Lösbarkeit algebraischer Gleichungssysteme

Frank-Olaf Schreyer
Mathematik und Informatik
Universität des Saarlandes

Einleitung

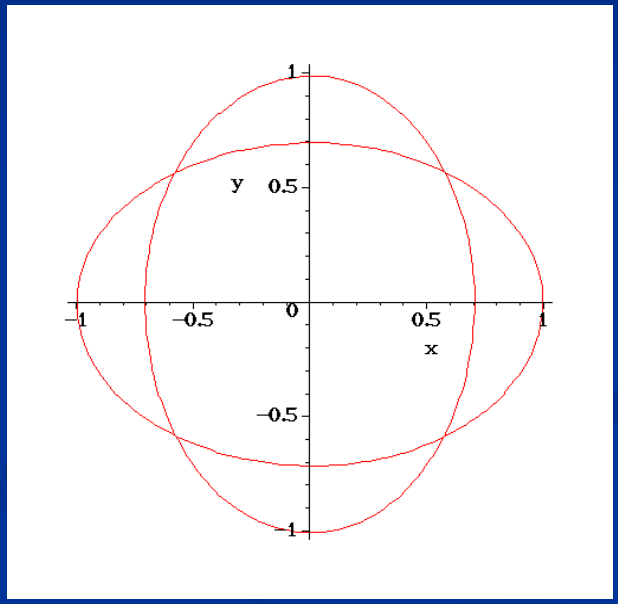
Ziel des Vortrags :

- mit Computeralgebra die Lösbarkeit algebraischer Gleichungssysteme entscheiden
- Strukturaussagen über die Lösungsmenge
  - Dimension des Lösungsraums ?
  - Anzahl der Lösungen ? (wenn endlich)
  - Parametrisierung der Lösungen, wenn möglich.

Beispiele

- Das Gleichungssystem

$$x^2+2y^2=1$$
$$2x^2+y^2=1$$



hat die 4 Lösungen :

$$(x,y) = \left(\frac{\pm\sqrt{3}}{3}, \frac{\pm\sqrt{3}}{3}\right)$$

Beispiele

- Das Gleichungssystem

$x^2+y^2=1$

$x - y = 2$

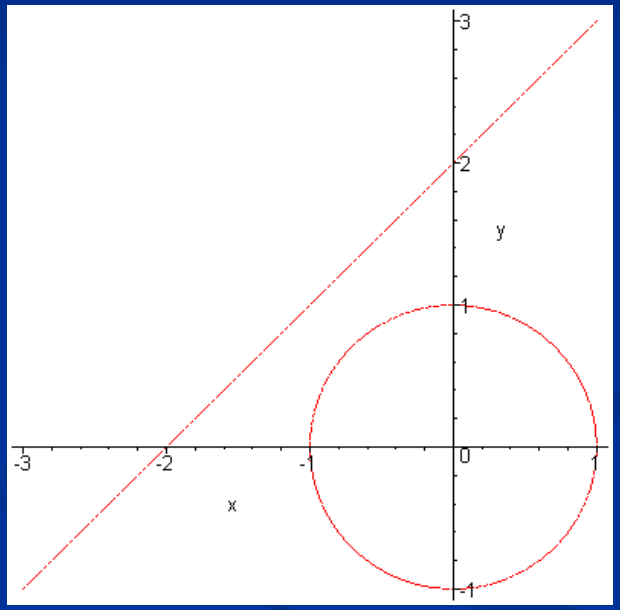
hat keine reelle Lösungen,

aber zwei komplexe:

$(1+i\,½\sqrt{2},\ 1-i\,½\sqrt{2})$

oder

$(1-i\,½\sqrt{2},\ 1+i\,½\sqrt{2})$.



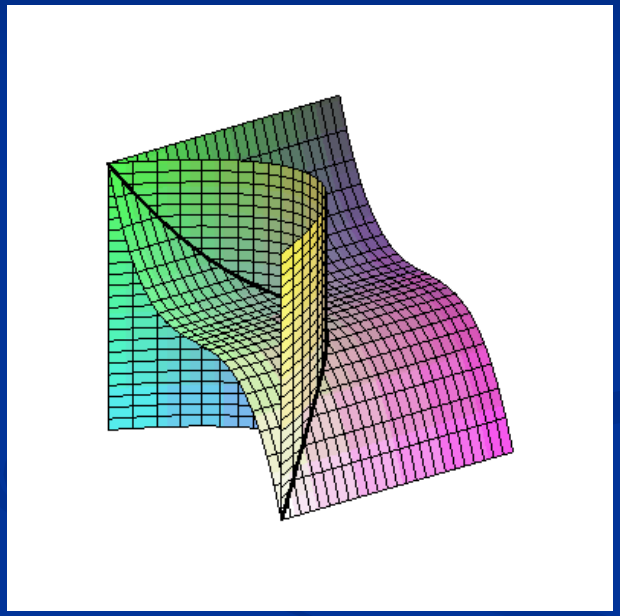
Beispiele

Das Gleichungssystem

$$y = x^2$$

$$z = x^3$$

hat eine Kurve als Lösungsmenge



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

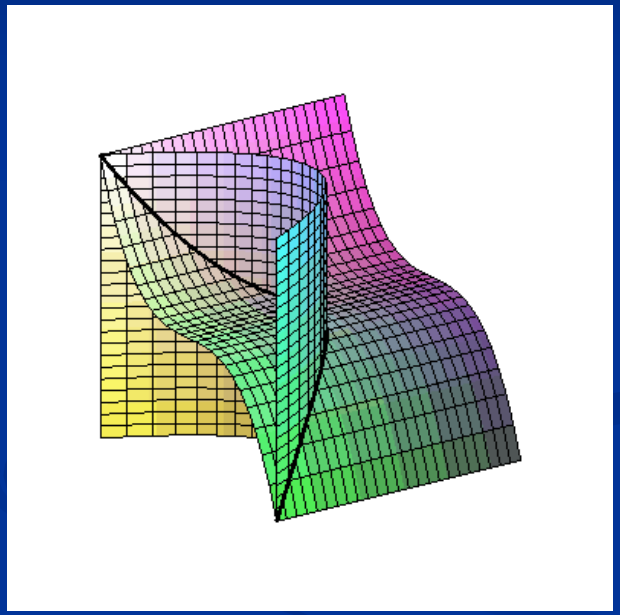
Beispiele

Das Gleichungssystem

$$y = x^2$$

$$z = x^3$$

hat eine Kurve als Lösungsmenge



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

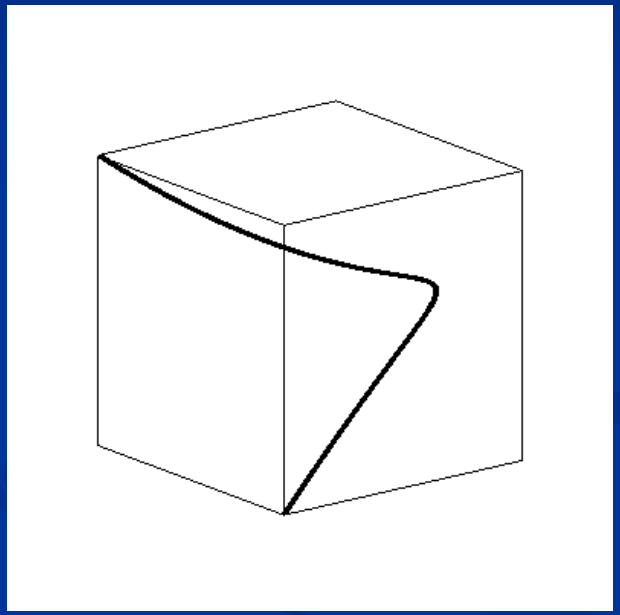
Beispiele

Das Gleichungssystem

$$y = x^2$$

$$z = x^3$$

hat eine Kurve als Lösungsmenge



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

Beispiele

Das Gleichungssystem

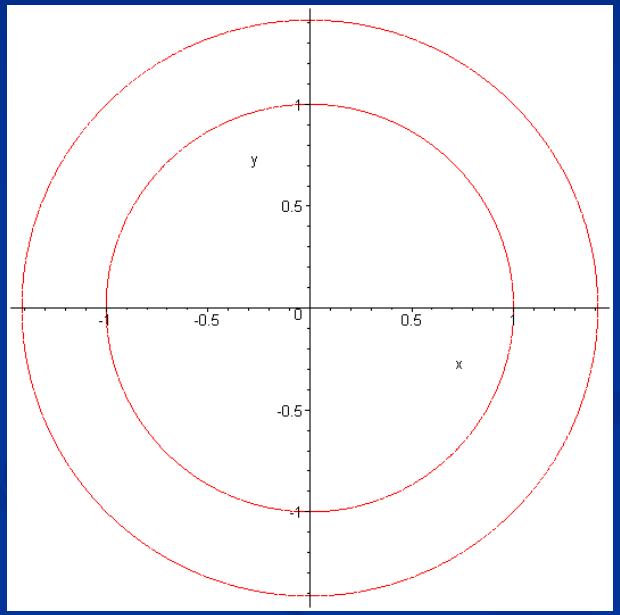
$x^2+y^2=1$

$x^2+y^2=2$

hat gar keine Lösungen,

da die Differenz der Gleichungen eine nicht lösbare Gleichung liefert:

$0=1$.



Allgemeine Aufgabenstellung

Gegeben sind endlich viele Polynome

$$f_1,\ldots,f_r \in \mathbb{Q}[x_1,\ldots,x_n]$$

in endlich vielen Variablen.

Hat das Gleichungssystem

$$f_1(x_1,\ldots,x_n)=0$$
$$\vdots$$
$$f_r(x_1,\ldots,x_n)=0$$

eine Lösung $a=(a_1,\ldots a_n) \in \mathbb{C}^n$?

Eine notwendige Bedingung

Ist $a = (a_1,\ldots,a_n) \in \mathbb{C}$ eine Lösung, dann

löst es auch jede Gleichung $f(x_1,\ldots,x_n)=0$

mit

$$f \in (f_1,\ldots,f_r) = \{g_1 f_1 + \ldots + g_r f_r : g_j \in \mathbb{Q}[x]\}$$

dem von $f_1,\ldots,f_r$ erzeugten **Ideal** im Polynomring

$$\mathbb{Q}[x] = \mathbb{Q}[x_1,\ldots,x_n] .$$

Hilbertscher Nullstellensatz

Sei k ein Körper,

$k \subseteq \mathbb{K}$ ein algebraisch abgeschlossener Oberkörper

und $f_1,\ldots, f_r \in k[x_1,\ldots,x_n]$ Polynome.

Das Gleichungssystem

$$f_1=0,\ldots, f_r=0$$

hat eine Lösung $a \in \mathbb{K}^n$ genau dann, wenn

$$1 \notin (f_1,\ldots, f_r)\,.$$

Wegen dem Nullstellensatz untersucht man die Lösungsmengen algebraischer Gleichungssysteme zunächst über dem algebraisch abgeschlossenen Körper

$$V = V(f_1,\ldots,f_r) = \{a \in \mathbb{K}^n : f_j(a) = 0\}$$

und untersucht die zweite Frage, wie

$$V(k) = V \cap k^n$$

aussieht erst anschließend.

V heißt Nullstellengebilde des Ideals und $V(k)$ die Menge der k-rationalen Punkte von V.

„Ideal membership“

Wie entscheidet man

$$1 \in (f_1,\ldots,f_r)\ ,$$

oder allgemeiner

$$f \in (f_1,\ldots,f_r)\ \ ?$$

Methode: Gröbner-Basen !

Der Gröbner-Basen Algorithmus verallgemeinert

1. Euklidischen Algorithmus in einer Variable
2. Gauß Algorithmus für lineare Gleichungssysteme.

Division mit Rest

Beispiel: Betrachten $f_1 = x^2+xy$.

- Jedes Polynom f lässt sich in der Form

$$f = gf_1 + h$$

darstellen, wobei kein Term von h durch x^2 teilbar ist.

Genauso kann man $f_2 = y^2+xy$ benutzen, um jeden durch y^2 teilbaren Term zu entfernen.

- Frage: Geht dies gleichzeitig, d.h. hat jedes f eine Darstellung

$$f = g_1f_1 + g_2f_2 + h,$$

wobei kein Term von h durch x^2 oder y^2 teilbar ist ?

- Frage: Geht dies gleichzeitig, d.h. hat jedes f eine Darstellung $f = g_1 f_1 + g_2 f_2 + h$, wobei h nur aus den Monomen 1, x, y und xy gebildet ist?

- Antwort: Nein, denn die Lösungsmenge

$$V(x^2+xy, y^2+xy) \supseteq V(x+y)$$

ist nicht endlich!

- Was lief falsch?

Wir haben die Leitterme x^2 und y^2 von

x^2+xy und y^2+xy

nicht kompatibel gewählt !

Monomordnungen

Definition Ein Monom ist ein Ausdruck

$$x^{\alpha} = x_1^{\alpha_1} x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \in k[x_1, \ldots, x_n],$$

ein Term von der Gestalt

$$c\, x^{\alpha}$$

mit $c \in k$. Eine (globale) Monomordnung ist eine vollständige Anordnung $>$ der Monome, die

1) $x^{\alpha} > x^{\beta} \Rightarrow x^{\alpha} x^{\gamma} > x^{\beta} x^{\gamma}$ und

2) $x_j > 1$ für alle j erfüllt.

Beispiele für Monomordnungen

Stets sei $x_1 > x_2 > \ldots > x_n$.

- Lexikographisch

  $x^\alpha > x^\beta \Leftrightarrow x^\alpha = x_1 \ldots x_1\ x_2 \ldots x_2 \ldots\ x_n \ldots x_n$ kommt
  α_1-mal α_2-mal α_n-mal

  vor $x^\beta = x_1 \ldots x_1 \ldots x_n \ldots x_n$ im Lexikon.
  β_1-mal β_n-mal

  Also

  $$x^2 > xy > xz > y^3 > y^2 > z > 1.$$

Beispiele für Monomordnungen

- Gewichtsordnungen

  $w_1,\ldots,w_n \in \mathbb{R}_{>0}$ $\mathbb{Q}$-linear unabhängige Gewichte.

  $$x^\alpha >_w x^\beta \Leftrightarrow \sum w_j \alpha_j > \sum w_j \beta_j$$

Beispiele für Monomordnungen

- Grad rückwärts lexikographisch

$x^\alpha >_{rlx} x^\beta \Leftrightarrow \deg x^\alpha > \deg x^\beta$ oder

$\deg x^\alpha = \deg x^\beta$ und der letzte

Exponent von $x^{\alpha-\beta}$ ist negativ.

Also

$x^2 >_{rlx} xy >_{rlx} y^2 >_{rlx} xz$.

Anders als bei lexikographisch:

$x^2 >_{lex} xy >_{lex} xz >_{lex} y^2$.

Leitterm

Gegeben eine Monomordnung $>$ und ein Polynom

$$f = \sum_{\alpha} c_{\alpha} x^{\alpha} ,$$

dann ist der Leitterm der Term

$$L(f) = c_{\beta} x^{\beta} \neq 0$$

mit dem größten Monom.

Divisionssatz

Seien $f_1,\ldots,f_r$ Polynome und $>$ eine Monomordnung auf $k[x_1,\ldots,x_n]$.
Für jedes weitere Polynom $f \in k[x_1,\ldots,x_n]$, gibt es eindeutig bestimmte Faktoren $g_1,\ldots,g_r \in k[x_1,\ldots,x_n]$ und einen eindeutigen Rest $h \in k[x_1,\ldots,x_n]$, so dass folgendes gilt:

1) $f = g_1 f_1 + \ldots g_r f_r + h$,
2) kein Term von $g_i L(f_i)$ lässt sich durch $L(f_j)$ für ein $j<i$ teilen,
3) kein Term von h lässt sich durch ein $L(f_j)$ teilen.

Beweis des Divisionssatzes

- Die Aussage ist klar, wenn $f_1,\ldots,f_r$ Monome sind:
  $\Rightarrow \exists!\ g_1^a,\ldots,g_r^a$ und h^a mit 2) und 3), so dass
  $$f = g_1^a L(f_1) + \ldots + g_r^a L(f_r) + h^a .$$
- $f^b = f - (g_1^a f_1 + \ldots + g_r^a f_r + h^a)$ hat dann einen Leitterm
  $$L(f^b) < L(f) !$$
- Mit Induktion nach $L(f)$ dürfen wir annehmen, dass
  $\exists$ Darstellung $f^b = g_1^b f_1 + \ldots + g_r^b f_r + h^b$.
  $\Rightarrow \quad g_1 = g_1^a + g_1^b, \ldots, g_r = g_r^a + g_r^b$ und $h = h^a + h^b$.

Beispiel

$f_1=x^3-xy^2$, $f_2=xy-y$ und

- $f=x^5-xy^2=x^2x^3-yxy$.

  $f=(x^2f_1-yf_2)+x^3y^2-y^2$

- $x^3y^2-y^2=y^2f_1+xy^4-y^2$
- $xy^4-y^2=y^3f_2+y^4-y^2$

Also $f=(x^2+y^2)f_1+(-y+y^3)f_2+y^4-y^2$

und $g_1=x^2+y^2$, $g_2=y^3-y$ sowie $h=y^4-y^2$

Gleiches Beispiel, andere Reihenfolge

$f_1 = xy - y$, $f_2 = x^3 - xy^2$, und

- $f = x^5 - xy^2 = x^2 x^3 - y xy$.

$f = (x^2 f_1 - y f_2) + x^3 y^2 - y^2$

- $x^3 y^2 - y^2 = x^2 y f_1 + x^2 y^2 - y^2$
- $x^2 y^2 - y^2 = xy f_1 + xy^2 - y^2$
- $xy^2 - y^2 = y f_1 + y^2 - y^2 = y f_1$

Also $f = x^2 f_2 + (-y + x^2 y + xy + y) f_1$

und $g_2 = x^2$, $g_1 = x^2 y + xy$ sowie $h = 0$.

Vergleich

- Im Allgemeinen hängt der Rest bei Division von der Reihenfolge der Polynome ab.

- Vorläufige Definition: Ein System von Polynome $f_1,\ldots,f_r$, bei denen die Reste nicht von der Reihenfolge abhängen, heißt Gröbner-Basis.

Ideal der Leitformen

Sei I ein Ideal im Polynomring $R=k[x_1,\ldots,x_n]$, d.h.

1. $f_1, f_2 \in I \Rightarrow f_1+f_2 \in I$,
2. $g \in R, f \in I \Rightarrow g f \in I$,

und $>$ eine Monomordnung.

Dann heißt

$$L(I)=(\{ L(f) \mid f \in I \})$$

das Ideal der Leitformen von I bzgl. $>$.

$L(I)$ ist ein monomiales Ideal also viel einfacher als I.

Definition: Gröbner-Basis

Seien $f_1,\ldots,f_r \in k[x_1,\ldots,x_n]$ Polynome, $>$ eine Monomordnung.

$f_1,\ldots,f_r$ sind eine Gröbner-Basis von $I=(f_1,\ldots,f_r)$, wenn

$$L(I)=(L(f_1),\ldots,L(f_r)).$$

Berechnung von Gröbner-Basen?

- $f_i , f_j \in I$. Betrachten das Monom

$$m_{ij}=ggT(L(f_i), L(f_j)).$$

In dem „S-Polynom“

$$Spol(f_i , f_j):=(L(f_j)/m_{ij}) f_i - (L(f_i)/m_{ij}) f_j$$

hebt sich der Leitterm weg !

Buchbergers Kriterium

$f_1,\ldots,f_r \in k[x_1,\ldots,x_n]$ sind eine Gröbner-Basis genau dann, wenn für alle $j<i$ das S-Polynom

$Spol(f_i, f_j) = (L(f_j)/m_{ij})\, f_i - (L(f_i)/m_{ij})\, f_j$

eine Divisionsdarstellung mit Rest $h=0$ besitzt.

Buchbergers Algorithmus

Input: $B=\{f_1,\ldots,f_r\}\subset k[x_1,\ldots,x_n]$.

Output: Gröbner-Basis.

1. Initialisiere $S:=\{(i,j)\mid i>j\}$.
2. while $S\neq\emptyset$ do (

   wähle $(i,j)\in S$; $S=S\setminus\{(i,j)\}$;

   berechne den Rest h von Spol(f_i , f_j) dividiert nach B;

   if $h\neq 0$ then ($f_{r+1}=h$; $B=B\cup\{f_{r+1}\}$;

   $S=S\cup\{(r+1,i)\mid i=1,..,r\}$; $r=r+1$));
3. Return B.

Der Algorithmus terminiert, da jedes monomiale Ideal endlich erzeugt ist.

Bemerkung

- Es reicht solche S-Paare (i,j) zu betrachten, so dass im S-Polynom $Spol(f_i, f_j) = m f_i - n f_j$ das Monom m ein Erzeuger von

  $$J_i = ((L(f_1), \ldots, L(f_{i-1})) : L(f_i))$$

  ist.

Dabei bezeichnet $(\mathcal{A} : \mathcal{B}) = \{g \in R \mid g\mathcal{B} \subseteq \mathcal{A}\}$ das Quotientenideal von $\mathcal{A}$ und $\mathcal{B}$.

- Auch geschickte Anordnung von $f_1, \ldots, f_r$ kann helfen.

Beispiel

Gegeben $f_1=x^3-xy^2$, $f_2=xy-y$ und $I=(f_1, f_2)$.

1) $J_1=(0)$, $J_2=(x^2)$.

2) $Spol(f_2, f_1) = x^2 f_2 - y f_1 = xy^3-x^2y=(y^2-x-1) f_2+y^3-y$

   $\Rightarrow$ $f_3 = y^3-y$ und $J_3=(x)$.

3. $Spol(f_3, f_2) = x f_3 - y^2 f_2 = y^3-xy = f_3 - f_2 + 0$.

$\Rightarrow$ f_1, f_2, f_3 sind eine Gröbner-Basis und

$L(I)=(x^3, xy, y^3)$.

Beweis von Buchbergers Kriterium

Notwendigkeit ist klar. Hinreichend:
Seien alle Reste von S-Polynomen Null und $f \in (f_1,\ldots,f_r)$, etwa $f=a_1 f_1+\ldots+a_r f_r$. Wir müssen $L(f) \in (L(f_1),\ldots,L(f_r))$ zeigen.

Erfüllen die a_i die Bedingung,
2) kein Term von $a_i L(f_i)$ lässt sich durch $L(f_j)$ für ein $j<i$ teilen,
dann ist dies klar.

Wir wollen die Darstellung von f in diese Form bringen.

Beweis von Buchbergers Kriterium

Dazu betrachten wir Polynomvektoren $k[x_1,\ldots,x_n]^r$ und die Abbildung

$$\varphi: k[x_1,\ldots,x_n]^r \longrightarrow k[x_1,\ldots,x_n],\ e_i \longmapsto f_i\ .$$

Terme in $k[x_1,\ldots,x_n]^r$ haben die Gestalt $x^\alpha e_i$, $e_i=(0,..,1,..0)$

Monomordnungen und Division mit Rest gibt es auch in $k[x_1,\ldots,x_n]^r$.

Zum Beispiel können wir die induzierte Monomordnung betrachten

$$x^\alpha e_i > x^\beta e_k \Leftrightarrow \quad x^\alpha L(f_i) > x^\beta L(f_k) \quad \text{oder}$$

$$x^\alpha L(f_i) = x^\beta L(f_k) \quad \text{und } i> k\ .$$

Die Divisionsdarstellung der S-Polynome gibt uns Elemente

$$G_{ij}:=(L(f_j)/m_{ij})\ e_i \ - (L(f_i)/m_{ij})\ e_j + \sum g_{ijk}\ e_k$$

Beweis von Buchbergers Kriterium

$G_{ij} := (L(f_j)/m_{ij})\, e_i - (L(f_i)/m_{ij})\, e_j + \sum g_{ijk}\, e_k \in \ker \varphi$,

da nach Vorausetzung die Division von $Spol(f_i,f_j)$ aufgeht,

$$\varphi: k[x_1,\ldots,x_n]^r \to k[x_1,\ldots,x_n],\ e_i \mapsto f_i \ .$$

Außerdem gilt $L(G_{ij}) = (L(f_j)/m_{ij})\, e_i$.

Wir betrachten nun den Rest $\sum g_i e_i$ von $\sum a_i e_i$ dividiert nach den G_{ij}´s.

Wegen $G_{ij} \in \ker \varphi$ ist

$$f = a_1 f_1 + \ldots + a_r f_r = g_1 f_1 + \ldots + g_r f_r$$

Die Koeffizienten $g_1,\ldots,g_r$ genügen 2) und die Behauptung $L(f) \in (L(f_1),\ldots,L(f_r))$ folgt.

Anwendungen

- Algorithmus, um „$1 \in (f_1, \ldots, f_r)$?“ und damit die Lösbarkeit algebraischer Gleichungssysteme zu entscheiden.
- Kriterium, das entscheidet, ob es nur endlich viele Lösungen gibt, mit Schranke für die Anzahl.
- Elimination von Variablen.
- Berechnungsmethode für die Lösungen.
- Methode, um die Dimension zu bestimmen.

Kriterium für endliche Lösungsmengen

- $I = (f_1, \ldots, f_r) \subset k[x_1, \ldots, x_n]$ ein Ideal und $k \subset \mathbb{K}$ ein algebraisch abgeschlossener Oberkörper von k.

  $$V(I) = \{a \in \mathbb{K}^n \mid f(a) = 0 \ \forall \ f \in I\}$$

  ist genau dann endlich, wenn die Menge der Monome $m \notin L(I)$ endlich ist.

- Genauer: Deren Anzahl ist eine obere Schranke für die Anzahl der Lösungen.

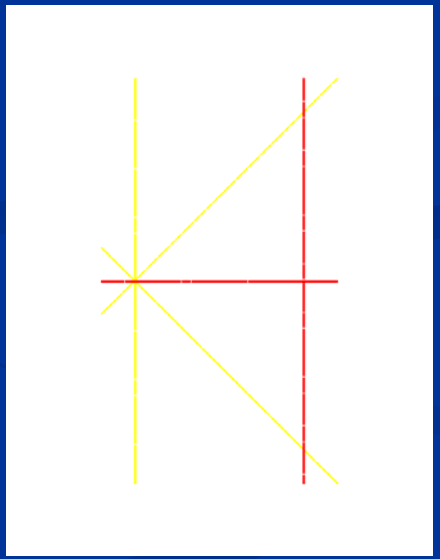
Beispiel

Im Fall $f_1=x^3-xy^2$, $f_2=xy-y$ und $I=(f_1, f_2)$ ist
$L(I)=(x^3, xy, y^3)$, also $\{m \notin L(I)\}=\{1,x,y, x^2, y^2\}$.
Es gibt also maximal 5 Lösungen.

In der Tat gibt es nur 3:

$$V(I)=\{(0,0),(1,1),(1,-1)\}.$$

Grund:
Die Lösung im Nullpunkt zählt dreifach.



Elimination von Variablen

Sei $I = (f_1,\ldots,f_r) \subseteq k[x_1,\ldots,x_n, y_1,\ldots,y_m]$.

Wir wollen die Variablen $x_1,\ldots,x_n$ von dem Gleichungssystem eliminieren.

Dazu betrachten wir $>_{lex}$ und berechnen eine Gröbner-Basis $f_1,\ldots,f_t$ von I.

Dann gilt:

- $I \cap k[y_1,\ldots,y_m] = (f_j \mid L(f_j) \in k[y_1,\ldots,y_m])$.

Grund: $L(f) \in k[y_1,\ldots,y_m] \Rightarrow f \in k[y_1,\ldots,y_m]$

Beispiel

Eliminieren x von $y-x^2=z-x^3=0$.

1. $f_1= x^2-y$; $J_1=(0)$;
2. $f_2=x^3-z$; $J_2=(1)$; $f_2-xf_1=xy-z$;
3. $f_3=xy-z$; $J_3=(x)$; $xf_3-yf_1=xz-y^2$;
4. $f_4=xz-y2$; $J_4=(x,y)$; $xf_4-zf_1+yf_3=0$;
   $yf_4-zf_3=-y^3+z^2$;
5. $f_5=y^3-z^2$; $J_5=(x)$; $xf_5-y^2f_3+zf_4=0$.

$\Rightarrow$ $(y-x^2,z-x^3)\cap k[y,z]=(y^3-z^2)$

Geometrische Interpretation

- $(y-x^2,z-x^3)\cap k[y,z] = (y^3-z^2)$

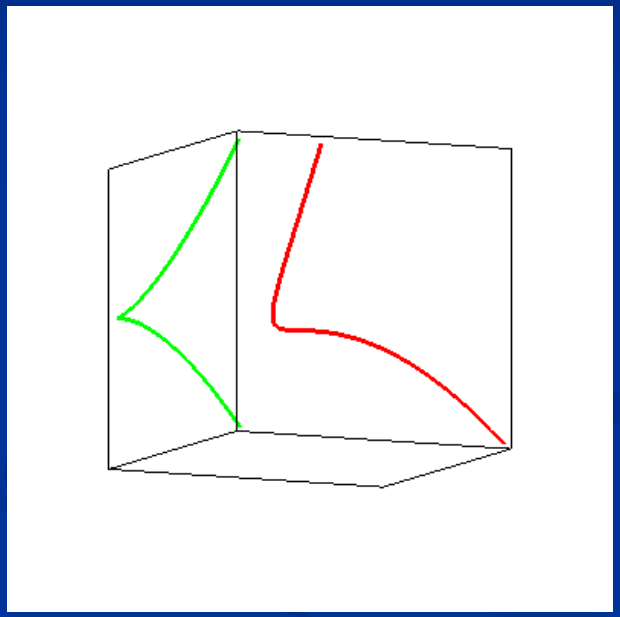
$\Rightarrow$ Die Raumkurve

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

wird auf die ebene Kurve

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

projeziert.



Berechnung von endlich vielen Lösungen

Seien n Polynome $f_1,\ldots,f_n \in \mathbb{Q}[x_1,\ldots,x_n]$ in n Variablen gegeben. In der Regel ist dann $V(f_1,\ldots,f_n) \subseteq \mathbb{C}^n$ endlich.

Berechnen wir eine lexikographische Gröbner-Basis, so hat diese in der Regel Dreiecksgestalt.

$x_1-h_1(x_2,\ldots,x_n)$, $x_2-h_2(x_3,\ldots,x_n)$,

$\ldots$, $x_{n-1}-h_{n-1}(x_n)$, $f(x_n)$.

$f(x_n)=0$ können wir dann etwa numerisch oder symbolisch lösen, und sukzessives Einsetzen gibt die Lösungsmenge.

Beispiel

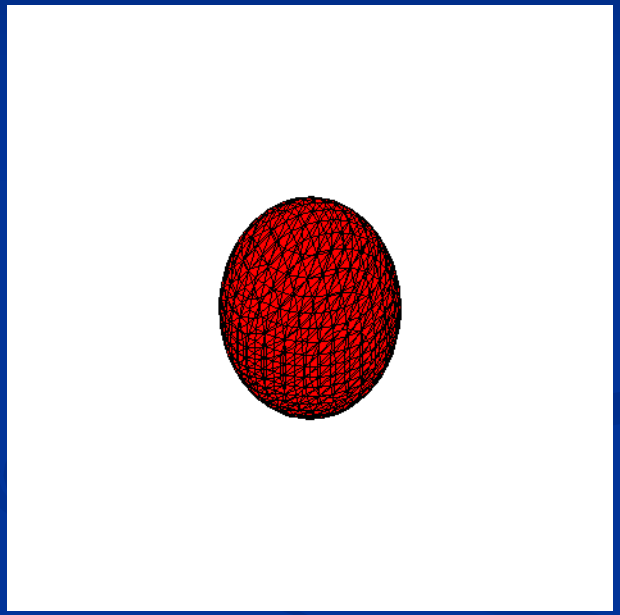
Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$

Beispiel

Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$

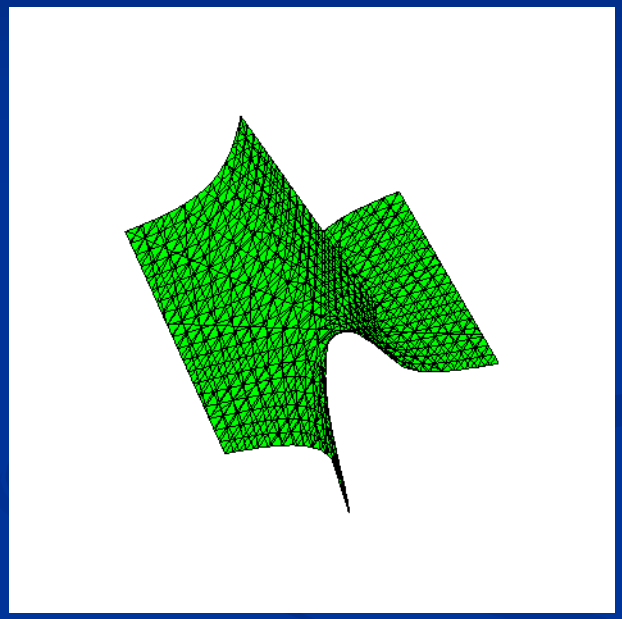


Ellipsoid

Beispiel

Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$

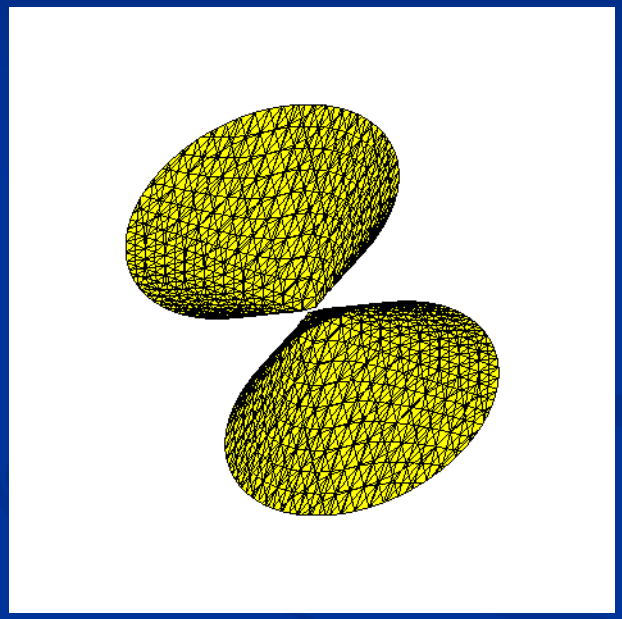


Hyperboloid

Beispiel

Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$

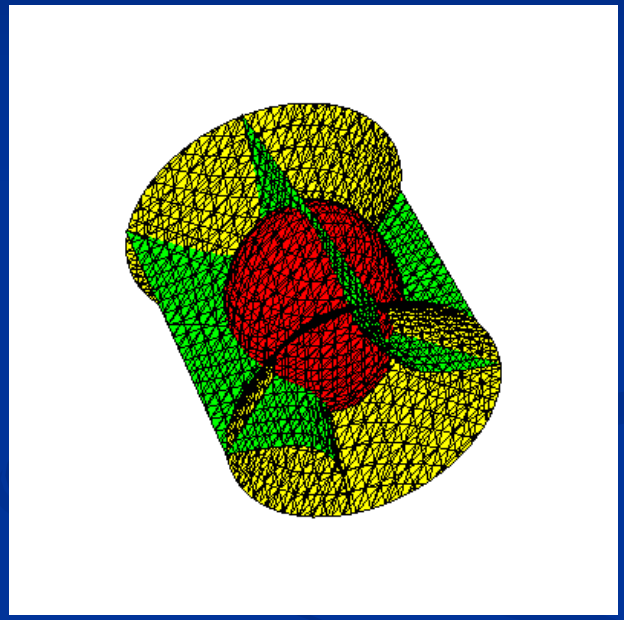


Kegel

Beispiel

Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$



Lexikographische Gröbner-Basis ist

$x-2yz,$

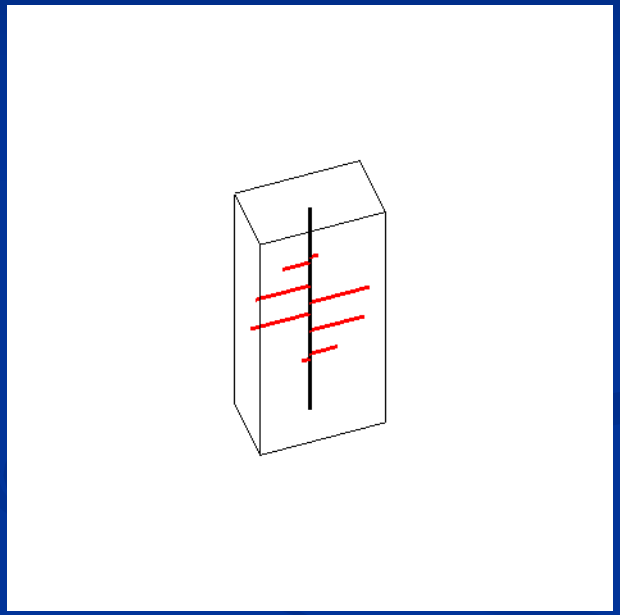
$y+18/17z^7-147/17z^5+2695/136z^3-2433/272z,$

$z^8- 49/6\ z^6+2797/144\ z^4 -1633/144\ z^2+269/576.$

Beispiel

Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$



Lexikographische Gröbner-Basis ist

$x-2yz$,

$y+18/17z^7-147/17z^5+2695/136z^3-2433/272z$,

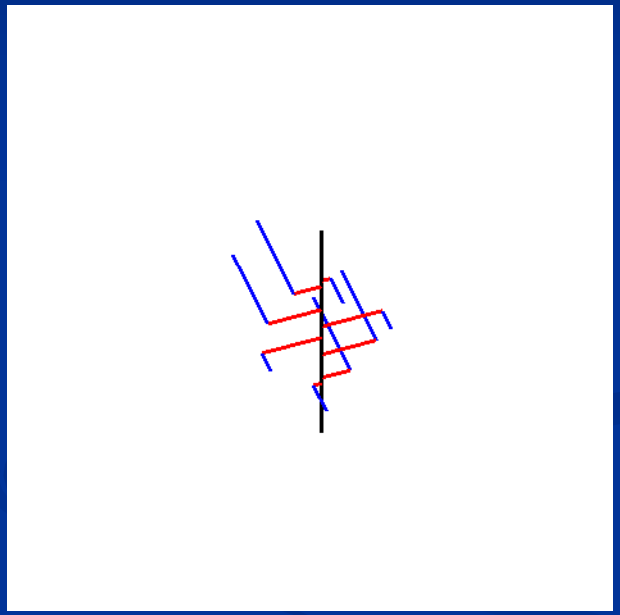
$z^8- 49/6\ z^6+2797/144\ z^4 -1633/144\ z^2+269/576$.

Die letzte Gleichung hat 8 Nullstellen.

Beispiel

Betrachten

- $4(x-1)^2+4y^2+2z^2-25=0$
- $x-2yz=0$
- $(x-1)^2-y^2-z^2=0$



Lexikographische Gröbner-Basis ist

$x-2yz$,

$y+18/17z^7-147/17z^5+2695/136z^3-2433/272z$,

$z^8- 49/6\ z^6+2797/144\ z^4 -1633/144\ z^2+269/576$.

Die letzte Gleichung hat 8 Nullstellen.

Satz von Bezout

Die Anzahl der Lösungen von n Gleichungen vom Grad $d_1,\ldots,d_n$ in n Unbestimmten ist falls endlich höchstens

$$d_1 d_2 \ldots d_n \ .$$

Im Beispiel: 3 Quadriken, $2^3=8$ Lösungen.

Dimension

Sei $I=(f_1,\ldots,f_r) \subseteq \mathbb{Q}[x_1,\ldots,x_n]$. Wenn

1. $L(I)$ die Potenzen x_j^N für $j=1,\ldots,n-d$ enthält, und
2. $L(I) \cap \mathbb{Q}[x_{n-d+1},\ldots,x_n] = (0)$, gilt,

dann ist $V(I)$ d-dimensional und die Projektion

$$V(I) \to \mathbb{C}^d,\ a=(a_1,\ldots,a_n) \mapsto (a_{n-d+1},\ldots,a_n)$$

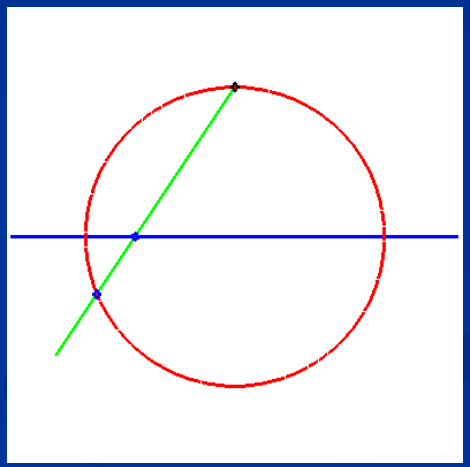
endlich und surjektiv.

Nach einem genügend allgemeinen Koordinatenwechsel wird diese Situation stets erreicht.

Parametrisierungen

Gelegentlich lassen sich Lösungsmengen rational parametrisieren.

Beispiel : der Kreis



Projektion vom Nordpol liefert

$\mathbb{R} \to V(x^2+y^2-1)\ ,\ t \mapsto (2t/(t^2+1)\ ,(t^2-1)/(t^2+1))$

Parametrisierungen

Sei $V=V(f_1,..,f_r)$ eine d-dimensionale Lösungsmenge.

- Frage: Können wir V parametrisieren?

  D.h. Gibt es eine (rationale) Abbildung

  $$\varphi: \mathbb{K}^d \cdots\!\!\rightarrow V$$

  mit dichten Bild ?

- Antwort: Im allgemeinen nicht, es gibt schon topologische Hindernisse !

Parametrisierbarkeitsbedingung

Notwendig und hinreichend für die Parametrisierbarkeit einer ebenen Kurve C vom Grad d ist $g=0$. Dabei ist

$$g := (d-1)(d-2)/2 - \sum_{p \in C} r_p(r_p-1)/2$$

wobei r_p = die Multiplizität von C in p ist und die Summe $\sum_{p \in C}$ über alle Punkte von C läuft, z.B. auch solche im „Unendlichen“, d.h. am Horizont.

Beispiel

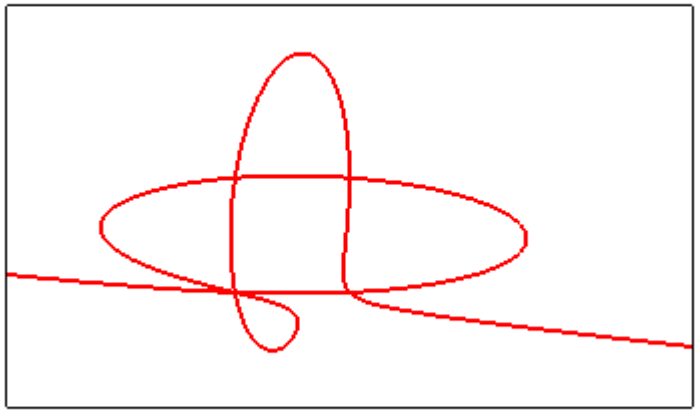
- Frage: Lässt sich

$$x^5+10x^4y+20x^3y^2+130xy^3-20xy^4+20y^5-2x^4-40x^3y-150x^2y^2$$
$$-90xy^3-40y^4+x^3+30x^2y+110xy^2+20y^3=0$$

parametrisieren ?

- Antwort: Ja, denn

$$g = (d-1)(d-2)/2 - \sum r_p(r_p-1)/2$$
$$= 6 - 3 - 1 - 1 - 1 = 0$$



Beispiel

- Wir wollen

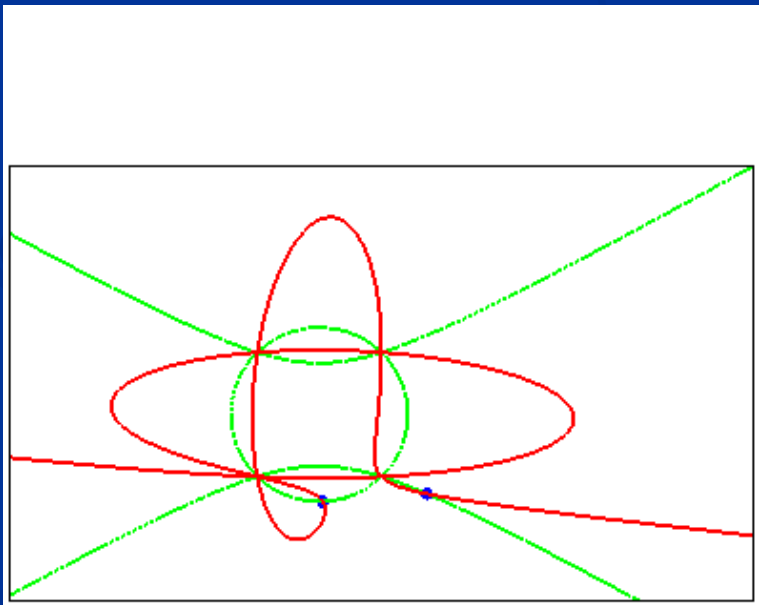
$x^5+10x^4y+20x^3y^2+130xy^3-20xy^4+20y^5-2x^4-40x^3y-150x^2y^2$
$-90xy^3-40y^4+x^3+30x^2y+110xy^2+20y^3=0$

parametrisieren. Wie ?

- Idee: Betrachten Quadriken durch die singulären Punkte:

$\Rightarrow$ 5*2 -3-2-2-2 = 1

$\Rightarrow$ Ein beweglichen Punkt nach Bezout.



Beispiel

- Wir wollen

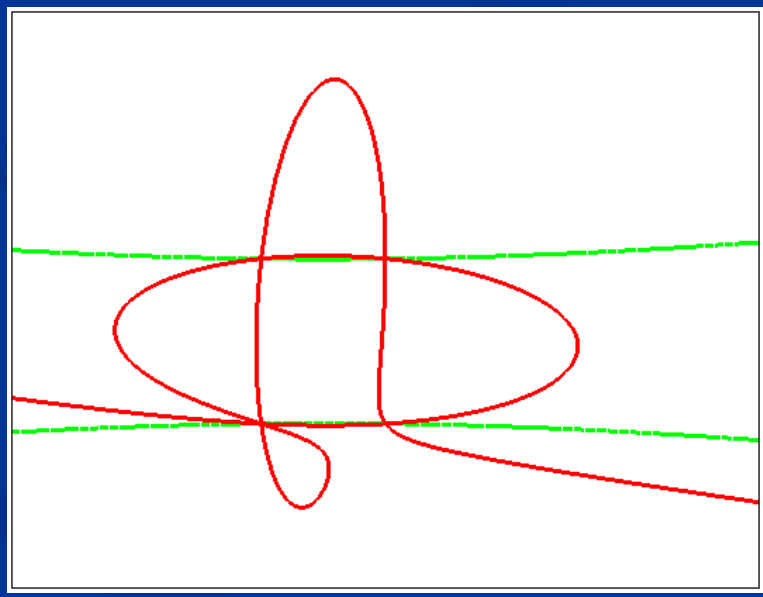
$x^5+10x^4y+20x^3y^2+130xy^3-20xy^4+20y^5-2x^4-40x^3y-150x^2y^2$
$-90xy^3-40y^4+x^3+30x^2y+110xy^2+20y^3=0$

parametrisieren. Wie ?

- Idee: Betrachten Quadriken durch die singulären Punkte:

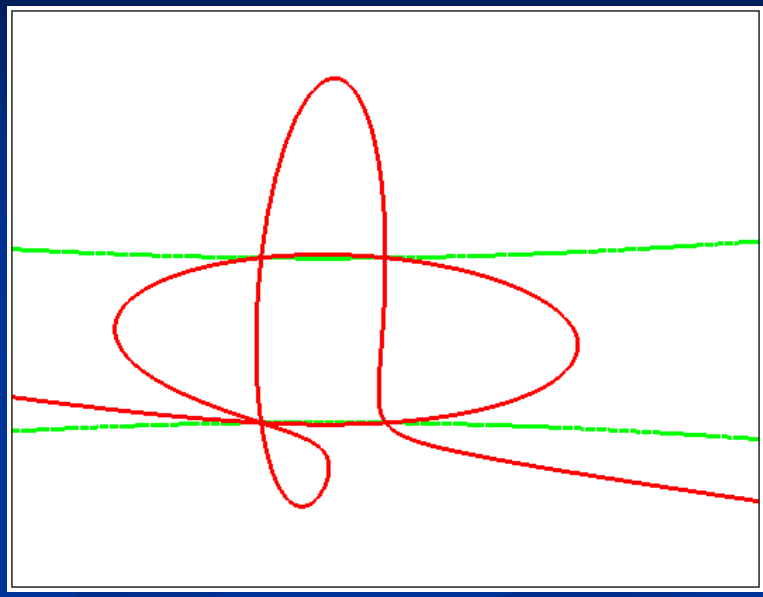
$\Rightarrow$ 5*2 -3-2-2-2 = 1

Ein beweglicher Punkt nach Bezout.



Beispiel

- Elimination liefert die Position des zusätzlichen Punkt in Abhängigkeit vom Parameter t der Quadriken.



$$x(t)=\frac{t^5+12t^4+151/4t^3+251/20t^2+43/40t+1/40}{t^5+12t^4+181/4t^3+28/5t^2+3/20t-1/400}$$

$$y(t)=\frac{t^5+9/2t^4-81/20t^3-69/40t^2-1/8t-1/400}{t^5+12t^4+181/4t^3+28/5t^2+3/20t-1/400}$$

Zusammenfassung

Wir haben gesehen, wie man mit Computeralgebra die

- Lösbarkeit algebraischer Gleichungssysteme entscheidet,
- Dimension und Anzahl der Lösungen bestimmt,
- eventuell eine Parametrisierung der Lösungsmenge berechnen kann.

- Hilfsmittel waren Gröbner-Basen, deren Berechnung den Euklidischen und Gaußschen Algorithmus verallgemeinert.

Computeralgebra Systeme

- Maple
- Macaulay2
- Singular

(Links auf meiner Homepage).

Literatur

- Cox, Little, O`Shea : Ideals, Varieties and Algorithms

Undergraduate Text in Mathematics, Springer Verlag 1991