## Lösungen nichtlinearer Gleichungssysteme mit Resultanten

Die klassische Aufgabe der Algebra besteht in der Lösung von Gleichungen und Gleichungssystemen. Im Falle eines Systems von Polynomgleichungen in mehreren Veränderlichen kann die Lösungsmenge sehr kompliziert sein; ist sie unendlich, kann man sie möglicherweise nicht einmal explizit angeben. Schon im Falle von nur einer Polynomgleichung in zwei Veränderlichen ist die Lösungsmenge im Allgemeinen eine Kurve. In einfachen Fällen wie $x^2 + y^2 = 1$ können wir diese identifizieren, hier als Kreis um den Nullpunkt mit Radius eins. Bei einer irreduziblen Gleichung eines hinreichend hohen Grades wird es sich aber oft um eine nicht in Parameterform angebbare Kurve ohne Namen handeln, und wenn wir – wie meist in der Computeralgebra – über einem kleinen Körper wie dem der rationalen Zahlen arbeiten, kann es sehr schwer sein, auch nur zu entscheiden, ob und gegebenenfalls wie viele rationale Lösungen es gibt. So ist beispielsweise die erst 1994 von ANDREW WILES bewiesene FERMATsche Vermutung äquivalent dazu, daß die Gleichung $x^n + y^n = 1$ über $\mathbb{Q}$ für ungerades $n \geq 3$ nur die beiden Lösungen $(0, 1)$ und $(1, 0)$ hat; für gerades $n \geq 4$ gibt es die vier Lösungen $(0, \pm 1)$ und $(\pm 1, 0)$. Über $\mathbb{R}$ ist die Lösungsmenge für gerades $n$ eine geschlossene Kurve, die im Quadrat mit Ecken $(\pm 1, \pm 1)$ liegt und sich diesem mit wachsendem $n$ immer mehr annähert; für ungerade $n$ haben wir den Graph der Funktion $y = \sqrt[n]{1 - x^n}$, was aber nur daran liegt, daß für ungerades $n$ die Gleichung $y^n = a$ für jedes $a \in \mathbb{R}$ genau eine reelle Lösung hat. Über anderen Körpern können die Lösungsmengen ganz anders aussehen.

Algorithmen zur Lösung nichtlinearer Gleichungssysteme gibt es daher vor allem in dem Fall, daß das Gleichungssystem auch über einem algebraisch abgeschlossenen Körper, der den Grundkörper enthält, nur endlich viele Lösungen hat. Dann kann man versuchen, diese Lösungen explizit aufzuzählen. Wie wir sehen werden, gelingt dies modulo des Problems, die Nullstellenmengen von Polynomen einer Veränderlichen zu finden. Für Polynome ab dem Grad fünf sind die Nullstellen zwar im Allgemeinen nicht durch Wurzelausdrücke in den Koeffizienten darstellbar, aber falls man etwa reelle Lösungen sucht, gibt es Algorithmen, um Intervalle zu finden die jeweils genau eine Nullstelle

enthalten, und es gibt auch Algorithmen, um mit reellen Zahlen zu rechnen, die gegeben sind durch ein Polynom, das in dieser Zahl verschwindet, und ein Intervall, in dem es keine weitere Nullstelle gibt.

Wenn die Lösungsmenge zumindest über einem algebraisch abgeschlossenen Körper unendlich ist, muß man sich meist damit begnügen, das Gleichungssystem auf eine möglichst einfache Form zu bringen, der man möglichst viele Eigenschaften der Lösungsmenge ansehen kann; an eine explizite Bestimmung ist meist nicht zu denken.

Im wesentlichen gibt es zwei Strategien zum Umgang mit nichtlinearen Gleichungssystemen: Resultanten und GRÖBNER-Basen. Heute befassen wir uns mit dem seit dem 19. Jahrhundert bekannten Ansatz mit Resultanten; nach Ostern wird es dann um GRÖBNER-Basen gehen.

Wie wir bereits wissen, haben zwei Polynome $f, g \in R[X]$ über einem faktoriellen Ring $R$ genau dann einen gemeinsamen Faktor positiven Grades in $R[X]$, wenn ihre Resultante verschwindet. Dies können wir anwenden, um aus einem System nichtlinearer Gleichungen eine Variable zu eliminieren und es so sukzessive auf Gleichungen in einer Veränderlichen zurückzuführen.

Betrachten wir zunächst den Fall von zwei Gleichungen in zwei Unbekannten. Wir haben also zwei Polynome $f, g \in k[X, Y]$ über dem Körper $k$ und suchen die Menge aller Paare $(x, y) \in k^2$ (oder auch in $K^2$ für einen größeren Körper $K$, der $k$ enthält), für die $f(x, y) = g(x, y) = 0$ ist.

Wir betrachten ein festes $x \in k$ und setzen diesen Wert in $f$ und $g$ für die Variable $X$ ein. Die resultierenden Polynome aus $k[Y]$ seien $\overline{f}(Y) = f(x, Y)$ und $\overline{g}(Y) = g(x, Y)$. Falls es eine Lösung $(x, y)$ mit dem betrachteten $x$ gibt, haben $\overline{f}$ und $\overline{g}$ die gemeinsame Nullstelle $y$, also den gemeinsamen Faktor $Y - y$, und damit verschwindet ihre Resultante $\mathrm{Res}_Y(\overline{f}, \overline{g}) \in k$. Wir wollen diese Resultante mit $\mathrm{Res}_Y(f, g) \in k[X]$ in Verbindung bringen.

Dazu schreiben wir

$$f = a_d Y^d + \cdots + a_1 Y + a_0 \qquad \text{und} \qquad g = b_e Y^e + \cdots b_1 Y + b_0$$

mit Polynomen $a_0, \ldots, a_d, b_0, \ldots, b_e \in k[X]$. Dann ist

$$\overline{f} = a_d(x)Y^d + \cdots + a_1(x)Y + a_0(x)$$

und

$$\overline{g} = b_e(x)Y^e + \cdots b_1(x)Y + b_0(x)\,.$$

Falls weder $a_d(x)$ noch $b_e(x)$ verschwinden, sind $\overline{f}$ und $\overline{g}$ Polynome vom Grad $d$ bzw. $e$, und ihre Resultante ist

$$\begin{vmatrix} a_d(x) & a_{d-1}(x) & \ldots & a_0(x) & 0 & \ldots & 0 \\ 0 & a_d(x) & \ldots & a_1(x) & a_0(x) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_d(x) & a_{d-1}(x) & \ldots & a_0(x) \\ b_e(x) & b_{e-1}(x) & \ldots & b_0(x) & 0 & \ldots & 0 \\ 0 & b_e(x) & \ldots & b_1(x) & b_0(x) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_e(x) & b_{e-1}(x) & \ldots & b_0(x) \end{vmatrix}.$$

Da eine Determinante nach dem LAPLACEschen Entwicklungssatz als eine alternierende Summe von geeigneten Produkten ihrer Einträge geschrieben werden kann, hat sie genau den Wert, den wir auch erhalten, wenn wir die Resultante von $f$ und $g$ bezüglich $Y$ berechnen und dann in dieses Polynom aus $k[X]$ den Wert $x$ einsetzen.

Betrachten wir als nächstes den Fall, daß $a_d(x) = 0$, aber $b_e(x) \neq 0$ ist. Dann hat zwar $\overline{g}$ noch den Grad $e$, aber der Grad von $\overline{f}$ ist kleiner als $d$; er sei etwa gleich $r$. $\mathrm{Res}_Y(\overline{f}, \overline{g})$ entsteht aus obiger Determinante, indem wir die ersten $(d-r)$ Spalten und die ersten $(d-r)$ Zeilen mit Koeffizienten von $g$ streichen, also die $(e+1)$-te bis $(e+d-r)$-te Zeile.

In der obigen Determinante ist, wenn $a_d(x)$ verschwindet, $b_e(x)$ der einzige von Null verschiedene Eintrag in der ersten Spalte. Wir können daher die Determinante nach der ersten Spalte entwickeln und erhalten $(-1)^e b_e(x)$ mal der Determinante, die aus der obigen durch Streichen der ersten Spalte und der $(e+1)$-ten Zeile entsteht.

Falls $r \leq e-2$ ist, steht auch in der ersten Zeile der neuen Determinante wieder $b_e(x)$ als einziger von Null verschiedener Eintrag, wir können

also wieder nach der ersten Spalte entwickeln, und so weiter. Insgesamt erhalten wir die Formel

$$\mathrm{Res}_Y(f,g)(x) = (-1)^{(d-r)e} b_e(x)^{d-r} \,\mathrm{Res}_Y(\overline{f},\overline{g})\,.$$

Da wir angenommen haben, daß $b_e(x)$ nicht verschwindet, verschwindet somit $\mathrm{Res}_Y(\overline{f},\overline{g})$ in diesem Fall genau dann, wenn $x$ eine Nullstelle von $\mathrm{Res}_Y(f,g) \in k[X]$ ist.

Im Fall, daß zwar $b_e(x)$ verschwindet, nicht aber $a_d(x)$, können wir genauso argumentieren und erhalten bis auf den Vorzeichenfaktor $(-1)^{(d-r)e}$, der hier wegfällt, ein analoges Ergebnis.

Bleibt noch der Fall, daß sowohl $a_d(x)$ als auch $b_e(x)$ verschwinden. In diesem Fall stehen in obiger Determinante in der ersten Spalte lauter Nullen, die Determinante verschwindet also unabhängig davon, ob $\mathrm{Res}_Y(\overline{f},\overline{g})$ verschwindet oder nicht. Insgesamt haben wir somit das folgende Ergebnis:

**Lemma:** $\mathrm{Res}_Y(f,g) \in k[X]$ verschwindet genau dann an der Stelle $x \in k$, wenn $\mathrm{Res}_Y(\overline{f},\overline{g}) = 0$ ist oder wenn $a_d(x)$ und $b_e(x)$ beide verschwinden. ∎

Mit etwas mehr Schreibaufwand, aber ansonsten genau mit der gleichen Rechnung, folgt allgemeiner

**Lemma:** $f, g \in k[X_1, \ldots, X_n]$ seien zwei Polynome in $n \geq 2$ Variablen, $(x_1, \ldots, x_{n-1})$ sei ein Punkt aus $k^{n-1}$, und $\overline{f}, \overline{g}$ seien die Polynome aus $k[X_n]$, die entstehen, wenn für $X_1, \ldots, X_{n-1}$ die Werte $x_1, \ldots, x_{n-1}$ eingesetzt werden. Dann verschwindet die Resultante $\mathrm{Res}_{X_n}(f,g) \in k[X_1, \ldots, X_{n-1}]$ genau dann an der Stelle $(x_1, \ldots, x_{n-1}) \in k^{n-1}$, wenn $\mathrm{Res}_{X_n}(\overline{f},\overline{g})$ verschwindet oder wenn bei der Darstellung von $f$ und $g$ als Polynom in $X_n$ über $k[X_1, \ldots, X_{n-1}]$ beide führende Koeffizienten im Punkt $(x_1, \ldots, x_{n-1})$ verschwinden. ∎

Dies wollen wir anwenden auf ein nichtlineares Gleichungssystem

$$f_1(X_1, \ldots, X_n) = \cdots = f_m(X_1, \ldots, X_n) = 0\,.$$

Wir nehmen an, $(x_1, \ldots, x_n) \in k^n$ sei eine Lösung.

Betrachten wir die Polynome $f_i$ als Polynome in $X_n$ mit Koeffizienten aus $k[X_1, \ldots, X_{n-1}]$, so können wir in diesen Koeffizienten $X_1 = x_1, \ldots, X_{n-1} = x_{n-1}$ setzen und erhalten so Polynome $\overline{f}_i \in k[X_n]$. Alle diese Polynome verschwinden in $x_n$; je zwei dieser Polynome haben also (mindestens) $(X_n - x_n)$ als gemeinsamen Faktor. Daher verschwindet die Resultante $\mathrm{Res}_{X_n}(\overline{f}_i, \overline{f}_j)$. Nach dem gerade bewiesenen Lemma ist somit $(x_1, \ldots, x_{n-1})$ eine Nullstelle des Polynoms

$$r_{ij} \underset{\text{def}}{=} \mathrm{Res}_{X_n}(f_i, f_j) \in k[X_1, \ldots, X_{n-1}] \,.$$

Damit können wir, zumindest im Fall einer endlichen Lösungsmenge, die Lösung des obigen Gleichungssystems zurückführen auf die eines Gleichungssystems in nur $n - 1$ Variablen: Wir lösen zunächst das Gleichungssystem

$$r_{ij}(X_1, \ldots, X_{n-1}) = 0 \quad \text{für } 1 \leq j < i \leq m$$

und setzen dann nacheinander jede Lösung $(x_1, \ldots, x_{n-1})$ in die $f_i$ ein. Wir erhalten ein Gleichungssystem

$$\overline{f}_1(X_n) = \cdots = \overline{f}_m(X_n) = 0$$

in einer Veränderlichen; seine Lösungen, falls es welche gibt, sind gerade die Nullstellen des größten gemeinsamen Teilers der $\overline{f}_i$. Sind $z_1, \ldots, z_p$ diese Nullstellen, so sind

$$(x_1, \ldots, x_{n-1}, z_1), \quad \ldots, \quad (x_1, \ldots, x_{n-1}, z_p)$$

Lösungen des ursprünglichen Gleichungssystems.

Das System der $\frac{1}{2}m(m-1)$ Gleichungen $r_{ij}$ in $n-1$ Variablen können wir auf die gleiche Weise zurückführen auf ein Gleichungssystem in $n-2$ Variablen, und so weiter, bis wir bei einem Gleichungssystem in nur einer Variablen angelangt sind.

Man beachte, daß nicht jede Lösung des Gleichungssystems in einer Variablen weniger zu einer Lösung des Ausgangssystems führen muß: Zum einen folgt aus dem Verschwinden von $\mathrm{Res}_{X_n}(f_i, f_j)$ nicht, daß auch $\mathrm{Res}_{X_n}(\overline{f}_i, \overline{f}_j)$ verschwinden muß; nach obigem Lemma könnte es

auch sein, daß einfach die beiden führenden Koeffizienten verschwinden. Zum anderen folgt aus dem Verschwinden von $\mathrm{Res}_{X_n}(\overline{f}_i, \overline{f}_j)$ nicht, daß $\overline{f}_i$ und $\overline{f}_j$ eine gemeinsame Nullstelle haben müssen, sondern nur, daß sie einen gemeinsamen Faktor haben. Dieser gemeinsame Faktor könnte im Falle $k = \mathbb{R}$ etwa $X^2 + 1$ sein und somit keine Nullstelle in $k$ haben.

Letzteres Problem können wir umgehen, wenn wir auch Lösungen aus Erweiterungskörpern $K$ von $k$ zulassen, allerdings müssen wir dabei beachten, daß nach Einsetzen eines Werts $x_n \in K$ für $X_n$ das Polynome $f_i(X_1, \ldots, X_{n-1}, x_n)$ im Allgemeinen nicht mehr in $k[X_1, \ldots, X_{n-1}]$ liegt, sondern im größeren Polynomring $K[X_1, \ldots, X_{n-1}]$. Wir müssen dann also im nächsten Schritt im größeren Körper $K$ rechnen, was erheblich aufwendiger sein kann als das Rechnen in $k$.

Selbst über einem algebraisch abgeschlossenen Körper kann es immer noch Probleme mit der Erweiterbarkeit von Lösungen geben: Verschwinden im Falle von drei Gleichungen $f_1, f_2, f_3$ die Resultanten $\mathrm{Res}_{X_n}(f_1, f_2)$, $\mathrm{Res}_{X_n}(f_1, f_3)$ und $\mathrm{Res}_{X_n}(f_2, f_3)$ alle drei in einem Punkt $(x_1, \ldots, x_n)$, so könnte es immer noch sein, daß es drei Elemente $z_1, z_2, z_3 \in k$ gibt, so daß

$$
\begin{aligned}
f_1(x_1, \ldots, x_{n-1}, z_2) &= f_1(x_1, \ldots, x_{n-1}, z_3) = 0\,, \\
\text{aber} \quad f_1(x_1, \ldots, x_{n-1}, z_1) &\neq 0\,, \\
f_2(x_1, \ldots, x_{n-1}, z_1) &= f_2(x_1, \ldots, x_{n-1}, z_3) = 0\,, \\
\text{aber} \quad f_2(x_1, \ldots, x_{n-1}, z_2) &\neq 0 \quad \text{und} \\
f_3(x_1, \ldots, x_{n-1}, z_1) &= f_3(x_1, \ldots, x_{n-1}, z_2) = 0\,, \\
\text{aber} \quad f_3(x_1, \ldots, x_{n-1}, z_3) &\neq 0
\end{aligned}
$$

ist, d.h. $\overline{f}_1$ und $\overline{f}_2$ haben die gemeinsame Nullstelle $z_3$, $\overline{f}_1$ und $\overline{f}_3$ die gemeinsame Nullstelle $z_2$ und $\overline{f}_2$ und $\overline{f}_3$ die gemeinsame Nullstelle $z_1$, ohne daß es eine gemeinsame Nullstelle aller drei Polynome geben muß.

Als einfaches Beispiel für die Lösung eines nichtlinearen Gleichungssystems mit Resultanten betrachten wir ein System aus zwei Gleichun-

gen in zwei Unbekannten über $\mathbb{Q}$; die beiden Gleichungen seien

$$x^2 + 2y^2 + 8x + 8y - 40 = 0 \qquad \text{und}$$
$$3x^2 + y^2 + 18x + 4y - 50 = 0\,.$$

Betrachten wir $Y$ als die erste und $X$ als die zweite Variable, müssen wir nach obigem Algorithmus die Resultante der beiden Polynome

$$f = \; X^2 + 2Y^2 + 8X + 8Y - 40 = 0 \qquad \text{und}$$
$$g = 3X^2 + Y^2 + 18X + 4Y - 50 = 0$$

aus $\mathbb{Q}[X, Y]$ bezüglich $X$ bestimmen. Die Berechnung der entsprechenden $4 \times 4$-Determinante (oder ein Computeralgebraisystem) führt zum Ergebnis

$$\mathrm{Res}_X(f, g) = 25Y^4 + 200Y^3 - 468Y^2 - 3472Y + 6820\,.$$

Die Nullstellen

$$y = -2 \pm \frac{1}{5}\sqrt{534 \pm 24\sqrt{31}}$$

dieses Polynom vierten Grades finden wohl nur Wenige ohne Einsatz eines Computeralgebrasystems; wenn wir nur an rationalen Lösungen interessiert sind, zeigt das Ergebnis, daß unser Gleichungssystem keine rationalen Lösungen hat.

Meist interessieren wir uns aber für alle komplexen Nullstellen; in diesem Fall müssen wir übergehen zu einem Körper $K$, der die Nullstellen der Resultante enthält (Wer Algebra gehört hat, sieht leicht, daß der Zerfällungskörper $K$ der Resultante über $\mathbb{Q}$ hier Grad vier hat). Dort haben wir die beiden Polynome $f(X, y)$ und $g(X, y) \in K[X]$, und bei Polynomen großen Grades würden wir deren ggT bilden, um dessen Nullstellen zu berechnen.

Hier sind beide Geichungen nur quadratisch; daher geht es schneller, wenn wir eine davon lösen und die beiden Lösungen in die zweite einsetzen. Wir wissen, daß mindestens eine auch Nullstelle das anderen Polynoms sein muß; es könnten aber auch beide sein. (Der Fall, daß beide führenden Koeffizienten verschwinden, kann hier nicht auftreten, denn die Koeffizienten von $X^2$ sind die Konstanten eins und drei.)

Da wir beim Lösen einer quadratischen Gleichung eine Quadratwurzel ziehen müssen, kann es sein, daß wir hierbei den Körper noch einmal erweitern müssen.

Einfacher wird es, wenn wir $Y$ statt $X$ eliminieren:

$$\mathrm{Res}_Y(f,g) = (5X^2 + 28X - 60)^2$$

ist das Quadrat eines quadratischen Polynoms, dessen Nullstellen

$$x = -\frac{14}{5} \pm \frac{4}{5}\sqrt{31}$$

uns die wohlbekannte Lösungsformel liefert. Diese Werte können wir nun in $f$ oder $g$ einsetzen, die entstehende Gleichung lösen und das Ergebnis ins andere Polynom einsetzen.

Alternativ können wir auch mit *beiden* Resultanten arbeiten: Ist $(x,y)$ eine gemeinsame Nullstelle von $f$ und $g$, so muß $x$ eine Nullstelle von $\mathrm{Res}_Y(f,g)$ sein und $y$ eine von $\mathrm{Res}_X(f,g)$. Da es nur $4 \times 2 = 8$ Kombinationen gibt, können wir diese hier einfach durch Einsetzen testen. Wie sich zeigt, hat das System die vier Lösungen

$$\left(-\frac{14}{5} + \frac{4}{5}\sqrt{31},\ -2 - \frac{1}{5}\sqrt{534 - 24\sqrt{31}}\right)$$
$$\left(-\frac{14}{5} + \frac{4}{5}\sqrt{31},\ -2 + \frac{1}{5}\sqrt{534 - 24\sqrt{31}}\right)$$
$$\left(-\frac{14}{5} - \frac{4}{5}\sqrt{31},\ -2 - \frac{1}{5}\sqrt{534 + 24\sqrt{31}}\right)$$
$$\left(-\frac{14}{5} - \frac{4}{5}\sqrt{31},\ -2 + \frac{1}{5}\sqrt{534 + 24\sqrt{31}}\right).$$