens zweidimensionaler \mathbb{R} -Vektorraum von homogenen Polynomen vom Grad zwei, die alle an den fünf Punkten P_4, \dots, P_8 verschwinden. Nun definieren zwei Polynome aber nur dann die gleiche Quadrik, wenn sie sich nur um ein skalares Vielfaches unterscheiden. Der zweidimensionale Vektorraum W' von Polynomen vom Grad zwei definiert also unendlich viele Quadriken, die durch die fünf Punkte P_4, \dots, P_8 gehen. Das steht aber im Widerspruch zu Proposition 6.1, da keine vier der fünf Punkte auf einer Geraden liegen und deshalb nur eine Quadrik durch die fünf Punkte gehen kann.

3. Fall: Keine drei der P_i liegen auf einer Geraden, aber sechs der P_i liegen auf einer Quadrik. Wäre die Quadrik Q nicht irreduzibel, so wäre sie die Vereinigung zweier Geraden, von denen dann mindestens eine drei Punkte enthalten würde. Da dies ausgeschlossen wurde, muß Q irreduzibel sein. Ohne Einschränkung können wir annehmen, daß die Punkte P_1, \dots, P_6 auf der Quadrik Q liegen. Wählen wir einen weiteren Punkt P auf Q und betrachten den Vektorraum

$$W = \{F \in V \mid F(P) = 0\},$$

dann gilt wie vorher $\dim_{\mathbb{R}}(W) \geq 2$, und wegen des Satzes von Bézout 4.7 ist Q eine Komponente von $V(F)$ für alle $F \in W$, da dann $V(F)$ und Q die sieben Punkte P_1, \dots, P_6, P gemeinsam haben. Ist G ein homogenes Polynom vom Grad zwei mit $V(G) = Q$, dann ist

$$W' = \left\{ \frac{F}{G} \mid F \in W \right\}$$

ein mindestens zweidimensionaler \mathbb{R} -Vektorraum von homogenen linearen Polynomen. Zudem hat jedes der Polynome die Punkte P_7 und P_8 als Nullstellen, da diese auf $V(F)$ liegen, aber nach Voraussetzung nicht auf Q liegen können.

Wegen $\dim_{\mathbb{R}}(W') \geq 2$ müßte es also unendlich viele Geraden durch die Punkte P_7 und P_8 geben. Das ist aber offenbar falsch.

Damit haben wir den gewünschten Widerspruch hergeleitet und gezeigt, daß $\dim_{\mathbb{R}}(V) = 2$ gilt. \square

Das Lemma ist eine etwas technische Formulierung des folgenden Satzes von Cayley-Bacharach.

Korollar 6.9 (Satz von Cayley-Bacharach)

Es seien C und C' zwei Kubiken in $\mathbb{P}_{\mathbb{R}}^2$, die sich in genau neun Punkten schneiden. Jede Kubik, die acht der neun Schnittpunkte enthält, enthält auch den neunten.

Beweis: Wir wollen zunächst begründen, weshalb keine vier der neun Punkte auf einer Geraden und keine sieben auf einer Quadrik liegen können. Wären vier der Punkte auf einer Geraden, dann müßte diese Gerade wegen des Satzes von Bézout 4.7 eine Komponente sowohl von C , als auch von C' sein und die beiden Kurven hätten unendlich viele Punkte gemeinsam. Nehmen wir nun an, daß sieben der Punkte auf einer Quadrik liegen. Ist diese Quadrik nicht irreduzibel, dann ist sie die Vereinigung von zwei Geraden und mindestens eine der Geraden müßte vier Punkte enthalten, was wir bereits ausgeschlossen haben. Ist die Quadrik irreduzibel, so muß sie wegen des Satzes von Bézout 4.7 eine Komponente sowohl von C als auch von C' sein, so daß diese wieder unendlich viele Punkte gemeinsam hätten. Damit haben wir gezeigt, daß keine vier der Schnittpunkte auf einer Geraden und keine sieben auf einer Quadrik liegen.

Halten wir nun acht der neun Schnittpunkte fest, P_1, \dots, P_8 , so können wir Lemma 6.8 anwenden und der \mathbb{R} -Vektorraum

$$V = \{F \in \mathbb{R}[x, y, z]_3 \mid F(P_1) = \dots = F(P_8) = 0\}$$

hat Dimension zwei. Es gibt zwei Polynome $G, H \in \mathbb{R}[x, y, z]_3$ mit $V(G) = C$ und $V(H) = C'$. Da die beiden Kubiken nicht gleich sind, sind G und H nicht skalare Vielfache voneinander, d.h. sie sind linear unabhängig. Also bilden sie eine Basis des Vektorraums V . Ist nun C'' eine beliebige Kubik, die die Punkte P_1, \dots, P_8 enthält, dann gibt es ein Polynom $F \in V$ mit $V(F) = C''$. Da (G, H) eine Basis von V ist, gibt es zudem reelle Zahlen $a, b \in \mathbb{R}$, so daß

$$F = a \cdot G + b \cdot H.$$

Aber damit gilt dann für den neunten Schnittpunkt P_9 von C und C'

$$F(P_9) = a \cdot G(P_9) + b \cdot H(P_9) = a \cdot 0 + b \cdot 0 = 0.$$

Mithin ist P_9 in C'' enthalten. \square

Wir erhalten den Beweis des Satzes von Pappos als unmittelbare Folgerung.

Beweis des Satzes von Pappos 6.7: Die drei grünen Geraden in Abbildung 47 bilden eine Kubik C , und ebenso bilden die drei roten Geraden dort eine Kubik C' . Die beiden Kubiken schneiden sich genau in den neun Punkten $A, B, C, A', B', C', P, Q$ und R . Die Kubik $C'' = g \cup g' \cup \overline{PQ}$ schneidet die beiden Kubiken C und C' in mindestens acht der neun Schnittpunkte. Nach dem Satz von Cayley-Bacharach muß sie also auch den neunten Schnittpunkt R enthalten. Nach Konstruktion kann dieser aber weder auf g noch auf g' liegen. Also sind die drei Punkte P, Q und R kollinear, d.h. sie liegen auf einer gemeinsamen Geraden. \square

Mit einem analogen Argument kann man folgende Version des Satzes von Pascal zeigen.

Korollar 6.10 (Satz von Pascal)

Gegeben sei ein Sechseck mit den Ecken A, B, C, D, E und F in der projektiven Ebene $\mathbb{P}_{\mathbb{R}}^2$ wie in Abbildung 50. Wir verlängern einander gegenüberliegende Seiten zu Geraden und berechnen deren Schnittpunkte, so daß wir drei weitere Punkte erhalten:

$$P = \overline{AB} \cap \overline{DE}, \quad Q = \overline{BC} \cap \overline{EF}, \quad \text{und} \quad R = \overline{CD} \cap \overline{FA}.$$

Genau dann liegen die drei Punkte P, Q und R auf einer Geraden, wenn die Punkte A, B, C, D, E und F auf einer Quadrik liegen.

Beweis: Wir veranschaulichen die Aussage in Abbildung 50, und wir verwenden

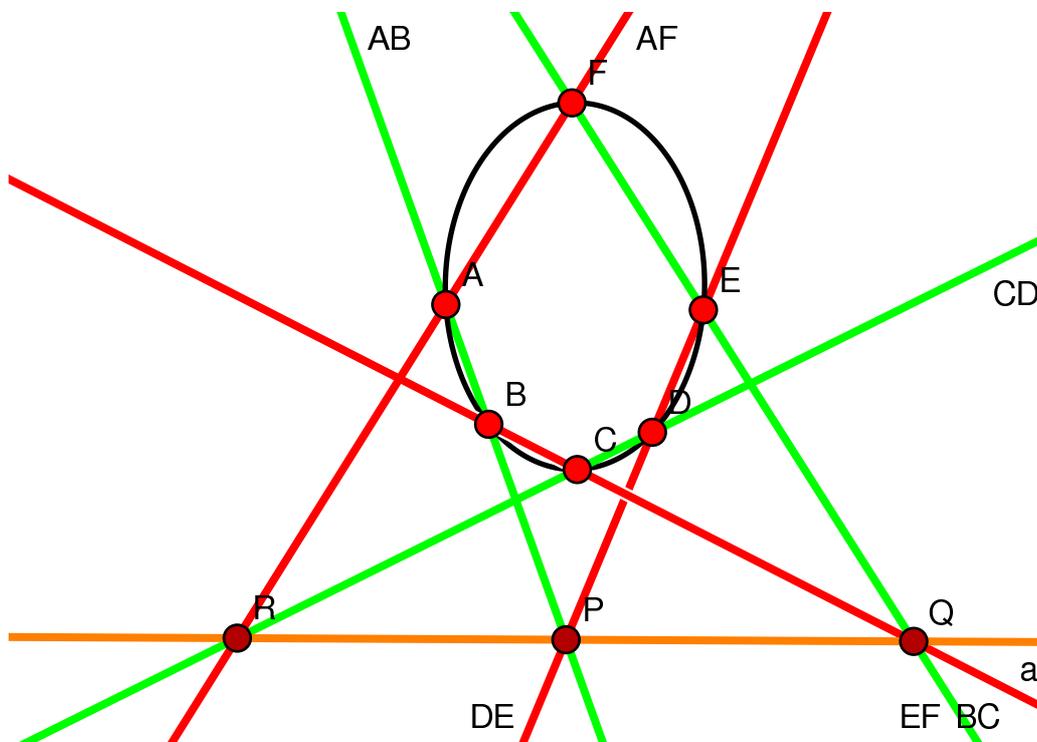


ABBILDUNG 50. Das magische Sechseck des Satzes von Pascal

im folgenden auch die Bezeichnungen und die Farbkodierung der Abbildung. Die

Vereinigung der drei grünen Geraden ist eine Kubik C , ebenso ist die Vereinigung der drei roten Geraden eine Kubik C' . Die beiden Kubiken schneiden sich in den neun Punkten A, B, C, D, E, F, P, Q und R .

Wir sollten hier vielleicht begründen, weshalb die Punkte paarweise verschieden sein müssen, wobei das für die Punkte A, \dots, F vorausgesetzt ist. Nehmen wir zunächst an, P wäre einer der Punkte A oder B . Dann würden die Punkte A, D, E oder die Punkte B, D, E auf einer Geraden liegen und könnten nicht Ecken eines Sechsecks sein. Aus dem gleichen Grund kann P keiner der anderen Punkte sein, und für Q und R argumentiert man analog.

Man beachte außerdem, daß eine Quadrik durch die Punkte A, B, C, D und E keine Vereinigung von zwei Geraden sein kann, da die sechs Punkte als Ecken eines Sechsecks vorausgesetzt sind und somit keine drei von ihnen auf einer Geraden liegen können. Eine Gerade schneidet die Quadrik also in höchstens zwei Punkten wegen des Satzes von Bézout 4.7.

Liegen P, Q und R auf einer Geraden L und ist M eine Quadrik durch die fünf Punkte A, B, C, D und E , dann ist die Vereinigung $C'' = L \cup M$ von L und M eine Kubik, die acht der neun Schnittpunkte von C und C' enthält. Mithin muß sie wegen des Satzes von Cayley-Bacharach auch den neunten enthalten, d.h. $F \in C'' = L \cup M$. Wäre F in $L = \overline{PQR}$ enthalten, dann wäre $L = \overline{FR} = \overline{FA}$ und damit wäre auch A in L . Mit A und Q wäre dann aber auch B in L . Aber dann wären A, B und F auf einer Geraden und könnten nicht die Ecken eines Sechsecks sein. Also liegt F in M und die Punkte A, \dots, F liegen auf einer Quadrik.

Liegen die Punkte A, B, C, D, E und F auf einer Quadrik M und ist L die Gerade durch P und Q , so geht die Kubik $C'' = L \cup M$ durch acht der neun Schnittpunkte von C und C' . Mithin muß auch den neunten enthalten, d.h. $R \in C'' = L \cup M$. Wäre $R \in M$, dann müßte R einer der beiden Schnittpunkte A oder F von L mit M sein, was wir bereits ausgeschlossen haben. Also liegt R in L , und P, Q und R liegen auf einer Geraden. \square

F) Aufgaben

Aufgabe 6.11

Berechnen Sie die Gleichung der Quadrik durch folgende Punkte und visualisieren Sie die Quadrik mit **Surfex**:

- $P_1 = (1 : 0 : 0), P_2 = (0 : 1 : 0), P_3 = (0 : 0 : 1), P_4 = (1 : 1 : 1), P_5 = (1 : 2 : 3)$.
- $P_1 = (0 : 0 : 1), P_2 = (1 : 0 : 1), P_3 = (0 : 1 : 1), P_4 = (0 : -1 : 1), P_5 = (-1 : 0 : 1)$.
- $P_1 = (0 : 0 : 1), P_2 = (-1 : 1 : 1), P_3 = (1 : 1 : 1), P_4 = (2 : 4 : 1), P_5 = (3 : 9 : 1)$.

Konstruieren Sie die dritte Quadrik in **Cinderella** oder in einem anderen Programm der dynamischen Geometrie.

Aufgabe 6.12 (Euler-Formel)

Beweisen Sie für ein homogenes Polynom $F \in \mathbb{K}[x, y, z]$ vom Grad d die Euler-Formel

$$d \cdot F = x \cdot \frac{\partial F}{\partial x} + y \cdot \frac{\partial F}{\partial y} + z \cdot \frac{\partial F}{\partial z}.$$

Aufgabe 6.13

Berechnen Sie die Diskriminante der Familie von ebenen projektiven Kurven vom Grad drei mit Singular. Verwenden Sie diese, um für folgende Punktconfiguration die singulären ebenen projektiven Kurven vom Grad drei zu berechnen und visualisieren Sie die Kurven, für die die zugehörigen Parameter reell sind:

$$\begin{aligned} P_1 &= (0 : 0 : 1) \\ P_2 &= (1 : 0 : 1) \\ P_3 &= (0 : 1 : 1) \\ P_4 &= (1 : 1 : 1) \\ P_5 &= (2 : 3 : 1) \\ P_6 &= (3 : 2 : 1) \\ P_7 &= (-2 : 2 : 1) \\ P_8 &= (2 : -2 : 1) \end{aligned}$$

Sie erhalten nur sieben verschiedene Kubiken. Einige müssen mit Vielfachheit gezählt werden!

Aufgabe 6.14

Berechnen Sie die Diskriminante der Familie von ebenen projektiven Kurven vom Grad drei mit Singular. Verwenden Sie diese, um für folgende Punktconfiguration die zwölf rationalen ebenen projektiven Kurven vom Grad drei zu berechnen und visualisieren Sie die Kurven, für die die zugehörigen Parameter reell sind:

$$\begin{aligned} P_1 &= (0 : 0 : 1) \\ P_2 &= (1 : 0 : 1) \\ P_3 &= (0 : 1 : 1) \\ P_4 &= (1 : 1 : 1) \\ P_5 &= (11 : 2 : 1) \\ P_6 &= (-1 : 12 : 1) \\ P_7 &= (12 : 4 : 1) \\ P_8 &= (-2 : -41 : 1) \end{aligned}$$

Aufgabe 6.15

Betrachten Sie die kubische Fläche im $\mathbb{P}_{\mathbb{C}}^3$, die durch die homogene Gleichung $F = w^2x - x^3 + w^2y + x^2y + xy^2 - y^3 + w^2z + x^2z + 2xyz + y^2z + xz^2 + yz^2 - z^3 = 0$ definiert wird. Berechnen Sie für diese Kubik die Covariante von Clebsch mit Hilfe der SINGULAR -Prozedur von Seite 97. Verwenden Sie diese, um die 27 Geraden der Kubik in der affinen Karte $\{w = 1\}$ mit Hilfe von **Surfex** zu visualisieren. Berechnen Sie anschließend die Gleichungen der Geraden mit Hilfe der Primärzerlegung und visualisieren Sie sie mit Hilfe von **Surfex**.

Aufgabe 6.16

Gegeben seien die Punkte $A = (-4 : 7 : 7)$, $B = (0 : 3 : 3)$, $C = (4 : -1 : -1)$, $A' = (-2 : 3 : 3)$, $B' = (2 : -1 : -1)$, $C' = (6 : -5 : -5) \in \mathbb{P}_{\mathbb{R}}^2$. Zeigen Sie, daß die Punkte A , B und C auf einer Geraden g liegen, und daß die Punkte A' , B' und C' auf einer Geraden g' liegen. Berechnen Sie dann die Schnittpunkte P , Q und R im Satz von Pappos 6.7 und zeigen Sie, daß diese auf einer gemeinsamen Geraden liegen. Visualisieren Sie die Aussage des Satzes von Pappos für diese Punktconfiguration mit Hilfe von *Cinderella* in der affinen Karte $\{z = 1\}$.

Aufgabe 6.17

Man gebe sich in *Cinderella* eine Quadrik durch fünf Punkte A , B , C , D und E sowie einen Punkte Q auf der Geraden \overline{BC} vor. Dann bestimme man Punkte F , P und R , so daß sie dem Satz von Pascal 6.10 genügen.

7 ANGEWANDTE ALGEBRAISCHE GEOMETRIE

(VON THOMAS MARKWIG)

Algebraische Gleichungen tauchen in vielen Anwendungsbereichen in ganz natürlicher Weise auf und Methoden der algebraischen Geometrie und der Computeralgebra werden verwendet, um diese Gleichungen zu lösen oder zu vereinfachen. Hierzu zählen u.a. die System- und Kontrolltheorie zur Steuerung von Prozessen; Gleichgewichtsreaktionen in der Kinematik; die Stabilitätsanalyse bei der Entwicklung von elektrischen Schaltungen; Bewegungsabläufe bei der Robotersteuerung; statistische Modelle in der algebraischen Statistik. Zudem spielen algebraische Varietäten mit zusätzlicher Struktur eine wichtige Rolle in der Kryptographie und der Kodierungstheorie. In dem vorliegenden Text wollen wir uns auf zwei Beispiele beschränken.

A) Die Griffis-Duffy Plattformen

Unser Ziel ist es, bestimmte Mechanismen zur Bewegung von Körpern im Raum zu untersuchen. Um einen solchen Mechanismus sinnvoll konzipieren zu können, sollten wir uns zunächst Gedanken darum machen, wodurch die Lage eines Körpers im Raum bestimmt ist und wie man sie verändern kann. Die Lage ist bestimmt durch den *Ort*, an dem sich der Körper befindet, und durch die *Ausrichtung*, die hat. Man kann die Lage verändern, indem man ihn an einen anderen Ort *verschiebt* und seine Ausrichtung *dreht* (vgl. Abbildung 51). Zur Veränderung der Lage haben

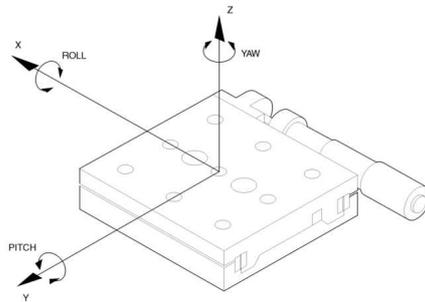


ABBILDUNG 51. Veränderung der Lage eines Körpers im Raum

wir mithin *sechs Freiheitsgrade*: eine Verschiebung in Richtung oben-unten, links-rechts und vorne-hinten sowie eine Drehung mit drei Drehrichtungen. D.h. um die neue Lage eines Körpers relativ zu seiner alten Lage zu beschreiben, benötigen wir einen Verschiebungsvektor $\mathbf{v} \in \mathbb{R}^3$ sowie eine Drehmatrix $\mathbf{A} \in \text{SO}(3)$. Die sechs Freiheitsgrade kommen dann daher, daß der Raum \mathbb{R}^3 sowie die spezielle orthogonale Gruppe $\text{SO}(3)$ jeweils die Dimension drei haben. Für die letztere Aussage beachte man, daß eine Matrix \mathbf{A} genau dann in $\text{SO}(3)$ liegt, wenn

$$\mathbf{A}^t \cdot \mathbf{A} = \mathbb{1}_3 \quad \text{und} \quad \det(\mathbf{A}) = 1.$$

Hat die Matrix \mathbf{A} die Einträge a_{ij} mit $1 \leq i, j \leq 3$, dann führt ein Koeffizientenvergleich der Matrizen zu neun Gleichungen, die zusammen mit der Determinante

das folgende Gleichungssystem ergeben:

$$\begin{array}{ll}
 1) & a_{11}^2 + a_{21}^2 + a_{31}^2 = 1 \\
 2) & a_{11} * a_{12} + a_{21} * a_{22} + a_{31} * a_{32} = 0 \\
 3) & a_{11} * a_{13} + a_{21} * a_{23} + a_{31} * a_{33} = 0 \\
 4) & a_{11} * a_{12} + a_{21} * a_{22} + a_{31} * a_{32} = 0 \\
 5) & a_{12}^2 + a_{22}^2 + a_{32}^2 = 1 \\
 6) & a_{12} * a_{13} + a_{22} * a_{23} + a_{32} * a_{33} = 0 \\
 7) & a_{11} * a_{13} + a_{21} * a_{23} + a_{31} * a_{33} = 0 \\
 8) & a_{12} * a_{13} + a_{22} * a_{23} + a_{32} * a_{33} = 0 \\
 9) & a_{13}^2 + a_{23}^2 + a_{33}^2 = 1 \\
 10) & -a_{13} * a_{22} * a_{31} + a_{12} * a_{23} * a_{31} + a_{13} * a_{21} * a_{32} \\
 & -a_{11} * a_{23} * a_{32} - a_{12} * a_{21} * a_{33} + a_{11} * a_{22} * a_{33} = 1
 \end{array}$$

Da die Matrix $A^t \cdot A$ symmetrisch ist, sind einige der Gleichungen überflüssig, aber wir sehen auf diesem Weg, daß die Gruppe $SO(3)$ eine affine algebraische Varietät ist, die im affinen Raum $\mathbb{A}_{\mathbb{R}}^9$ mit den Koordinaten $(a_{ij} \mid 1 \leq i, j \leq 3)$ liegt. Wir können mit Hilfe von SINGULAR die Dimension dieser Varietät ausrechnen.

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> ring r=0,(a11,a12,a13,a21,a22,a23,a31,a32,a33),dp;
> matrix A[3][3]=a11,a12,a13,a21,a22,a23,a31,a32,a33;
> M=transpose(A)*A;
> ideal I=M[1,1]-1,M[1,2],M[1,3],M[2,2]-1,M[2,3],M[3,3]-1,det(A)-1;
> dim(std(I));
3

```

Die Drehgruppe hat also wirklich Dimension drei.

Um einen Mechanismus zu konstruieren, der einen Körper im Raum bewegt, bedienen wir uns zweier Platten. Eine der Platten ist am Boden verankert, auf der anderen ist der Körper befestigt, so daß wir nur die beiden Platten relativ zueinander bewegen müssen. Dazu verbinden wir die beiden Platten durch Beine miteinander. Die Länge der Beine soll variabel sein und sie sollen über Kugelgelenke mit den Platten verbunden sein. Wir wollen die Lage der Platte nun durch Veränderung der Länge der Beine kontrollieren. Da wir sechs Freiheitsgrade in unserer Bewegung haben, sollte es möglich sein, mit sechs Beinen eine stabile Konstruktion zu erreichen, d.h. wenn wir die Beine auf einer festen Länge arretieren, sollte die Konstruktion starr sein und die obere Platte unbeweglich. Man beachte dabei, daß die Kugelgelenke frei beweglich sind, so daß man bei weniger als sechs Beinen den Mechanismus in sich drehen kann! Eine Konstruktion dieser Art wird eine *Stewart-Gough Plattform* genannt (siehe Abbildung 52).



ABBILDUNG 52. Allgemeine Stewart-Gough Plattform
(http://de.wikipedia.org/wiki/Stewart_Plattform)

Solche Plattformen werden zur Robotersteuerung (siehe Abbildung 53) eingesetzt. Entwickelt wurden sie zum Testen der Abnutzung von Autoreifen (siehe Abbildung 54). Sie finden aber auch ein vielen anderen Bereichen Einsatz, etwa für Flugsimulatoren (siehe Abbildung 55), bei der Steuerung von Satellitenantennen (siehe Abbildung 56) oder in der Mikrochirurgie (siehe Abbildung 57).



ABBILDUNG 53. Industrieroboter

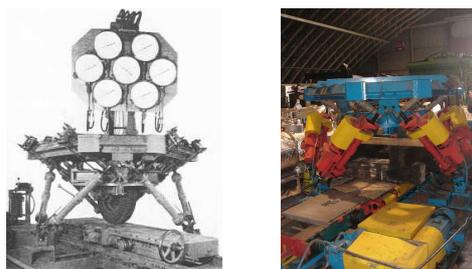


ABBILDUNG 54. Gough Plattform 1954 / 2000 (Dunlop, Proc. IMechE, 1965-66)

Bei der Kontrolle der Steuerung der Plattform gibt es nun zwei prinzipielle Fragestellungen. Zum einen möchte man in der Lage sein, bei gegebener Beinlänge die möglichen Lagepositionen der Platte angeben zu können (*direkte Kinematik*), zum anderen möchte man wissen, welche Beinlängen notwendig sind, um eine vorgegebene Position zu erreichen (*inverse Kinematik*).



ABBILDUNG 55. Flugsimulator (Lufthansa)
(http://de.wikipedia.org/wiki/Stewart_Plattform)



ABBILDUNG 56. Ausrichtung von Satellitenantennen (Physik Instrumente, M-840)



ABBILDUNG 57. Chirurgischer Roboter (Physik Instrumente, M-850)
(Fraunhofer Institut IPA, Stuttgart)

Um das Problem angehen zu können, führen wir Bezeichnungen ein. Die Basispunkte der sechs Beine im Raum wollen wir mit $\mathbf{a}_1, \dots, \mathbf{a}_6$ bezeichnen, die Endpunkte mit $\mathbf{b}_1, \dots, \mathbf{b}_6$ (siehe Abbildung 58). Die Länge des i -ten Beines ist dann

$$L_i = |\mathbf{b}_i - \mathbf{a}_i| = \sqrt{(\mathbf{b}_{i1} - \mathbf{a}_{i1})^2 + (\mathbf{b}_{i2} - \mathbf{a}_{i2})^2 + (\mathbf{b}_{i3} - \mathbf{a}_{i3})^2}$$

der euklidische Abstand der Punkte \mathbf{a}_i und \mathbf{b}_i . Eine Lageänderung der Plattform wird durch eine Abbildung

$$\Phi_{A,v} : \mathbb{R}^3 \longrightarrow \mathbb{R}^3 : \mathbf{b} \mapsto A \cdot \mathbf{b} + \mathbf{v}$$

beschrieben, bei der $A \in SO(3)$ eine Drehmatrix ist und $\mathbf{v} \in \mathbb{R}^3$ ein Verschiebungsvektor ist. Dabei werden die Basispunkte der Beine festgelassen, und nur die Endpunkte der Beine werden bewegt, d.h.

$$\mathbf{b}_i \mapsto \Phi_{A,v}(\mathbf{b}_i).$$

Für die *inverse Kinematik* wollen wir bei gegebener Endposition $\Phi_{A,v}(\mathbf{b}_1), \dots, \Phi_{A,v}(\mathbf{b}_6)$ die Beinlängen L_1, \dots, L_6 bestimmen. Dies geschieht

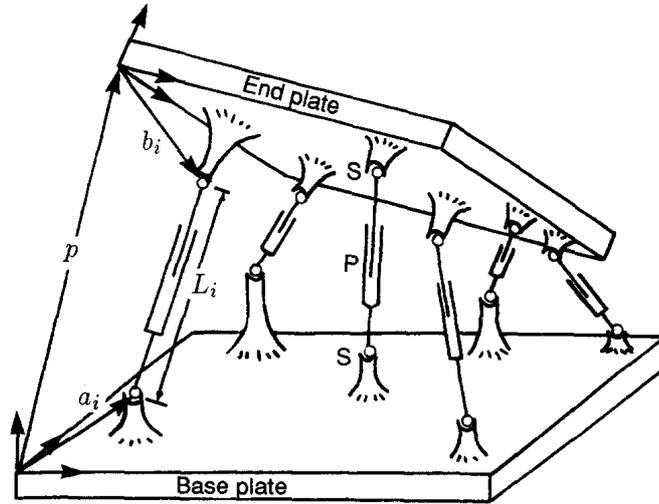


ABBILDUNG 58. Beschreibung der Bewegung der Plattform [Wam96]

durch einfaches Einsetzen der Werte:

$$L_i^2 = |\Phi_{A,v}(b_i) - a_i|^2.$$

Die Abbildung

$$F : \mathbb{R}^3 \times \text{SO}(3) \longrightarrow \mathbb{R}^6 : (v, A) \mapsto (|\Phi_{A,v}(b_i) - a_i|^2 \mid i = 1, \dots, 6)$$

ist eine Parametrisierung der Lösung der inversen Kinematik. Es handelt sich dabei um eine *polynomiale Parametrisierung*, und das Bild ist eine affine algebraische Varietät!

Das Problem der *direkten Kinematik* ist etwas schwieriger. Hier sind die Beinlängen L_1, \dots, L_6 gegeben und die Koordinaten von A und v sind gesucht. Wir müssen im Raum $\mathbb{R}^3 \times \text{SO}(3)$ mit den Koordinaten a_{ij} und v_k die sechs Gleichungen

$$L_i^2 = |\Phi_{A,v}(b_i) - a_i|^2 = |A \cdot b_i + v - a_i|^2$$

für $i = 1, \dots, 6$ lösen. Die Lösungsmenge sollte eine nulldimensionale algebraische Varietät, d.h. eine endliche Menge von Punkte (v, A) in $\mathbb{R}^3 \times \text{SO}(3)$ sein.

Der konkrete Mechanismus hängt nun entscheidend von der relativen Lage der Punkte a_i und b_j , $i, j = 1 \dots, 6$, zueinander ab. 1991 haben die Ingenieure Griffis und Duffy für einen bestimmten Konfigurationstyp (siehe Abbildung 60) ein Patent eingereicht, bei dem es ganz wesentlich um effiziente Verfahren zur Lösung der Kinematik ging (siehe Abbildung 59). Drei der Basis- bzw. Endpunkte der Beine sollen jeweils ein Dreieck bilden bei dem die verbliebenen drei Basis- bzw. Endpunkte auf den Mittelpunkten der Seiten liegen. Wir können dabei die Basis- und die Endpunkte so wählen, daß die Dreiecke gleichseitig von gleicher Seitenlänge 2 sind, daß die Beine alle die Länge $\sqrt{3}$ haben und daß die Verbindung der Beine miteinander der Konfiguration *Fig 12* in Abbildung 60 entspricht, z.B.

$$a_1 = b_4 = (-1, 0, 0), a_2 = b_5 = (0, 0, 0), a_3 = b_6 = (1, 0, 0),$$

2080822



PCT
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁵ : G09B 9/08</p> <p>(21) International Application Number: PCT/US91/02983 (22) International Filing Date: 1 May 1991 (01.05.91)</p> <p>(30) Priority data: 517,371 1 May 1990 (01.05.90) US</p> <p>(71) Applicant: UNIVERSITY OF FLORIDA [US/US]; 223 Grinter Hall, Division of Sponsored Research, Gainesville, FL 32611 (US).</p> <p>(72) Inventors: GRIFFIS, Michael, W. ; 4321 Northwest 27th Drive, Gainesville, FL 32605 (US). DUFFY, Joseph ; 3823 Southwest 77th Street, Gainesville, FL 32608 (US).</p>	<p>(11) International Publication Number: WO 91/17536</p> <p>(43) International Publication Date: 14 November 1991 (14.11.91)</p> <p>(74) Agents: LAND, John et al.; Spensley Horn Jubas & Lubitz, 1880 Century Park East, Fifth Floor, Los Angeles, CA 90067 (US).</p> <p>(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, KR, LU (European patent), NL (European patent), SE (European patent).</p> <p>Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>
---	--

(54) Title: METHOD AND APPARATUS FOR CONTROLLING GEOMETRICALLY SIMPLE PARALLEL MECHANISMS WITH DISTINCT CONNECTIONS

(57) Abstract

A system, method and apparatus for controlling, via a closed-form forward displacement computation, the position and orientation of a movable platform of a parallel mechanism. A movable platform is supported above a base platform by a plurality of parallel support legs such as linear actuators. The dimensions of the base platform and the movable platform, as well as the lengths of the support legs, are provided to a control system. The control system is operative to compute at least one closed-form forward displacement solution (51) of the geometry of polyhedron (an octahedron for the disclosed embodiments) formed by the movable platform, the base platform, and the support legs. The control system determines a final position and orientation of the movable platform by eliminating imaginary roots of the closed-form solutions and roots which would result in discontinuous paths of travel for the movable platform. A novel special 6-6 parallel mechanism (Fig. 12) is also disclosed. The control system is suitable for controlling known 3-3 or 6-3 Stewart platforms in a novel manner, as well as controlling the novel special 6-6 parallel mechanism. The special 6-6 parallel mechanism is distinguished from a general 6-6 by the fact that it is geometrically reducible to an octahedron, and therefore it has a simple geometry, even though its legs possess distinct connections. Also disclosed is a method for reducing the novel special 6-6 parallel mechanism to a Stewart platform equivalent, which is then controlled by the disclosed closed-form forward displacement control system.

ABBILDUNG 59. Das Patent von Griffis und Duffy

$$a_4 = b_1 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}, 0 \right), a_5 = b_2 = (0, \sqrt{3}, 0), a_6 = b_3 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}, 0 \right).$$

Diese Lage ist natürlich etwas idealisiert, da die Punkte a_i auf den Punkten b_j liegen. In der Praxis sollte das nicht möglich sein, und wenn die Konfiguration gut ist, sollten wir aus dieser idealisierten Lage auch nicht herauskommen, ohne die Länge der Beine zu ändern. D.h. wenn wir die Eingangsdaten in unser obiges Gleichungssystem für die inverse Kinematik einsetzen, so sollten wir eine nulldimensionale Lösungsmenge erhalten. Wir können die Dimension der Lösungsmenge mit SINGULAR berechnen:

WO 91/17536

2090822

PCT/US91/02983

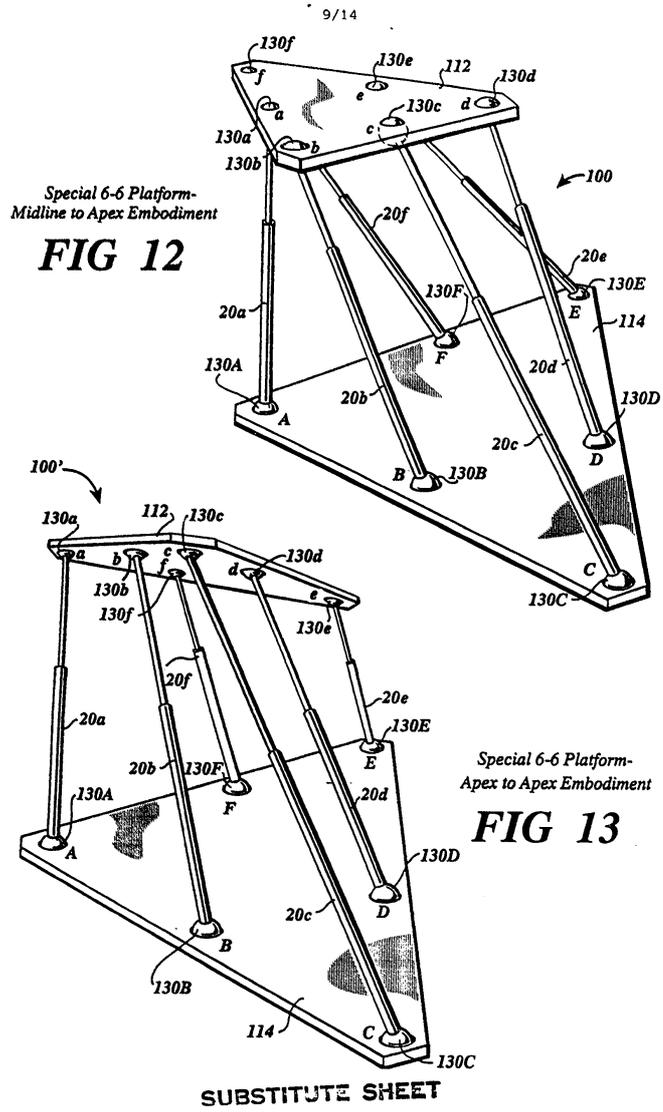


ABBILDUNG 60. Der Konfigurationstyp von Griffis und Duffy

```

SINGULAR /
A Computer Algebra System for Polynomial Computations / version 3-0-4
0<
by: G.-M. Greuel, G. Pfister, H. Schoenemann \ Nov 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern \
> // Eine schlechte Griffis-Duffy Konfiguration
. ///////////////////////////////////////////////////////////////////
. ring RR=(0,s),(v1,v2,v3,a11,a12,a13,a21,a22,a23,a31,a32,a33),dp;
> minpoly=s^2-3; // dadurch wird s zur Wurzel aus 3
    
```

```

> // Rotationsmatrix + Verschiebungsvektoren
. matrix A[3][3]=a11,a12,a13,a21,a22,a23,a31,a32,a33;
> matrix v[6][3]=v1,v2,v3,v1,v2,v3,v1,v2,v3,v1,v2,v3,v1,v2,v3;
> // Punkte der Basisplatte
. matrix a[6][3]=
. -1,0,0,
. 0,0,0,
. 1,0,0,
. 1/2,s/2,0,
. 0,s,0,
. -1/2,s/2,0;
> // Punkte der Endplatte
. matrix b[6][3]=
. 1/2,s/2,0,
. 0,s,0,
. -1/2,s/2,0,
. -1,0,0,
. 0,0,0,
. 1,0,0;
> // Beinlaengen
. matrix L[6][1]=s,s,s,s,s,s;
> // Berechne die 6 Gleichungen
. ideal I;
> matrix D[3][6]=A*transpose(b)+transpose(v)-transpose(a);
> for (int i=1;i<=6;i++)
. {
.   I[i]=L[1,1]^2-(D[1,i]^2+D[2,i]^2+D[3,i]^2);
. }
> // Füge die Gleichungen der SO(3) hinzu
. matrix M[3][3]=transpose(A)*A;
> I=I,M[1,1]-1,M[1,2],M[1,3],M[2,1],M[2,2]-1,M[2,3],
.   M[3,1],M[3,2],M[3,3]-1,det(A)-1;
> // Berechne die Dimension des Ideals I
. dim(groebner(I));
1

```

Die Lösungsmenge hat Dimension eins! Es gibt also eine eindimensionale Familie von Bewegungen, die ohne Änderung der Beinlänge durchgeführt werden kann? An dieser Stelle ist Vorsicht geboten! Das Ergebnis wurde zwar über den rationalen Zahlen berechnet, es sagt zunächst aber nur, daß man über den komplexen Zahlen einen Freiheitsgrad für die Bewegungen hat. Das allein sollte den potentiellen Nutzer eines solchen Mechanismus aber schon vorsichtig werden lassen. Einige Zusatzüberlegungen oder schlicht eine Simulation des Mechanismus zeigen dann sehr schnell, daß man in der Tat schon über \mathbb{R} den Mechanismus bewegen kann, ohne die Beinlängen zu verändern. Der Mechanismus ist also nicht starr und für die oben angedeuteten

Anwendungen damit unbrauchbar. Die Kurve, die ein Punkt, der an der Endplatte des Mechanismus angebracht ist, bei der Bewegung beschreibt, ist in Abbildung 61 dargestellt.

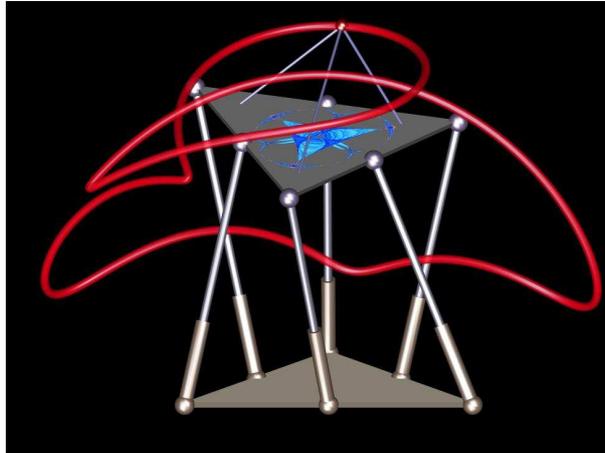
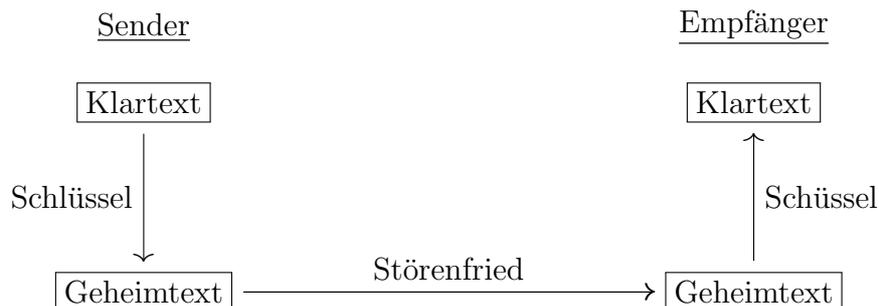


ABBILDUNG 61. Der Freiheitsgrad der Griffis-Duffy Plattform (Doug Arnold & Charles Wampler, Institute for Mathematics and its Applications, Minneapolis)

Dies ist ein Beispiel, wie Methoden der algebraischen Geometrie bei Stabilitätsuntersuchungen von Robotermechanismen eingesetzt werden können. Der Artikel [Bon03] bietet einen schönen Überblick über die Anfänge der Stewart-Gough Plattformen. Wer sich mit dem mathematischen Aspekt der Kinematik der Plattformen näher vertraut machen möchte, der sei auf die folgende Literatur verwiesen: [BR79], [SW05], [Wam96] und [HK00].

B) Elliptische Kurven in der Kryptographie

In der Kryptographie möchte man eine Nachricht über einen unsicheren Kanal schicken. Es gilt nun zu verhindern, daß ein Störenfried die Informationen mithören und *verstehen* oder *unbemerkt verändern* kann. Da wir den Kanal als unsicher annehmen, können wir das *Mithören* in aller Regel nicht verhindern. Also muß beim Verstehen und Verändern angesetzt werden. Die Grundidee ist, den Text zu verschlüsseln.

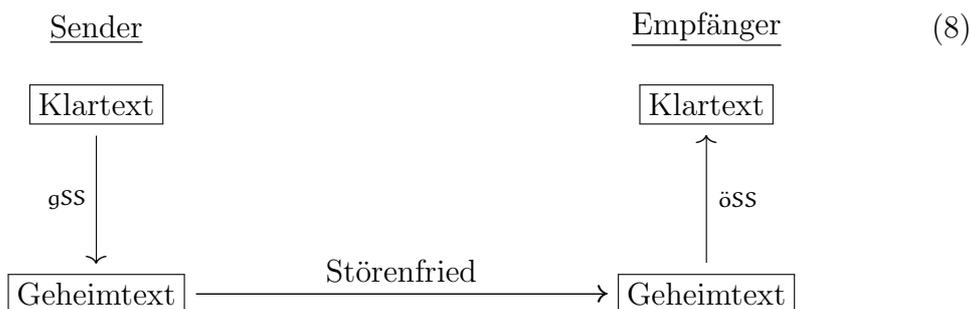


In der einfachsten Form der aus dem alten Rom überlieferten *Caesar Chiffre* vertauscht man die Buchstaben der Nachricht zyklisch, z.B.

a	b	c	d	e	...	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓
m	n	o	p	q	...	j	k	l

Der Schlüssel besteht hierbei aus einer einzigen Zahl, nämlich um wieviel Buchstaben man das “a” nach rechts geschiftet hat; im obigen Beispiel ist dies 12. Eine solch einfache Verschlüsselung ist natürlich auch sehr einfach von einem Störenfried zu brechen. Aber sie weist ein wichtiges Merkmal auf, das auch allen der nach Caesar entwickelten Verschlüsselungsverfahren bis ins letzte Jahrhundert eigen war: der gleiche Schlüssel dient zum Verschlüsseln und zum Entschlüsseln, muß also *geheim* bleiben! Man nennt solche Verschlüsselungsverfahren deshalb *symmetrisch*, und eines ihrer wesentlichen Sicherheitsrisiken besteht darin, daß Sender und Empfänger zunächst einmal den geheimen Schlüssel austauschen müssen, ohne dabei abgehört werden zu können.

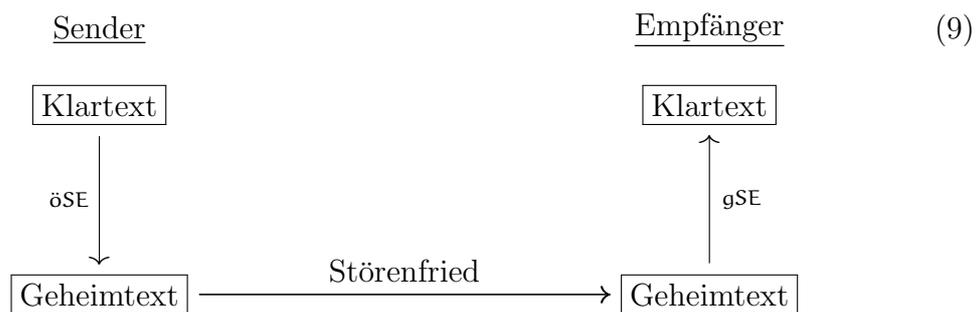
Eine Idee von Whitfield Diffie und Martin Hellman (siehe [DH76]) aus den siebziger Jahren revolutionierte die Kryptographie. Zum Ver- und Entschlüsseln sollten zwei unterschiedliche Schlüssel verwendet werden, und die Kenntnis von einem der beiden und der Nachricht sollte es nicht erlauben, auf den anderen zurückzuschließen. So könnte der Sender einen der beiden Schlüssel *geheim* halten, den anderen aber *öffentlich* bekannt geben. Damit ist es leicht, eine Nachricht so zu verschlüsseln, daß dem Empfänger jede Veränderung auffallen würde. Wir stellen dies in dem folgenden Schema dar, wobei *gSS* für den *geheimen Schlüssel des Senders* steht und *öSS* für den *öffentlichen Schlüssel des Senders*:



Der Störenfried kann die Nachricht zwar abfangen, mit dem (auch ihm bekannten) öffentlichen Schlüssel entschlüsseln und kennt dann deren Inhalt. Da ihm aber der geheime Schlüssel fehlt, kann er die Nachricht nicht verfälschen, wieder verschlüsseln und gefälscht weiter schicken.

Wenn man die Nachricht geheim halten möchte, sollte der Empfänger je einen geheimen und öffentlichen Schlüssel haben. Wie dann die Verschlüsselung aussehen kann, stellen wir in folgendem Schema dar, wobei wir für den geheimen Schlüssel des Empfängers die Abkürzung *gSE* verwenden und für seinen öffentlichen Schlüssel

die Abkürzung öSE :



Da der Störenfried den geheimen Schlüssel des Empfängers nicht kennt, kann er die Nachricht auch nicht entschlüsseln. Verschlüsselungsverfahren dieser Art nennt man *asymmetrisch*, oder spezieller *public key Verfahren*. Aber damit ein solches Verfahren funktionieren kann, muß es einigen wichtigen Anforderungen genügen, und um dies zu beschreiben sollten wir den Begriff der *Verschlüsselung* etwas mathematischer fassen.

Bei der Caesar Chiffre aus obigem Beispiel werden Textblöcke verschlüsselt, die aus einem einzigen Buchstaben bestehen, und man kann die Verschlüsselung als *Abbildung*

$$f_k : \mathcal{N} \longrightarrow \mathcal{N}$$

der Menge

$$\mathcal{N} = \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{f}, \mathbf{g}, \mathbf{h}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{l}, \mathbf{m}, \mathbf{n}, \mathbf{o}, \mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s}, \mathbf{t}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}\}$$

in sich selbst auffassen, die von dem Schlüssel k abhängt (in obigem Beispiel $k = 12$) und die *Nachricht* um k Stellen verschiebt – wobei wir im Alphabet mit \mathbf{a} weiter machen, wenn wir bei \mathbf{z} angekommen sind. Wichtig ist dabei, daß die Funktion eine *Umkehrfunktion* besitzt (man nennt die Funktion f_k dann *bijektiv*), die es erlaubt, den Prozeß rückgängig zu machen. In unserem Fall ist dies die Funktion f_{-k} , die eine Nachricht um k Stellen nach links verschiebt. Auch sie hängt von einem Schlüssel ab, und es ist im wesentlichen der gleiche Schlüssel – das Verschlüsselungsverfahren ist *symmetrisch*! Da man für jeden zulässigen Schlüssel eine Funktion f_k zum Verschlüsseln benötigt, spricht man auch von einer *Familie* von Funktionen $\{f_k \mid k \in \mathcal{S}\}$, wobei \mathcal{S} die Menge der zulässigen Schlüssel sein soll. Im Fall der Caesar Chiffre könnten wir $\mathcal{S} = \{-25, -24, \dots, 24, 25\}$ wählen.

Im allgemeinen wird man Textblöcke größerer Länge verschlüsseln, und man wird sie in aller Regel zunächst durch einen einfachen Übersetzungsmechanismus in Ziffern überführen, um leichter die Methoden der Mathematik anwenden zu können. Bei der Caesar Chiffre könnte man z.B. die Buchstaben durch ihre Position im Alphabet ersetzen, $\mathbf{a} = 1$, $\mathbf{b} = 2$, etc., und man könnte \mathcal{N} auf dem Weg etwa mit $\{1, 2, \dots, 26\}$ oder gar mit \mathbb{Z}_{26} gleichsetzen. Jedenfalls schadet es nichts, wenn wir vereinfachend davon ausgehen, daß die Nachricht, die wir verschlüsseln wollen aus einer Zahl besteht! Für das oben beschriebene *public key Verfahren* benötigen wir

dann eine Familie von bijektiven Funktionen $\mathcal{F} = \{f_k : \mathcal{N} \rightarrow \mathcal{N} \mid k \in \mathcal{S}\}$ auf der Menge \mathcal{N} der Nachrichten, so daß für jeden Schlüssel $gS \in \mathcal{S}$ ein Schlüssel $oS \in \mathcal{S}$ existiert mit

$$f_{gS} \circ f_{oS} = f_{oS} \circ f_{gS} = \text{id}_{\mathcal{N}}. \quad (10)$$

Die Abbildung f_{oS} ist dann die Inverse von f_{gS} , so daß man die Bedingung (10) auch alternativ schreiben könnte als

$$f_k \in \mathcal{S} \implies f_k^{-1} \in \mathcal{S}.$$

Die beiden Eigenschaften in (10) bedeuten für die Anwendung, daß es egal ist, ob man den öffentlichen oder den geheimen Schlüssel zum *Verschlüsseln* verwendet, der jeweils andere kann zum *Entschlüsseln* verwendet werden. Das haben wir in den beiden oben beschriebenen Anwendungen (siehe (8) und (9)) bereits ausgenutzt.

Ein ungemein wichtiger Punkt dabei ist natürlich, daß man aus der Kenntnis der Familie \mathcal{F} sowie eines gegebenen öffentlichen Schlüssels oS *keine Chance* hat, den zugehörigen geheimen Schlüssel gS zu bestimmen. Dabei heißt *keine Chance* nicht, daß es prinzipiell unmöglich ist, sondern daß der notwendige Rechenaufwand nicht in sinnvoller Zeit zu bewerkstelligen ist. Zugleich muß der Rechenaufwand zur Bestimmung von $f_k(n)$ bei gegebenem n und k sehr gering sein, damit man das Verfahren auch praktisch anwenden kann!

Eine solche Familie von Funktionen haben Ronald Rivest, Adi Shamir und Leonard Adleman 1977 (siehe [RSA78]) gefunden, und daraus ist das *RSA-Verfahren* entstanden, das aus mathematischer Sicht nicht mehr als die Primfaktorzerlegung der ganzen Zahlen und ein paar einfache Ergebnisse wie den Chinesischen Restsatz oder den Kleinen Satz von Fermat braucht. Entscheidend dabei ist folgende Erkenntnis: so einfach die Zerlegung einer Zahl in Primfaktoren *im Prinzip* auch ist, so schwierig ist sie doch ganz *konkret* durchzuführen (selbst für gute Computer), wenn die Zahlen einmal mehrere hundert Ziffern besitzen!

Wenn man das RSA-Verfahren einzusetzen will, dann wird man die zu verschickende Nachricht zunächst in eine ganze Zahl umwandeln und dann diese Zahl verschlüsseln und das Ergebnis später entschlüsseln. Man geht also in einem ersten Schritt vom Klartext zu Zahlen über. Der große Vorteil einer Nachricht, die eine ganze Zahl ist, liegt darin, daß wir auf der Menge der ganzen Zahlen Operationen wie die Addition und die Multiplikation zur Verfügung haben. Wir können mit ihnen rechnen. \mathbb{Z} ist eine algebraische Struktur!

Neuere Ansätze in der Kryptographie beruhen darauf in obigem Verfahren die Menge der ganzen Zahlen durch eine andere algebraische Struktur zu ersetzen, für die es andere Rechenoperationen gibt, die leicht durchführbar sind, deren Umkehrung ohne Zusatzinformation aber nahezu unmöglich ist. Hier bieten die elliptischen Kurven eine vielversprechende Alternative.

Definition 7.1

Eine nicht-singuläre ebene projektive Kurve vom Grad drei über einem Körper K wird eine *elliptische Kurve* genannt.

Beispiel 7.2

Die Kurve $V(F)$ mit $F = y^2z - x \cdot (x - \frac{1}{2} \cdot z) \cdot (x - z)$ ist eine elliptische Kurve. Um das zu sehen, müssen wir zeigen, daß die partiellen Ableitungen nur dann alle null werden, wenn $(x, y, z) = (0, 0, 0)$ ist (siehe auch den Beweis von Satz 6.4):

$$\frac{\partial F}{\partial x} = -3x^2 + 3xz - \frac{1}{2} \cdot z^2 = 0,$$

$$\frac{\partial F}{\partial y} = 2yz = 0,$$

$$\frac{\partial F}{\partial z} = \frac{3}{2} \cdot x^2 + y^2 - xz = 0.$$

Die zweite Gleichung bedingt, daß $y = 0$ oder $z = 0$ gilt. Ist $y = 0$, so folgt aus der dritten Gleichung, daß $x = 0$ oder $x = z$ gilt. In beiden Fällen liefert die erste Gleichung $-\frac{1}{2} \cdot z^2 = 0$, also $z = 0$. Ist statt dessen $z = 0$, so liefert die erste Gleichung $-3x^2 = 0$ und damit $x = 0$. Dann ist aber wegen der dritten Gleichung mit $y^2 = 0$ auch $y = 0$. Also ist die Kurve hat also keinen singulären Punkt in der projektiven Ebene \mathbb{P}_K^2 .

Wir visualisieren diese elliptische Kurve für $K = \mathbb{R}$ in Abbildung 62.

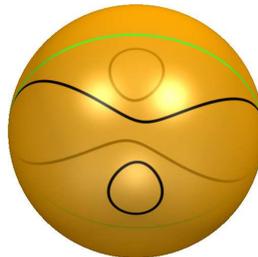


ABBILDUNG 62. Die elliptische Kurve $y^2z - x \cdot (x - \frac{1}{2} \cdot z) \cdot (x - z) = 0$

Elliptische Kurven sind für die Kryptographie deshalb von Nutzen, weil wir auf ihnen einerseits eine Addition definieren können, so daß wir mit den Punkten der Kurve *rechnen* können, und weil andererseits der sogenannte *diskrete Logarithmus* schwer zu berechnen ist. Was heißt das? Statt $P+P+P$ sind wir es gewohnt $3 \cdot P$ zu schreiben. Wir können Punkte einer elliptischen Kurve also mit ganzen Zahlen multiplizieren. Während es in den ganzen Zahlen nun sehr einfach ist, diese Operation rückgängig zu machen, d.h. durch 3 zu dividieren, ist das für eine elliptische Kurve im allgemeinen sehr schwer. Wenn wir die Addition erläutert haben, verwundert dieser Umstand vielleicht weniger. Das bekannteste Verschlüsselungsverfahren, das auf dem diskreten Logarithmus beruht ist sicher das *El-Gamal* verfahren (siehe z.B. [BSW99]).

Wir wollen nun die Addition auf der elliptischen Kurve aus Beispiel 7.2 geometrisch definieren. Man kann dies auch mit rein algebraischen Mitteln tun, und das ist

für die elliptischen Kurven, die in der Kryptographie eingesetzt werden, in der Tat notwendig.

Bemerkung 7.3 (Addition auf einer elliptischen Kurve)

Wollen wir zwei Punkte A und B auf der elliptischen Kurve

$$\mathcal{C} = V\left(y^2z - x \cdot \left(x - \frac{1}{2} \cdot z\right) \cdot (x - z)\right) \subset \mathbb{P}_{\mathbb{C}}^2$$

addieren, so gehen wir wie folgt vor.

Durch die Punkte A und B gibt es genau eine Gerade \mathcal{G} , die die Kurve \mathcal{C} wegen des Satzes von Bézout in genau einem weiteren Punkt C schneidet (siehe Abbildung 63). Diesen verbinden wir mit dem Punkt $O = (0 : 1 : 0)$ und erhalten so eine Gerade \mathcal{H} , die die Kurve \mathcal{C} wieder in genau einem weiteren Punkt schneiden wird (siehe Abbildung 64). Diesen Punkt definieren wir als die Summe von A und B .

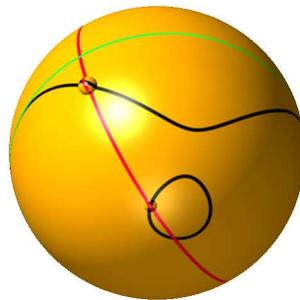


ABBILDUNG 63. Die Kurve \mathcal{C} mit den Punkten A und B markiert sowie der Geraden \mathcal{G} . Der nicht markierte Schnittpunkt von \mathcal{C} mit \mathcal{G} ist der Punkt C .

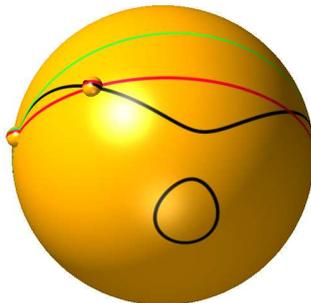


ABBILDUNG 64. Die Kurve \mathcal{C} mit den Punkten O und C markiert sowie der Geraden \mathcal{H} . Der nicht markierte Schnittpunkt von \mathcal{C} mit \mathcal{H} ist der Punkt $A + B$.

So wie wir unsere Konstruktion geschildert haben, funktioniert sie nur, wenn die auftretenden Punkte jeweils alle verschieden sind. Was tun wir wenn A und B gleich

sind? Wir wählen die Gerade \mathcal{G} dann als Tangente an \mathcal{C} im Punkt A . Dies ist naheliegend, wenn man sich ausgehend von zwei verschiedenen Punkte A und B vorstellt, daß man B langsam in den Punkt A verschiebt. Die Verbindungsgerade von A und B , die auch die Sekante durch A und B genannt wird, konvergiert dann gegen die Tangente an \mathcal{C} im Punkt A . Diese hat nun Schnittvielfachheit 2 im Punkt A , so daß der Satz von Bézout uns immer noch nur einen weiteren Schnittpunkt liefert. Dabei müssen wir den Begriff *weiterer* geeignet interpretieren. Es ist durchaus möglich, daß es keinen neuen Schnittpunkt gibt, sondern daß die Vielfachheit eines alten Schnittpunktes höher als erwartet ist. In diesem Fall ist sie nur in diesem einen Schnittpunkt höher und sie ist genau um eins höher. Wir nennen ihn also den *weiteren* Schnittpunkt. Entsprechendes gilt für die Gerade \mathcal{H} und den Punkt $A + B$.

Wir behaupten, daß die elliptische Kurve \mathcal{C} mit dieser Addition eine abelsche Gruppe ist, d.h. daß die Rechengesetze der Addition gelten, wie wir sie von den ganzen Zahlen her kennen.

Als abelsche Gruppe muß \mathcal{C} insbesondere ein neutrales Element der Addition haben. Dieses ist der Punkt $O = (0 : 1 : 0)$. Um das zu sehen, überlegen wir uns, wie der Punkt $A + O$ konstruiert wird. Die Gerade \mathcal{G} durch die Punkte A und O schneidet \mathcal{C} in genau einem weiteren Punkt C . Diesen verbinden wir mit dem Punkt O und erhalten so die Gerade \mathcal{H} . Da C und O aber beide auf \mathcal{G} liegen, muß notwendigerweise $\mathcal{G} = \mathcal{H}$ gelten. Der dritte Schnittpunkt von \mathcal{H} mit \mathcal{C} ist mithin der Punkt A . Dies zeigt, daß $A + O = A$. Die übrigen Gesetzmäßigkeiten zeigt man ähnlich, wobei das Assoziativgesetz größere Probleme bereitet. \square

Unserer Definition zufolge können wir elliptische Kurven über jedem beliebigen Körper K betrachten. Bisher haben wir dabei stets die Philosophie vertreten, daß wir mit $K = \mathbb{Q}$ rechnen, über $K = \mathbb{R}$ zeichnen und daß die Aussagen nur über $K = \mathbb{C}$ sicher richtig sind. Für die Belange der Kryptographie ist aber keiner dieser Körper geeignet! Die Elemente der Kurve sollen den Nachrichten entsprechen, die man verschicken möchte. Lange Nachrichten zerlegt man dazu in mehrere Blöcke fester Länge. Wir benötigen deshalb nur eine endliche und a priori beschränkte Anzahl an Punkten der Kurve. Wenn wir nur endlich viele Punkte brauchen, dann ist es auch sinnvoll mit Kurven zu arbeiten, die nur aus endlich vielen Punkten bestehen, da die Rechenoperationen dann leichter auf einem Rechner implementiert und exakt ausgeführt werden können. Wenn die Kurve nur aus endlich vielen Punkten bestehen soll, aber ein eindimensionales Gebilde über dem Grundkörper K ist, dann sollte wohl auch K tunlichst nur endlich viele Elemente enthalten. Man verwendet in der Kryptographie deshalb Verallgemeinerungen des Körpers $\mathbb{F}_2 = \{0, 1\}$, den wir ganz zu Beginn kennen gelernt haben (siehe Beispiel 1.5).

Die kryptographischen Verfahren, die man mit Hilfe von elliptischen Kurven über endlichen Körpern erhält, sind weit besser, als andere Verfahren, weil das Dividieren durch ganze Zahlen in elliptischen Kurven soviel schwerer ist. Dies bedeutet, daß

man kryptographische Schlüssel verwenden kann, die deutlich kleiner sind und die deshalb im Prinzip schnelleres Rechnen erlauben. Zur Zeit ist die Bitlänge eines als sicher angesehenen Schlüssels bei der sogenannten *Elliptic Curve Cryptography* etwa um einen Faktor sechs kürzer.

Methoden der algebraischen Geometrie liefern ein wichtiges Werkzeug zur sicheren Datenübertragung. Dabei geht nicht nur simples Rechnen und manipulieren von Polynomen ein, sondern knallharte Theorie!

8 SURFEX

(VON OLIVER LABS)

Siehe Olivers Skript sowie [HL08].

LITERATUR

- [Apé87] Francois Apéry, *Models of the real projective plane*, Vieweg, 1987.
- [Bon03] Ilian Bonev, *The true origins of parallel robots*, <http://www.parallemic.org/Reviews/Review007.html>, January 2003.
- [BR79] O. Bottema and B. Roth, *Theoretical kinematics*, North-Holland Series in Applied Mathematics and Mechanics, vol. 24, North-Holland Publishing Co, Amsterdam, 1979.
- [BSW99] Albrecht Beutelspacher, Jörg Schwenk, and Klaus-Dieter Wolfenstetter, *Moderne Verfahren der Kryptographie*, 3 ed., Vieweg, 1999.
- [Cle61] Alfred Clebsch, *Zur Theorie der algebraischen Flächen*, J. Reine Angew. Math. **LIIIX** (1861), 93–108.
- [DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. on Info. Theory **IT-22** (1976), 644–654.
- [EHO⁺08] Stephan Endrass, H. Huelf, R. Oertel, R. Schmitt, K. Schneider, and J. Beigel, *Surf: A tool to visualize algebraic curves and surfaces*, Tech. report, Universtiat Mainz, 2008, <http://surf.sourceforge.net>.
- [Euk91] Euklid, *Die Elemente*, 8 ed., Bibliothek klassischer Texte, Wissenschaftliche Buchgesellschaft, 1991.
- [Fis94] Gerd Fischer, *Ebene algebraische Kurven*, Vieweg, 1994.
- [GPS05] G.-M. Greuel, G. Pfister, and H. Schönemann, *SINGULAR 3.0*, A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005, <http://www.singular.uni-kl.de>.
- [HK00] Manfred L. Husty and Adolf Karger, *Self-motions of Griffis-Duffy type parallel manipulators*, Proceedings of the 2000 IEEE International Conference on Robotics and Automation, San Francisco CA, April 2000, pp. 7–12.
- [HL08] Stephan Holzer and Oliver Labs, *SURFEX 0.90*, Tech. report, University of Mainz, University of Saarbrücken, 2008, www.surfex.AlgebraicSurface.net.
- [HRG08] Ulrich H. Hortenkamp and Jürgen Richter-Gebert, *The interactive geometry software cinderella.2*, Tech. report, Technische Universität München, 2008.
- [Lab01] Oliver Labs, *Kubische flächen und die coblesche hexaederform*, Master’s thesis, Universität Mainz, 2001.
- [LvS03] Oliver Labs and Duco van Straten, *A visual introduction to cubic surfaces using SPICY*, Algebra, Geometry and Software Systems (Michael Joswig and N. Takayama, eds.), Springer, 2003.
- [Rei92] Miles Reid, *Undergraduate algebraic geometry*, LMS Student Texts, vol. 12, LMS, 1992.
- [RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126.
- [SW05] Andrew Sommese and Charles W. Wampler, *The numerical solution of systems of polynomials arising in engineering and science*, World Scientific, 2005.
- [Wam96] Charles Wampler, *Forward displacement analysis of general six-in-parallel sps (Stewart) platform manipulators using Soma coordinates*, Mech. Mach. Theory **31** (1996), no. 3, 331–337.