Kapitel 2
Systeme von nichtlinearen Polynomgleichungen

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 und, sofern sie unendlich ist, möglicherweise nicht einmal explizit angebbar: Im Gegensatz zum Fall linearer Gleichungen können wir hier im allgemeinen keine endliche Menge von Lösungen finden, durch die sich alle anderen Lösungen ausdrücken lassen. Trotzdem gibt es Algorithmen, mit denen sich nichtlineare Gleichungssysteme deutlich vereinfachen lassen, und zumindest bei endlichen Lösungsmengen lassen sich diese auch konkret angeben – sofern wir die Nullstellen von Polynomen einer Veränderlichen explizit angeben können.

§1: Variablenelimination mit Resultanten

Wir wissen aus Kapitel 1, daß zwei Polynome $f, g \in R[X]$ über einem faktoriellen Ring R genau dann einen gemeinsamen Faktor haben, 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 $(x, y) \in k^2$, 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 ist; 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

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

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. Dann entsteht $\mathrm{Res}_Y(\overline{f}, \overline{g})$ aus obiger Determinante, indem wir die ersten $(d - r)$ Spalten und die ersten $(d - r)$ Zeilen mit Koeffizienten von g streichen.

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 Determinate, 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, auch das gleiche 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 nichlineares 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 Gleichunssystems 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 Gleichungssystem mit den r_{ij} können wir auf die gleiche Weise zurückführen auf eines 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 $Res_{X_n}(f_i, f_j)$ nicht, daß auch $\text{Res}_{X_n}(\overline{f}_i, \overline{f}_j)$ verschwinden muß; nach obigem Lemma könnte es auch sein, daß einfach die beiden führenden Koeffizienten verschwinden. Zum anderen folgt aus dem Verschwinden von $\text{Res}_{X_n}(\overline{f}_i, \overline{f}_j)$ 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 verschwindet, wenn wir über einem sogenannten algebraisch abgeschlossenen Körper arbeiten:

Definition: Ein Körper k heißt *algebraisch abgeschlossen*, wenn jedes Polynom positiven Grades aus $k[X]$ mindestens eine Nullstelle in k hat.

Induktiv folgt leicht, daß über einem algebraisch abgeschlossenen Körper jedes Polynom in ein Produkt von Linearfaktoren zerfällt:

Lemma: Ist k algebraisch abgeschlossen und $f \in k[X]$ ein Polynom vom Grad $d > 0$, so gibt es Elemente $a_d, z_1, \ldots . z_d \in k$ derart, daß

$$f = a_d(X - z_1) \cdots (X - z_d)$$

ist.

Beweis: Im Falle $d = 1$ ist das klar; sei also $d > 1$. Da k algebraisch abgeschlossen ist, hat f eine Nullstelle z_d. Teilen wir f mit Rest durch $(X - z_d)$, erhalten wir eine Darstellung $f = q \cdot (X - z_d) + r$, wobei $\deg r < \deg(X - z_d) = 1$ ist, d.h. r ist eine Konstante. Setzen wir $X = z_d$ ein, folgt, daß $r = f(z_d) = 0$ ist, d.h. $f = q \cdot (X - z_d)$ ist durch $X - z_d$ teilbar. Der Quotient q hat Grad $d - 1$, läßt sich also nach Induktionsvoraussetzung schreiben als $q = a_d(X - z_1) \cdots (X - z_{d-1})$, woraus die behauptete Darstellung von f folgt. ∎

Auch 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 alle drei Resultanten

$\mathrm{Res}_{X_n}(f_1, f_2)$, $\mathrm{Res}_{X_n}(f_1, f_3)$ und $\mathrm{Res}_{X_n}(f_2, f_3)$, so könnte es immer noch sein, daß es drei verschiedene Elemente $z_1, z_2, z_3 \in k$ gibt derart, daß $\overline{f}_1$ und $\overline{f}_2$ die gemeinsame Nullstelle z_1 haben, $\overline{f}_1$ und $\overline{f}_3$ die gemeinsame Nullstelle z_2 und $\overline{f}_2$ und $\overline{f}_3$ die gemeinsame Nullstelle z_3, 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 Gleichungen in zwei Unbekannten; die beiden Gleichungen seien

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

Betrachten wir Y als die erste und X als die zweite Variable, müssen wir nach obigem Algorithmus die Resultante bezüglich X berechnet; Maple gibt uns das Ergebnis

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

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

Diese können wir beispielsweise in g einsetzen, die entstehende quadratische Gleichung für x lösen, um dann zu testen, ob das Lösungspaar (x, y) auch eine Nullstelle von g ist. Zumindest mit Maple ist das durchaus machbar. Einfacher wird es aber, 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. (Wir könnten natürlich auch zunächst den ggT der beiden durch Einsetzen entstandenen Polynome bilden, aber den hier betrachteten kleinen Graden lohnt sich der Aufwand für einen EUKLIDischen Algorithmus nicht.)

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

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

§2: Gleichungssysteme und Ideale

Wenn wir lineare Gleichungssysteme mit dem GAUSS-Algorithmus lösen, verändern wir das Gleichunssystem sukzessive, indem wir Gleichungen so durch Linearkombinationen mit anderen Gleichungen ersetzen, daß sich an der Lösungemenge nichts ändert. Die sämtlichen linearen Gleichungen in n Unbekannten über einem Körper k bilden einen $(n+1)$-dimensionalen Vektorraum, in dem die Gleichungen eines linearen Gleichungssystems einen Untervektorraum erzeugen. Dieser besteht aus allen Linearkombinationen der gegebenen Gleichungen, und das sind gleichzeitig alle linearen Gleichungen, die auf der Lösungsmenge des linearen Gleichungssystems verschwinden. Zwei lineare Gleichungssysteme haben somit genau dann die gleiche Lösungsmenge, wenn sie den gleichen Untervektorraum erzeugen.

Wenn wir Systeme nichtlinearer Gleichungen betrachten, können wir Gleichungen nicht nur mir Konstanten multiplizieren, sondern auch mit Polynomen. Anstelle von Untervektorräumen sollten wir daher andere Strukturen betrachten, die sogenannten Ideale:

Definition: Eine nichtleere Teilmenge I eines kommutativen Rings R heißt *Ideal*, in Zeichen $I \lhd R$, wenn gilt:
1.) Für je zwei Elemente $f, g \in I$ ist auch $f + g \in I$
2.) Für jedes $f \in I$ und jedes $r \in R$ liegt auch rf in I.

Bei den Produkten verlangen wir also, daß sie bereits dann in R liegen, wenn nur *ein* Faktor in R liegt. Wenn wir die Elemente von R als Gleichungen interpretieren, zum Beispiel als Polynome, die verschwinden sollen, ist das in der Tat sinnvoll: Wenn wir eines der Polynome mit irgendeinem beliebigen Polynom multiplizieren, verschwindet es immer noch auf der Lösungsmenge der Gleichung.

Die Bedingung, daß ein Ideal mindestens ein Element enthalten muß, können wir auch ersetzen durch die Bedingung, daß es die Null von R enthalten muß, denn wenn es irgendein Element $f \in R$ enthält, muß es gemäß der zweiten Bedingung auch $0 \cdot f = 0$ enthalten.

Um mit dem Idealbegriff vertraut zu werden, betrachten wir zunächst Ideale im Ring der ganzen Zahlen:

Lemma: Zu jedem Ideal $I \lhd \mathbb{Z}$ gibt es eine ganze Zahl $n \in \mathbb{Z}$, so daß $I = \{nq | q \in \mathbb{Z}\}$.

Beweis: I ist nach Definition nicht leer, enthält also mindestens ein Element. Falls I nur aus der Null besteht, können wir $n = 0$ setzen und sind fertig. Wenn es ein Element $m \neq 0$ gibt, enthält das Ideal auch dessen sämtliche ganzzahlige Vielfachen, insbesondere also gibt es in I dann positive Zahlen. Die kleinste dieser Zahlen sei n. Wir wollen uns überlegen, daß I genau aus den ganzzahligen Vielfachen von n besteht.

Dazu sei $m \in I$ ein beliebiges Element von I. Wir dividieren m mit Rest durch q; das Ergebnis sei

$$m : n = q \quad \text{Rest } r \quad \text{mit} \quad 0 \leq r < n \,.$$

Dann liegt mit m und n auch $r = m - qn$ in I und ist echt kleiner als n. Da n die kleinste positive Zahl in I ist, muß daher $r = 0$ sein, d.h. $m = qn$ ist ein ganzzahliges Vielfaches von n.

■

Definition: *a)* Ist R ein Ring und $f \in R$ so bezeichnen wir

$$(f) \underset{\text{def}}{=} \{rf \mid r \in R\}$$

als das von f erzeugte *Hauptideal.*
b) R heißt *Hauptidealring,* wenn jedes Ideal von R ein Hauptideal ist.

Wie wir gerade gesehen haben, ist also $\mathbb{Z}$ ein Hauptidealring.

Allgemeiner definieren wir

Definition: Ist R ein Ring und ist $M \subset R$ eine Teilmenge von R, so ist das *von M erzeugte Ideal* (M) das kleinste Ideal von R, das M enthält, d.h. den Durchschnitt aller Ideale, die M enthalten. Für eine endliche Menge $M = \{f_1, \ldots, f_m\}$ schreiben wir (M) kurz als $(f_1, \ldots, f_m)$. Die Menge M bezeichnen wir als ein *Erzeugendensystem* des Ideals I.

Diese Definition macht nicht wirklich klar, wie das von M erzeugte Ideal aussieht. Da uns in der Computeralgebra nur endlich erzeugte Ideale interessieren, möchte ich mich auf diesen Fall beschränken; die Verallgemeinerung auf beliebige Mengen M sollte für jeden, der den folgenden Beweis verstanden hat, offensichtlich sein.

Lemma: $\left(f_1, \ldots, f_m\right) = \left\{ \sum_{i=1}^{m} r_i f_i \;\middle|\; r_i \in R \right\}$

Beweis: Da jedes Ideal, das $f_1, \ldots, f_m$ enthält, auch für $r_1, \ldots, r_m \in R$ die Elemente $r_i f_i$ enthält und damit auch deren Summe, ist klar, daß die rechte Seite in jedem Ideal enthalten ist, das die f_i enthält. Außerdem ist die rechtsstehende Menge selbst ein Ideal: Da sie die f_i enthält, ist sie nicht leer; die Summe zweier Elemente ist offensichtlich wieder ein Element, da wir einfach die Koeffizienten addieren müssen, und wenn wir ein Element mit einem beliebigen Element $r \in R$ multiplizieren, werden einfach alle Koeffizienten mit r multipliziert. Somit ist die rechte Seite in der Tat das kleinste Ideal, das alle f_i enthält. ∎

Sei nun $R = k[X_1, \ldots, X_n]$ der Polynomring in n Variablen über einem Körper k,und seien $f_1, \ldots, f_m \in R$ Polynome. Wir interessieren uns für die Lösungsmenge des durch die f_i gegebenen Gleichungssystems,

also die Menge aller $(x_1, \ldots, x_n) \in k^n$, für die alle f_i verschwinden. Wir definieren gleich allgemein

Definition: Die Nullstellenmenge einer Teilmenge $M \subseteq k[X_1, \ldots, X_n]$ ist

$$V(M) \underset{\text{def}}{=} \left\{(x_1, \ldots, x_n) \in k^n \;\middle|\; f(x_1, \ldots, x_n) = 0 \text{ für alle } f \in M\right\}.$$

Im Falle eine endlichen Menge $M = \{f_1, \ldots, f_m\}$ schreiben wir kurz $V(f_1, \ldots, f_m)$.

(In der algebraischen Geometrie bezeichnet man Mengen dieser Art als Varietäten; daher der Buchstabe V.)

Lemma: Ist $I = (f_1, \ldots, f_m)$ das von den f_i erzeugte Ideal, so ist

$$V(I) = V(f_1, \ldots, f_m).$$

Beweis: Da alle f_i in I liegen, ist natürlich $V(I) \subseteq V(f_1, \ldots, f_m)$. Umgekehrt sei $(x_1, \ldots, x_n)$ ein Element von $V(f_1, \ldots, f_m)$ und g irgendein Element von I. Nach dem vorigen Lemma gibt es Polynome $r_i \in R$; so daß $g = \sum_{i=1}^{m} r_i f_i$ ist. Damit ist auch

$$g(x_1, \ldots, x_n) = \sum_{i=1}^{m} r_i(x_1, \ldots, x_m) f_i(x_1, \ldots, x_m) = 0,$$

so daß $(x_1, \ldots, x_n)$ in $V(I)$ liegt. Damit ist das Lemma bewiesen. ∎

Dieses Lemma zeigt, daß zwei Gleichungssysteme

$$f_1(x_1, \ldots, x_n) = 0, \quad \ldots, \quad f_m(x_1, \ldots, x_n) = 0$$

und

$$g_1(x_1, \ldots, x_n) = 0, \quad \ldots, \quad g_r(x_1, \ldots, x_n) = 0$$

die gleiche Lösungsmenge haben, wenn die Ideale $(f_1, \ldots, f_m)$ und $(g_1, \ldots, g_r)$ übereinstimmen.

Die Umkehrung dieser Aussage ist allerdings falsch. Ein einfaches Gegenbeispiel haben wir bereits bei nur einer Gleichung in einer Variablen: Die Gleichungen

$$x = 0, \qquad x^2 = 0, \qquad x^3 = 0, \qquad \ldots$$

haben allesamt nur die Null als Lösung, aber natürlich sind die Ideale $(x^d) \lhd k[X]$ für verschiedene Werte von d verschieden. Gegen Ende dieses Kapitels werden wir diese Frage, wann so etwas vorkommt, genauer untersuchen.

Zum Abschluß dieses Paragraphen soll nur noch kurz festgehalten werden, wie sich Ideale und Nullstellenmengen zueinander verhalten. Dazu müssen wir zunächst die Summe und das Produkt zweier Ideale definieren:

Definition: *a)* Die Summe $I + J$ zweier Ideale I, J eines Rings R ist das kleinste Ideal, das sowohl I als auch J enthält.
b) Das Produkt IJ dieser Ideale ist das kleinste Ideal, das alle Produkte fg mit $f \in I$ und $g \in J$ enthält.

Man überlegt sich leicht (mit dem gleichen Argument, mit dem wir das Ideal $(f_1, \ldots, f_m)$ oben explizit bestimmt haben), daß $I + J$ gerade die Menge aller $f + g$ mit $f \in I$ und $g \in J$ ist; IJ dagegen enthält im allgemeinen auch Elemente, die sich *nicht* in der Form fg mit $f \in I$ und $g \in J$ darstellen lassen: Ist etwa $I = J = (X, Y) \lhd \mathbb{R}[X, Y]$, so enthält IJ mit $X^2 = X \cdot X$ und $Y^2 = Y \cdot Y$ auch deren Summe $X^2 + Y^2$, die sich nicht als Produkt zweier Polynome aus $\mathbb{R}[X, Y]$ schreiben läßt. Wenn wir $\mathbb{R}$ durch $\mathbb{C}$ ersetzen, läßt sich $X^2 + Y^2$ zwar zerlegen als $(X + iY)(X - iY)$, aber auch in $\mathbb{C}[X, Y]$ gibt es irreduzible Polynome in $(X, Y) \cdot (X, Y)$, die sich somit nicht als Produkt darstellen lassen. In IJ liegen daher auch alle (endlichen) Summen der Form $\sum f_i g_i$ mit $f_i \in I$ und $g_i \in J$; da diese (analog zum obigen Argument) ein Ideal bilden, besteht IJ genau aus diesen Summen.

Satz: Für zwei Ideale I, J im Polynomring $R = k[X_1, \ldots, X_n]$ gilt
a) Ist $I \subseteq J$, so ist $V(J) \subseteq V(I)$
b) $V(I + J) = V(I) \cap V(J)$
c) $V(IJ) = V(I) \cup V(J)$

Beweis: a) Sei $(x_1, \ldots, x_n) \in V(J)$. Dann verschwindet $f(x_1, \ldots, x_n)$ für alle $f \in J$, erst recht also für alle $f \in I$, d.h. $(x_1, \ldots, x_n) \in V(I)$.

b) Da $I + J$ das kleinste Ideal ist, das sowohl I als auch J enthält, liegt $V(I + J)$ nach *a)* sowohl in $V(I)$ als auch in $V(J)$, also auch in deren Durchschnitt. Liegt umgekehrt ein Punkt $(x_1, \ldots, x_n)$ sowohl in $V(I)$ als auch in $V(J)$, so liegt er auch in $V(I + J)$, denn wie wir gerade gesehen haben, läßt sich jedes Element von $I + J$ schreiben als $f + g$ mit $f \in I$ und $g \in J$, und sowohl f als auch g verschwinden im Punkt $(x_1, \ldots, x_n)$.

c) Da IJ erzeugt wird von den Produkten fg mit $f \in I$ und $g \in J$ und jedes dieser Produkte sowohl in I als auch in J liegt, ist IJ eine Teilmenge sowohl von I als auch von J; somit liegt $V(I) \cup V(J)$ nach *a)* in $V(IJ)$. Umgekehrt sei $(x_1, \ldots, x_n) \in V(IJ)$, liege aber nicht in $V(I)$. Dann gibt es ein $f \in I$ mit $f(x_1, \ldots, x_n) \neq 0$. Für jedes $g \in J$ liegt aber fg in IJ, so daß das Produkt $f(x_1, \ldots, x_n)g(x_1, \ldots, x_n)$ verschwinden muß. Da die Funktionswerte im Körper k liegen und der Faktor $f(x_1, \ldots, x_n)$ nicht verschwindet, muß $g(x_1, \ldots, x_n) = 0$ sein für alle $g \in J$; der Punkt liegt also in $V(J)$. Somit liegt er in jedem Fall in $V(I) \cup V(J)$.

■

§3: Gauß und Euklid

Kehren wir zurück zur Lösung nichtlinearer Gleichungssysteme. Die in §1 skizzierte Methode mit Resultanten war bereits im 19. Jahrhundert wohlbekannt. Der im Rest dieses Kapitels vorgestellte alternative Ansatz wurde erst 1966 von dem österreichischen Mathematiker BRUNO BUCHBERGER entwickelt; auch sein Ansatz hat, genau wie die Theorie der Resultanten, Anwendungen, die weit über das Problem der Lösung nichtlinearer Gleichungssysteme hinausgehen. In der Tat wurde die Grundidee des Verfahrens bereits knapp vor BUCHBERGER, und ohne daß dieser davon wußte, von dem japanischen Mathematiker HEISUKE HIRONAKA entdeckt, der es für ein klassisches Problem der algebraischen Geometrie entwickelte: Für die damit bewiese sogenannte Auflösung der Singularitätens einer algebraischen Varietät über einem Körper der Charakteristik null erhielt HIRONAKA 1970 die Fields-Medaille, die damals höchste Auszeichnung der Mathematik.

Ausgangspunkt sind der GAUSS-Algorithmus zur Lösung linearer Gleichungssysteme und der Algorithmus zur Polynomdivision, wie er im EUKLIDischen Algorithmus zur Berechnung des ggT zweier Polynome verwendet wird:

Wenn wir ein lineares Gleichungssystem durch GAUSS-Elimination lösen, bringen wir es zunächst auf eine Treppengestalt, indem wir die erste vorkommende Variable aus allen Gleichungen außer der ersten eliminieren, die zweite aus allen Gleichungen außer den ersten beiden, uns so weiter, bis wir schließlich Gleichungen haben, deren letzte entweder nur eine Variable enthält oder aber eine Relation zwischen Variablen, für die es sonst keine weiteren Bedingungen mehr gibt. Konkret sieht ein Eliminationsschritt folgendermaßen aus: Wenn wir im Falle der beiden Gleichungen

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = u \tag{1}$$

$$b_1x_1 + b_2x_2 + \cdots + b_nx_n = v \tag{2}$$

die Variable X_1 mit Hilfe von (1) aus (2) eliminieren wollen, ersetzen wir die zweite Gleichung durch ihre Summe mit $-b_1/a_1$ mal der ersten. Die theoretische Rechtfertigung für diese Umformung besteht darin, daß das Gleichungssystem bestehend aus (1) und (2) sowie das neue Gleichungssystem dieselbe Lösungsmenge haben, und daran ändert sich auch dann nichts, wenn noch weitere Gleichungen dazukommen.

Ähnlich können wir vorgehen, wenn wir ein nichtlineares Gleichungssystem in nur einer Variablen betrachten: Am schwersten sind natürlich die Gleichungen vom höchsten Grad, also versuchen wir, die zu reduzieren auf Polynome niedrigeren Grades. Das kanonische Verfahren dazu ist die Polynomdivision: Haben wir zwei Polynome

$$f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \quad \text{und}$$

$$g = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$$

mit $m \leq n$, so dividieren wir f durch g, d.h. wir berechnen einen Quotienten q und einen Rest r derart, daß $f = qg + r$ ist und r kleineren Grad als g hat. Konkret: Bei jedem Divisionsschritt haben wir ein Polynom

$$f = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0\,,$$

das wir mit Hilfe des Divisors

$$g = b_e X^e + b_{e-1} X^{e-1} + \cdots + b_1 X + b_0$$

reduzieren, indem wir es ersetzen durch

$$f - \frac{b_e}{a_d} X^{d-e} g \,,$$

und das führen wir so lange fort, bis f auf ein Polynom von kleinerem Grad als g reduziert ist: Das ist dann der Divisionsrest r. Auch hier ist klar, daß sich nichts an der Lösungsmenge ändert, wenn man die beiden Gleichungen f, g ersetzt durch g, r, denn

$$f = qg + r \quad \text{und} \quad r = f - qg \,,$$

d.h. f und g verschwinden genau dann für einen Wert x, wenn g und r an der Stelle x verschwinden.

In beiden Fällen ist die Vorgehensweise sehr ähnlich: Wir vereinfachen das Gleichungssystem schrittweise, indem wir eine Gleichung ersetzen durch ihre Summe mit einem geeigneter Vielfachen einer anderen Gleichung.

Dieselbe Strategie wollen wir auch anwenden Systeme von Polynomgleichungen in mehreren Veränderlichen. Erstes Problem dabei ist, daß wir nicht wissen, wie wir die Monome eines Polynoms anordnen sollen und damit, was der führende Term ist. Dazu gibt es eine ganze Reihe verschiedener Strategien, von denen je nach Anwendung mal die eine, mal die andere vorteilhaft ist. Wir wollen uns daher zunächst damit beschäftigen.

§4: Monomordnungen und der Divisionsalgorithmus

Wir betrachten Polynome in n Variablen $X_1, \ldots, X_n$ und setzen zur Abkürzung

$$X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \quad \text{mit} \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0 \,.$$

Terme der Form X^α bezeichnen wir als *Monome;* der Grad des Monoms X^α ist die Summe der α_i.

Eine Anordnung der Monome ist offensichtlich äquivalent zu einer Anordnung auf $\mathbb{N}_0^n$, und es gibt sehr viele Möglichkeiten, diese Menge anzuordnen. Für uns sind allerdings nur Anordnungen interessant, die einigermaßen kompatibel sind mit der algebraischen Struktur des Polynomrings $k[X_1, \ldots, X_n]$; beispielsweise wollen wir sicherstellen, daß der führende Term des Produkts zweier Polynome das Produkt der führenden Terme der Faktoren ist – wie wir es auch vom Eindimensionalen her gewohnt sind. Daher definieren wir

Definition: *a)* Eine Monomordnung ist eine Ordnungsrelation „$<$“ auf $\mathbb{N}_0^n$, für die gilt

1. „$<$“ ist eine Linear- oder Totalordnung, d.h. für zwei Elemente $\alpha, \beta \in \mathbb{N}_0^n$ ist entweder $\alpha < \beta$ oder $\beta < \alpha$ oder $\alpha = \beta$.
2. Für $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ gilt $\alpha < \beta \Longrightarrow \alpha + \gamma < \beta + \gamma$.
3. „$<$“ ist eine Wohlordnung, d.h. jede Teilmenge $I \subseteq \mathbb{N}_0^n$ hat ein kleinstes Element.

b) Für ein Polynom $f = \sum_{\alpha \in I} c_\alpha X^\alpha \in k[X_1, \ldots, X_n]$ mit $c_\alpha \neq 0$ für alle $\alpha \in I \subset \mathbb{N}_0$ sei γ das größte Element von I bezüglich einer fest gewählten Monomordnung. Dann bezeichnen wir bezüglich dieser Monomordnung

- γ = multideg f als Multigrad von f
- X^γ = FM f als führendes Monom von f
- c_γ = FK f als führenden Koeffizienten von f
- $c_\gamma X^\gamma$ = FT f als führenden Term von f

Der Grad deg f von f ist, wie in der Algebra üblich, der höchste Grad eines Monoms von f; je nach gewählter Monomordnung muß das nicht unbedingt der Grad des führenden Monoms sein.

Beispiele von Monomordnungen sind

a) Die lexikographische Ordnung: Hier ist $\alpha < \beta$ genau dann, wenn für den ersten Index i, in dem sich α und β unterscheiden, $\alpha_i < \beta_i$ ist. Betrachtet man Monome X^α als Worte über dem (geordneten) Alphabet $\{X_1, \ldots, X_n\}$, kommt hier ein Monom X^α genau dann vor X^β, wenn die entsprechenden Worte im Lexikon in dieser Reihenfolge gelistet

werden. Die ersten beiden Forderungen an eine Monomordnung sind klar, und auch die Wohlordnung macht keine großen Probleme: Man betrachtet zunächst die Teilmenge aller Exponenten $\alpha \in I$ mit kleinstmöglichem α_1, unter diesen die Teilmenge mit kleinstmöglichem α_2, *usw.*, bis man bei α_n angelangt ist. Spätestens hier ist die verbleibende Teilmenge einelementig, und ihr einziges Element ist das gesuchte kleinste Element von I.

b) Die graduierte lexikographische Ordnung: Hier ist der Grad eines Monoms erstes Ordnungskriterium: Ist $\deg X^\alpha < \deg X^\beta$, so definieren wir $\alpha < \beta$. Falls beide Monome gleichen Grad haben, soll $\alpha < \beta$ genau dann gelten, wenn α im lexikographischen Sinne kleiner als β ist. Auch hier sind offensichtlich alle drei Forderungen erfüllt.

c) Die inverse lexikographische Ordnung: Hier ist $\alpha < \beta$ genau dann, wenn für den *letzten* Index i, in dem sich α und β unterscheiden. Das entspricht offensichtlich gerade der lexikographischen Anordnung bezüglich des rückwärts gelesenen Alphabets $X_n, \ldots, X_1$. Entsprechend läßt sich natürlich auch bezüglich jeder anderen Permutation des Alphabets eine Monomordnung definieren, so daß diese Ordnung nicht sonderlich interessant ist – außer als Bestandteil der im folgenden definierten Monomordnung:

d) Die graduierte inverse lexikographische Ordnung: Wie bei der graduierten lexikographischen Ordnung ist hier der Grad eines Monoms erstes Ordnungskriterium: Falls $\deg X^\alpha < \deg X^\beta$, ist $\alpha < \beta$, und nur falls beide Monome gleichen Grad haben, soll $\alpha < \beta$ genau dann gelten, wenn α im Sinne der inversen lexikographischen Ordnung *größer* ist als β. Man beachte, daß wir hier also nicht nur die Reihenfolge der Variablen invertieren, sondern auch die Ordnungsrelation im Fall gleicher Grade. Es ist nicht schwer zu sehen, daß auch damit eine Monomordnung definiert wird; siehe Übungsblatt.

Für das folgende werden wir noch einige Eigenschaften einer Monomordnung benötigen, die in der Definition nicht erwähnt sind.

Als erstes wollen wir uns überlegen, daß bezüglich jeder Monomordnung auf $\mathbb{N}_0^n$ kein Element kleiner sein kann als $(0, \ldots, 0)$: Wäre nämlich $\alpha < (0, \ldots, 0)$, so wäre wegen der zweiten Eigenschaft auch

$$2\alpha = \alpha + \alpha < \alpha + (0, \ldots, 0) = \alpha$$

und so weiter, so daß wir eine unendliche Folge

$$\alpha > 2\alpha > 3\alpha > \cdots$$

hätten, im Widerspruch zur dritten Forderung.

Daraus folgt nun sofort, daß das Produkt zweier Monome größer ist als jeder der beiden Faktoren und damit auch, daß ein echter Teiler eines Monoms immer kleiner ist als dieses. Außerdem folgt, daß für ein Produkt von Polynomen stets $\mathrm{FM}(fg) = \mathrm{FM}(f) \cdot \mathrm{FM}(g)$ ist.

Die Eliminationsschritte beim GAUSS-Algorithmus können auch als Divisionen mit Rest verstanden werden, und beim EUKLIDischen Algorithmus ist ohnehin alles Division mit Rest. Für ein Verallgemeinerung der beiden Algorithmen auf Systeme nichtlinearer Gleichungssysteme brauchen wir also auch einen Divisionsalgorithmus für Polynome in mehreren Veränderlichen, der die eindimensionale Polynomdivision mit Rest und die Eliminationsschritte beim GAUSS-Algorithmus verallgemeinert.

Beim GAUSS-Algorithmus brauchen wir im allgemeinen mehr als nur einen Eliminationsschritt, bis wir eine Gleichung auf eine Variable reduziert haben; entsprechend wollen wir auch hier einen Divisionsalgorithmus betrachten, der gegebenenfalls auch mehrere Divisoren gleichzeitig behandeln kann.

Wir gehen also aus von einem Polynom $R = f \in k[X_1, \ldots, X_n]$, wobei k irgendein Körper ist, in dem wir rechnen können, meistens also $k = \mathbb{Q}$ oder $k = \mathbb{F}_p$. Dieses Polynom wollen wir dividieren durch die Polynome $f_1, \ldots, f_m \in R$, d.h. wir suchen Polynome $a_1, \ldots, a_m, r \in R$, so daß

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

ist, wobei r in irgendeinem noch zu präzisierenden Weise kleiner als die f_i sein soll.

Da es sowohl bei GAUSS als auch bei EUKLID auf die Anordnung der Terme ankommt, legen wir als erstes eine Monomordnung fest; wenn im folgenden von führenden Termen *etc.* die Rede ist, soll es sich stets um die führenden Terme *etc.* bezüglich dieser Ordnung handeln.

Mit dieser Konvention geht der Algorithmus dann folgendermaßen:

Gegeben sind $f, f_1, \ldots, f_m \in R$
Berechnet werden $a_1, \ldots, a_m, r \in R$ mit $f = a_1 f_1 + \cdots + a_m f_m + r$

1. Schritt (Initialisierung): Setze $a_1 = \cdots = a_m = r = 0$ und $p = f$.

2. Schritt (Endebedingung): Falls $p = 0$ endet der Algorithmus.

3. Schritt (Divisionsschritt) Falls keiner der führenden Terme FT f_i den führenden Term FT p teilt, wird p ersetzt durch $p - \mathrm{FT}\, p$ und r durch $r + \mathrm{FT}\, p$. Andernfalls sei i der kleinste Index, für den FT f_i Teiler von FT p ist; der Quotient sei q. Dann wird a_i ersetzt durch $a_i + q$ und p durch $p - q f_i$. Weiter geht es mit dem 2. Schritt.

Offensichtlich ist die Bedingung $f - p = a_1 f_1 + \cdots + a_m f_m + r$ nach der Initialisierung im ersten Schritt erfüllt, und sie bleibt auch bei jeder Anwendung des Divisionsschritts erfüllt. Außerdem endet der Algorithmus nach endlich vielen Schritten: Bei jedem Divisionsschritt wird der führende Term von p eliminiert, und alle Monome, die eventuell neu dazukommen, sind kleiner oder gleich dem führenden Monom von f_i. Da letzteres das (alte) führende Monom von p teilt, kann es nicht größer sein als dieses, d.h. der führende Term des neuen p ist kleiner als der des alten. Wegen der Wohlordnungseigenschaft einer Monomordnung kann es keine unendliche absteigende Kette von Monomen geben; daher muß der Algorithmus nach endlich vielen Schritten abbrechen.

Bei der klassischen Polynomdivision für Polynome in einer Variablen über einem Körper wissen wir, daß der Rest kleineren Grad hat als der Divisor. Das muß hier nicht der Fall sein; wir können nur sagen, daß der Rest keine Monome enthält, die durch den führenden Term eines der Divisoren f_i teilbar sind.

Um den Algorithmus besser zu verstehen, betrachten wir zunächst zwei Beispiele:

Als erstes dividieren wir $f = X^2Y + XY^2 + Y^2$ durch $f_1 = XY - 1$ und $f_2 = Y^2 - 1$.

Zur Initialisierung setzen wir $a_1 = a_2 = r = 0$ und $p = f$. Wir verwenden die lexikographische Ordnung; bezüglich derer ist der führende Term von p gleich X^2Y und der von f_1 gleich XY. Letzteres teilt X^2Y, wir setzen also

$$p \leftarrow p - Xf_1 = XY^2 + X + Y^2 \quad \text{und} \quad a_1 \leftarrow a_1 + X = X\,.$$

Neuer führender Term von p ist XY^2; auch das ist ein Vielfaches von XY, also setzen wir

$$p \leftarrow p - Yf_1 = X + Y^2 + Y \quad \text{und} \quad a_1 \leftarrow a_1 + Y = X + Y\,.$$

Nun ist X der führende Term von p, und der ist weder durch XY noch durch Y^2 teilbar, also kommt er in den Rest:

$$p \leftarrow p - X = Y^2 + Y \quad \text{und} \quad r \leftarrow r + X = X\,.$$

Der nun führende Term Y^2 von p ist gleichzeitig der führende Term von f_2 und nicht teilbar durch XY, also wird

$$p \leftarrow p - f_2 = Y + 1 \quad \text{und} \quad a_2 \leftarrow a_2 + 1 = 1\,.$$

Die verbleibenden Terme von p sind weder durch XY noch durch Y^2 teilbar, kommen also in den Rest, so daß wir als Ergebnis erhalten

$$f = a_1f_1 + a_2f_2 + r \quad \text{mit} \quad a_1 = X + Y, \quad a_2 = 1 \quad \text{und} \quad r = X + Y + 1\,.$$

Wenn wir statt durch das Paar (f_1, f_2) durch (f_2, f_1) dividiert hätten, hätten wir im ersten Schritt zwar ebenfalls X^2Y durch XY dividiert, denn durch Y^2 ist es nicht teilbar. Der neue führende Term XY^2 ist aber durch beides teilbar, und wenn f_2 an erster Stelle steht, nehmen wir im Zweifelsfall dessen führenden Term. Man rechnet leicht nach, daß man hier mit folgendem Ergebnis endet:

$$f = a_1f_1 + a_2f_2 + r \quad \text{mit} \quad a_1 = X + 1, \quad a_2 = X \quad \text{und} \quad r = X + 1\,.$$

Wie wir sehen, sind also sowohl die „Quotienten“ a_i als auch der „Rest“ r von der Reihenfolge der f_i abhängig. Sie hängen natürlich im allgemeinen auch ab von der verwendeten Monomordnung; deshalb haben wir die schließlich eingeführt.

Als zweites Beispiel wollen wir $f = XY^2 - X$ durch die beiden Polynome $f_1 = XY + 1$ und $f_2 = Y^2 - 1$ dividieren. Im ersten Schritt dividieren wir XY^2 durch XY mit Ergebnis Y, ersetzen also f durch $-X - Y$. Diese beiden Terme sind weder durch XY noch durch Y^2 teilbar, also ist unser Endergebnis

$$f = a_1 f_1 + a_2 f_2 + r \quad \text{mit} \quad a_1 = Y, \quad a_2 = 0 \quad \text{und} \quad r = -X - Y\,.$$

Hätten wir stattdessen durch (f_2, f_1) dividiert, hätten wir als erstes XY^2 durch Y^2 dividiert mit Ergebnis X; da $f = X f_2$ ist, geht die Division hier ohne Rest auf. Der Divisionsalgorithmus erlaubt uns also nicht einmal die sichere Feststellung, ob f als Linearkombination der f_i darstellbar ist oder nicht; als alleiniges Hilfsmittel zur Lösung nichtlinearer Gleichungssysteme reicht er offenbar nicht aus. Daher müssen wir in den folgenden Paragraphen noch weitere Werkzeuge betrachten.

§4: Der Hilbertsche Basissatz

Die Grundidee des Algorithmus von BUCHBERGER besteht darin, das Gleichungssystem so abzuändern, daß möglichst viele seiner Eigenschaften bereits an den führenden Termen der Gleichungen ablesbar sind.

Angenommen, wir haben ein nichtlineares Gleichungssystem

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

mit $f_i \in R = k[X_1, \ldots, X_n]$; seine Lösungsmenge sei $\mathcal{L} \subseteq k^n$.

Wie wir aus §2 wissen, hängt $\mathcal{L}$ nur ab von dem Ideal $I = (f_1, \ldots, f_m)$; zur Lösung des Systems sollten wir daher versuchen, ein möglichst „einfaches“ Erzeugendensystem für dieses Ideal zu finden.

Ganz besonders einfach (wenn auch selten ausreichend) sind Ideale, die von Monomen erzeugt werden:

Definition: Ein Ideal $I \lhd R = k[X_1, \ldots, X_n]$ heißt *monomial,* wenn es von (nicht notwendigerweise endlich vielen) Monomen erzeugt wird.

Nehmen wir an, I werde erzeugt von den Monomen X^α mit α aus einer Indexmenge A. Ist dann X^β irgendein Monom aus I, kann es als endliche Linearkombination

$$X^\beta = \sum_{i=1}^{r} f_i X^{\alpha_i} \quad \text{mit} \quad \alpha_i \in A$$

geschrieben werden, wobei die f_i irgendwelche Polynome aus R sind. Da sich jedes Polynom als Summe von Monomen schreiben läßt, können wir f_i als k-Linearkombination von Monomen X^γ schreiben und bekommen damit eine neue Darstellung von X^β als Summe von Termen der Form $cX^\gamma X^\alpha$ mit $\alpha \in A, \beta \in \mathbb{N}_0^n$ und $c \in k$. Sortieren wir diese Summanden nach den resultierenden Monomen $X^{\gamma+\alpha}$, entsteht eine k-Linearkombination verschiedener Monome, die insgesamt gleich X^β ist. Das ist aber nur möglich, wenn diese Summe aus dem einen Summanden X^β besteht, d.h. β läßt sich schreiben in der Form $\beta = \alpha + \gamma$ mit einem $\alpha \in A$ und einem $\gamma \in \mathbb{N}_0^n$.

Dies zeigt, daß ein Monom X^β genau dann in I liegt, wenn $\beta = \alpha + \gamma$ ist mit einem $\alpha \in A$ und einem $\gamma \in \mathbb{N}_0^n$, d.h. X^β ist das Produkt eines der erzeugenden Monome mit *irgendeinem* Monom. Das Ideal I besteht genau aus den Polynomen f, die sich als k-Linearkombinationen solcher Monome schreiben lassen.

Damit folgt insbesondere, daß ein Polynom f genau dann in einem monomialen Ideal I liegt, wenn jedes seiner Monome dort liegt.

Lemma von Dickson: Jedes monomiale Ideal in $R = k[X_1, \ldots, X_n]$ kann von endlich vielen Monomen erzeugt werden.

Der *Beweis* wird durch vollständige Induktion nach n geführt. Im Fall $n = 1$ ist alles klar, denn da sind die Monome gerade die Potenzen der einzigen Variable, und natürlich erzeugt jede Menge von Potenzen genau dasselbe Ideal wie die Potenz mit dem kleinsten Exponenten aus dieser Menge. Hier kommt man also sogar mit einem einzigen Monom aus.

Im Fall $n > 1$ und $\alpha \in \mathbb{N}_0^n$ setzen wir $X'^\alpha = X_1^{\alpha_1} \cdots X_{n-1}^{\alpha_{n-1}}$ und

betrachten das Ideal

$$J = \left(X'^{\alpha} \;\middle|\; X^{\alpha} \in I\right) \lhd k[X_1, \ldots, X_{n-1}] .$$

Nach Induktionsvoraussetzung wird J erzeugt von endlich vielen Monomen X'^{α}

Jedes Monom aus aus dem endlichen Erzeugendensystem von J läßt sich in der Form X'^{α} schreiben mit einem $\alpha \in \mathbb{N}_0^n$, für das X^{α} in I liegt. Unter den Indizes α_n, die wir dabei jeweils an das $(n-1)$-tupel $(\alpha_1, \ldots, \alpha_{n-1})$ anhängen, sei r der größte. Dann liegt $X'^{\alpha'} X_n^r$ für jedes Monom aus dem Erzeugendensystem von J in I und damit für jedes Monom aus J. Die endlich vielen Monome $X^{\alpha'} X_n^r$ erzeugen also zumindest ein Teilideal von I.

Es gibt aber natürlich auch noch Monome in I, in denen X_n mit einem kleineren Exponenten als r auftritt. Um auch diese Elemente zu erfassen, betrachten wir für jedes $s < r$ das Ideal $J_s \lhd k[X_1, \ldots, X_{n-1}]$, das von allen jeden Monomen X'^{α} erzeugt wird, für die $X'^{\alpha} X_n^s$ in I liegt. Auch jedes der J_s wird nach Induktionsannahme erzeugt von endlich vielen Monomen X'^{α}, und wenn wir die sämtlichen Monome $X'^{\alpha} X_n^s$ zu unserem Erzeugendensystem hinzunehmen (für alle $s = 0, 1, \cdots, r-1$), haben wir offensichtlich ein Erzeugendensystem von I aus endlich vielen Monomen gefunden.

■

LEONARD EUGENE DICKSON (1874–1954) wurde in Iowa geboren, wuchs aber in Texas auf. Seinen Bachelor- und Mastergrad bekam er von der University of Texas, danach ging er an die Universität von Chicago. Mit seiner 1896 dort eingereichte Dissertation *Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group* wurde er der erste dort promovierte Mathematiker. Auch die weiteren seiner 275 wissenschaftlichen Arbeiten, darunter acht Bücher, beschäftigen sich vor allem mit der Algebra und Zahlentheorie. Den größten Teil seines Berufslebens verbrachte er als Professor an der Universität von Chicago, dazu kommen regelmäßige Besuche in Berkeley.

Beliebige Ideale sind im allgemeinen nicht monomial; schon das von $X + 1$ erzeugte Ideal in $k[X]$ ist ein Gegenbeispiel, denn es enthält weder das Monom X noch das Monom 1, im Widerspruch zu der oben gezeigten Eigenschaft eines monomialen Ideals, zu jedem seiner Elemente auch dessen sämtliche Monome zu enthalten.

Um monomiale Ideale auch für die Untersuchung solcher Ideale nützlich zu machen, wählen wir eine Monomordnung auf R und definieren für ein beliebiges Ideal $I \lhd R \underset{\text{def}}{=} k[X_1, \ldots, X_n]$ das monomiale Ideal

$$\mathrm{FM}(I) = \Big(\mathrm{FM}(f) \;\Big|\; f \in I \setminus \{0\}\Big)\,,$$

das von den führenden Monomen *aller* Elemente von I erzeugt wird – außer natürlich dem nicht existierenden führenden Term der Null.

Nach dem Lemma von DICKSON ist $\mathrm{FM}(I)$ erzeugt von endlich vielen Monomen. Jedes dieser Monome ist, wie wir eingangs gesehen haben, ein Vielfaches eines der erzeugenden Monome, also eines führenden Monoms eines Elements von I. Ein Vielfaches des führenden Monoms ist aber das führende Monom des entsprechenden Vielfachen des Elements von I, denn $\mathrm{FM}(X^\gamma f) = X^\gamma\,\mathrm{FM}(f)$, da für jede Monomordnung gilt $\alpha < \beta \Longrightarrow \alpha + \beta < \alpha + \gamma$. Somit wird $\mathrm{FM}(I)$ erzeugt von endlich vielen Monomen der Form $\mathrm{FM}(f_i)$, wobei die f_i Elemente von I sind. Wir wollen sehen, daß die Elemente f_i das Ideal I erzeugen; damit folgt insbesondere

Hilbertscher Basissatz: Jedes Ideal $I \lhd R = k[X_1, \ldots, X_n]$ hat ein endliches Erzeugendensystem.

Beweis: Wie wir bereits wissen, gibt es Elemente $f_1, \ldots f_m \in I$, so daß $\mathrm{FM}(I)$ von den Monomen $\mathrm{FM}(f_i)$ erzeugt wird. Um zu zeigen, daß die Elemente f_i das Ideal I erzeugen, betrachten wir ein beliebiges Element $f \in I$ und versuchen, es als R-Linearkombination der f_i zu schreiben. Division von f durch $f_1, \ldots, f_m$ zeigt, daß es Polynome $a_1, \ldots, a_m$ und r in R gibt derart, daß

$$f = a_1 f_1 + \cdots + a_m f_m + r\,.$$

Wir sind fertig, wenn wir zeigen können, daß der Divisionsrest r verschwindet.

Falls r *nicht* verschwindet, zeigt der Divisionsalgorithmus, daß das führende Monom FM(r) von r durch kein führendes Monom FM(f_i) eines der Divisoren f_i teilbar ist. Andererseits ist aber

$$r = f - (a_1 f_1 + \cdots + a_m f_m)$$

ein Element von I, und damit liegt FM(r) im von den FM(f_i) erzeugten Ideal FM(I). Somit muß FM(r) Vielfaches eines FM(f_i) sein, ein Widerspruch. Also ist $r = 0$.

■

DAVID HILBERT (1862–1943) wurde in Königsberg geboren, wo er auch zur Schule und zur Universität ging. Er promovierte dort 1885 mit einem Thema aus der Invariantentheorie, habilitierte sich 1886 und bekam 1893 einen Lehrstuhl. 1895 wechselte er an das damalige Zentrum der deutschen wie auch internationalen Mathematik, die Universität Göttingen, wo er bis zu seiner Emeritierung im Jahre 1930 lehrte. Seine Arbeiten umfassen ein riesiges Spektrum aus unter anderem Invariantentheorie, Zahlentheorie, Geometrie, Funktionalanalysis, Logik und Grundlagen der Mathematik sowie auch zur Relativitätstheorie. Er gilt als einer der Väter der modernen Algebra.

§5: Gröbner-Basen und der Buchberger-Algorithmus

Angesichts der Rolle der führenden Monome im obigen Beweis bietet sich folgende Definition an für eine Idealbasis, bezüglich derer möglichst viele Eigenschaften bereits an den führenden Monomen abgelesen werden können:

Definition: Eine endliche Teilmenge $G = \{g_1, \ldots, g_m\} \subset I$ eines Ideals $I \lhd R = k[X_1, \ldots, X_n]$ heißt Standardbasis oder GRÖBNER-Basis von I, falls die Monome FM(g_i) das Ideal FM(I) erzeugen.

WOLFGANG GRÖBNER wurde 1899 im damals noch österreichischen Südtirol geboren. Nach Ende des ersten Weltkriegs, in dem er an der italienischen Front kämpfte, studierte er zunächst an der TU Graz Maschinenbau, beendete dieses Studium aber nicht, sondern begann 1929 an der Universität ein Mathematikstudium. Nach seiner Promotion ging er zu EMMY NOETHER nach Göttingen, um dort Algebra zu lernen. Aus materiellen Gründen

mußte er schon bald nach Österreich zurück, konnte aber auch dort zunächst keine Anstellung finden, so daß er Kleinkraftwerke baute und im Hotel seines Vaters aushalf. Ein italienischen Mathematiker, der dort seinen Urlaub verbrachte, vermittelte ihm eine Stelle an der Universität Rom, die er 1939 wieder verlassen mußte, nachdem er sich beim Anschluß Südtirols an Italien für die deutsche Staatsbürgerschaft entschieden hatte. Während des zweiten Weltkriegs arbeitete er größtenteils an einem Forschungsinstitut der Luftwaffe, nach Kriegsende als Extraordinarius in Wien, dann als Ordinarius in Innsbruck, wo er 1980 starb. Seine Arbeiten beschäftigen sich mit der Algebra und algebraischen Geometrie sowie mit Methoden der Computeralgebra zur Lösung von Differentialgleichungen.

Die Theorie der GRÖBNER-Basen wurde von seinem Studenten BRUNO BUCHBERGER in dessen Dissertation entwickelt. BUCHBERGER wurde 1942 in Innsbruck geboren, wo er auch Mathematik studierte und 1966 bei GRÖBNER promovierte mit der Arbeit *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*. Er arbeitete dann zunächst als Assustent. nach seiner Habilitation als Dozent an der Universität Innsbruck, bis er 1974 einen Ruf auf den Lehrstuhl für Computermathematik an der Universität Linz erhielt. Dort gründete er 1987 das Research Institute for Symbolic Computation (RISC), dessen Direktor er bis 1999 war. 1989 initiierte er in Hagenberg (etwa 20 km nordöstlich von Linz) die Gründung eines Softwareparks mit angeschlossener Fachhochschule; er hat mittlerweile fast Tausend Mitarbeiter. Außer mit Computeralgebra beschäftigt er sich auch im Rahmen des Theorema-Projekts mit dem automatischen Beweisen mathematischer Aussagen.

Wie der obige Beweis des HILBERTschen Basissatzes zeigt, erzeugt eine GRÖBNER-Basis das Ideal, und jedes Ideal im Polynomring hat eine GRÖBNER-Basis. Bevor wir uns damit beschäftigen, wie man diese berechnen kann, wollen wir zunächst eine wichtige Eigenschaften betrachten.

Sei $g_1, \ldots, g_m$ GRÖBNER-Basis eines Ideals $I \lhd R$. Wir wollen ein beliebiges Element $f \in R$ durch $g_1, \ldots, g_m$ dividieren. Dies liefert als Ergebnis

$$f = a_1 g_1 + \cdots + a_m g_m + r\,,$$

wobei kein Monom von r durch eines der Monome FM(g_i) teilbar ist. Wie wir wissen, sind allerdings bei der Polynomdivision im allgemeinen weder der Divisionsrest r noch die Koeffizienten a_i auch nur im entferntesten eindeutig. Wir wollen untersuchen, wie sich das hier verhält.

Sei etwa

$$f = a_1 g_1 + \cdots + a_m g_m + r = b_1 g_1 + \cdots + b_m g_m + s\,;$$

dann ist

$$(a_1 - b_1)g_1 + \cdots + (a_m - b_m)g_m = s - r\,.$$

Links steht ein Element von I, also auch rechts. Andererseits enthält aber weder r noch s ein Monom, das durch eines der Monome FM(g_i) teilbar ist, d.h. $r - s = 0$. Somit ist bei der Division durch die Elemente einer GRÖBNER-Basis der Divisionsrest eindeutig bestimmt. Insbesondere ist f genau dann ein Element von I, wenn der Divisionsrest verschwindet. Wenn wir eine GRÖBNER-Basis haben, können wir also leicht entscheiden, ob ein gegebenes Element $f \in R$ im Ideal I liegt.

Nachdem im Fall einer GRÖBNER-Basis der Divisionsrest nicht von der Reihenfolge der Basiselemente abhängt, können wir ihn durch ein Symbol bezeichnen, das nur von der *Menge* $G = \{g_1, \ldots, g_m\}$ abhängt; wir schreiben $\overline{f}^G$.

Als nächstes wollen wir uns überlegen, wie sich eine GRÖBNER-Basis eines vorgegebenen Ideals I finden läßt.

Dazu müssen wir uns als erstes überlegen, *wie* das Ideal vorgegeben sein soll. Wenn wir damit rechnen wollen, müssen wir irgendeine Art von endlicher Information haben; was sich anbietet ist natürlich ein endliches Erzeugendensystem.

Wir gehen also aus von einem Ideal $I = (f_1, \ldots, f_m)$ und suchen eine GRÖBNER-Basis. Das Problem ist, daß die Monome FM(f_i) im allgemeinen nicht ausreichen, um das monomiale Ideal FM(I) zu erzeugen, denn dieses enthält ja *jedes* Monom eines jeden Elements von *I* und nicht nur das führende. Wir müssen daher neue Elemente produzieren, deren führende Monome in den gegebenen Elementen f_i oder auch anderen Elementen von I erst weiter hinten vorkommen.

BUCHBERGERs Idee dazu war die Konstruktion sogenannter S-Polynome: Seien $f, g \in R$ zwei Polynome; FM(f) = X^α und FM(g) = X^β seien ihre führenden Monome, und X^γ sei das kgV von X^α und X^β, d.h. $\gamma_i = \max(\alpha_i, \beta_i)$ für alle $i = 1, \ldots, n$. Das S-Polynom von f und g ist

$$S(f,g) = \frac{X^\gamma}{\mathrm{FT}(f)} \cdot f - \frac{X^\gamma}{\mathrm{FT}(g)} \cdot g\,.$$

Da $\frac{X^\gamma}{\mathrm{FT}(f)} \cdot f$ und $\frac{X^\gamma}{\mathrm{FT}(g)} \cdot g$ beide nicht nur dasselbe führende Monom X^γ haben, sondern es wegen der Division durch den führenden *Term* statt nur das führende Monom auch beide mit Koeffizient eins enthalten, fällt es bei der Bildung von $S(f,g)$ weg, d.h. $S(f,g)$ hat ein kleineres führendes Monom. Das folgende Lemma ist der Kern des Beweises, daß S-Polynome alles sind, was wir brauchen, um GRÖBNER-Basen zu berechnen.

Lemma: Für die Polynome $f_1, \ldots, f_m \in R$ sei

$$S = \sum_{i=1}^{m} \lambda_i X^{\alpha_i} f_i \quad \text{mit} \quad \lambda_i \in k \quad \text{und} \quad \alpha_i \in \mathbb{N}_0^n$$

eine Linearkombination, zu der es ein $\delta \in \mathbb{N}_0^n$ gebe, so daß alle Summanden X^δ als führendes Monom haben, d.h. α_i + multideg $f_i = \delta_i$ für $i = 1, \ldots, m$. Falls multideg $S < \delta$ ist, gibt es Elemente $\lambda_{ij} \in k$, so daß

$$S = \sum_{i=1}^{m} \sum_{j=1}^{m} \lambda_{ij} X^{\gamma_{ij}} S(f_i, f_j)$$

ist mit $X^{\gamma_{ij}} = \mathrm{kgV}\big(\mathrm{FM}(f_i), \mathrm{FM}(f_j)\big)$.

Beweis: Der führende Koeffizient von f_i sei μ_i; dann ist $\lambda_i \mu_i$ der führende Koeffizient von $\lambda_i X^{\alpha_i} f_i$. Somit ist multideg S genau dann kleiner als δ, wenn $\sum_{i=1}^{m} \lambda_i \mu_i$ verschwindet. Wir normieren alle $X^{\alpha_i} f_i$ auf führenden Koeffizienten eins, indem wir $p_i = X^{\alpha_i} f_i / \mu_i$ betrachten; dann ist

$$\begin{aligned} S = \sum_{i=1}^{m} \lambda_i \mu_i p_i = {} & \lambda_1\mu_1(p_1 - p_2) + (\lambda_1\mu_1 + \lambda_2\mu_2)(p_2 - p_3) + \cdots \\ & + (\lambda_1\mu_1 + \cdots + \lambda_{m-1}\mu_{m-1})(p_{m-1} - p_m) \\ & + (\lambda_1\mu_1 + \cdots + \lambda_m\mu_m)p_m \,, \end{aligned}$$

wobei der Summand in der letzten Zeile genau dann verschwindet, wenn multideg $S < \delta$.

Da alle p_i denselben Multigrad δ und denselben führenden Koeffizienten eins haben, kürzen sich in den Differenzen $p_i - p_j$ die führenden Terme

weg, genau wie in den S-Polynomen. In der Tat: Bezeichnen wir den Multigrad von $\mathrm{kgV}\big(\mathrm{FM}(f_i), \mathrm{FM}(f_j)\big)$ mit γ_{ij}, so ist

$$p_i - p_j = X^{\delta-\gamma_{ij}} S(f_i, f_j)\,.$$

Damit hat die obige Summendarstellung von S die gewünschte Form. ∎

Daraus folgt ziemlich unmittelbar

Satz: Ein Erzeugendensystem $f_1, \ldots, f_m$ eines Ideals I im Polynomring $R = k[X_1, \ldots, X_n]$ ist genau dann eine GRÖBNER-Basis, wenn jedes S-Polynom $S(f_i, f_j)$ bei der Division durch $f_1, \ldots, f_m$ Rest null hat.

Beweis: Als R-Linearkombination von f_i und f_j liegt das S-Polynom $S(f_i, f_j)$ im Ideal I; falls $f_1, \ldots, f_m$ eine GRÖBNER-Basis von I ist, hat es also Rest null bei der Division durch $f_1, \ldots, f_m$.

Umgekehrt sei $f_1, \ldots, f_m$ ein Erzeugendensystem von $I \lhd R$ mit der Eigenschaft, daß alle $S(f_i, f_j)$ bei der Division durch $f_1, \ldots, f_m$ (in irgendeiner Reihenfolge) Divisionsrest null haben. Wir wollen zeigen, daß $f_1, \ldots, f_m$ dann eine GRÖBNER-Basis ist, d.h. daß $\mathrm{FM}(f_1), \ldots, \mathrm{FM}(f_m)$ das Ideal $\mathrm{FM}(I)$ erzeugen.

Sei also $f \in I$ ein beliebiges Element; wir müssen zeigen, daß $\mathrm{FM}(f)$ im von den $\mathrm{FM}(f_i)$ erzeugten Ideal liegt.

Da f in I liegt, gibt es eine Darstellung

$$f = h_1 f_1 + \cdots + h_m f_m \quad \text{mit} \quad h_i \in R\,.$$

Falls sich hier bei den führenden Termen nichts wegkürzt, ist der führende Term von f die Summe der führenden Terme gewisser Produkte $h_i f_i$, die allesamt dasselbe führende Monom $\mathrm{FM}(f)$ haben. Wegen $\mathrm{FM}(h_i f_i) = \mathrm{FM}(h_i)\,\mathrm{FM}(f_i)$ liegt $\mathrm{FM}(f)$ daher im von den $\mathrm{FM}(f_i)$ erzeugten Ideal.

Falls sich die maximalen unter den führenden Termen $\mathrm{FT}(h_i f_i)$ gegenseitig wegkürzen, läßt sich die entsprechende Teilsumme der $h_i f_i$ nach dem vorigen Lemma auch als eine Summe von S-Polynomen schreiben.

Diese wiederum lassen sich nach Voraussetzung durch den Divisionsalgorithmus als Linearkombinationen der f_i darstellen. Damit erhalten wir eine neue Darstellung

$$f = \widetilde{h}_1 f_1 + \ldots + \widetilde{h}_m f_m \quad \text{mit} \quad \widetilde{h}_i \in R\,,$$

in der der maximale Multigrad eines Summanden echt kleiner ist als in der obigen Darstellung, denn in der Darstellung als Summe von S-Polynomen sind die Terme mit dem maximalem Multigrad verschwunden.

Mit dieser Darstellung können wir wie oben argumentieren: Falls sich bei den führenden Termen nichts wegkürzt, haben wir FM(f) als Element des von den FM(f_i) erzeugten Ideals dargestellt, andernfalls erhalten wir wieder via S-Polynome und deren Reduktion eine neue Darstellung von f als Linearkombination der f_i mit noch kleinerem maximalem Multigrad der Summanden, und so weiter. Das Verfahren muß schließlich mit einer Summe ohne Kürzungen bei den führenden Termen enden, da es nach der Wohlordnungseigenschaft einer Monomordnung keine unendliche absteigende Folge von Multigraden geben kann. ∎

Der BUCHBERGER-Algorithmus in seiner einfachsten Form macht aus diesem Satz ein Verfahren zur Berechnung einer GRÖBNER-Basis aus einem vorgegebenen Erzeugendensystem eines Ideals:

Gegeben sind m Elemente $f_1, \ldots, f_m \in R = k[X_1, \ldots, X_n]$.

Berechnet wird eine GRÖBNER-Basis $g_1, \ldots, g_r$ des davon erzeugten Ideals $I = (f_1, \ldots, f_m)$ mit $g_i = f_i$ für $i \leq m$.

1. Schritt (Initialisierung): Setze $g_i = f_i$ für $i = 1, \ldots, m$; die Menge $\{g_1, \ldots, g_m\}$ werde mit G bezeichnet.

2. Schritt: Setze $G' = G$ und teste für jedes Paar $(f, g) \in G' \times G'$ mit $f \neq g$, ob der Rest r bei der Division von $S(f, g)$ durch die Elemente von G' (in irgendeiner Reihenfolge angeordnet) verschwindet. Falls nicht, wird G ersetzt durch $G \cup \{r\}$.

3. Schritt: Ist $G = G'$, so endet der Algorithmus mit G als Ergebnis; andernfalls geht es zurück zum zweiten Schritt.

Wenn der Algorithmus im dritten Schritt endet, ist der Rest bei der Division von $S(f, g)$ durch die Elemente von G stets das Nullpolynom; nach dem gerade bewiesenen Satz ist G daher eine GRÖBNER-Basis. Da sowohl die S-Polynome als auch ihre Divisionsreste in I liegen und G ein Erzeugendensystem von I enthält, ist auch klar, daß es sich dabei um eine GRÖBNER-Basis von I handelt. Wir müssen uns daher nur noch überlegen, daß der Algorithmus nach endlich vielen Iterationen abbricht.

Wenn im zweiten Schritt ein nichtverschwindender Divisionsrest r auftaucht, ist dessen führendes Monom durch kein führendes Monom eines Polynoms $g \in G$ teilbar. Das von den führenden Monomen der $g \in G$ erzeugte Ideal von R wird daher größer, nachdem G um r erweitert wurde. Wenn dies unbeschränkt möglich wäre, könnte das Ideal FM(I) kein endliches Erzeugendensystem haben, im Widerspruch zum Lemma von DICKSON. Also kann der zweite Schritt nur endlich oft durchlaufen werden.

Der Algorithmus kann natürlich auf mehrere offensichtliche Weisen optimiert werden: Beispielsweise stößt man beim wiederholten Durchlaufen des zweiten Schritts immer wieder auf dieselben S-Polynome, die daher nicht jedes Mal neu berechnet werden müssen, und wenn eines dieser Polynome einmal Divisionsrest null hatte, hat es auch bei jedem weiteren Durchgang Divisionsrest null, denn dann wird ja wieder durch dieselben Polynome (plus einiger neuer) dividiert. Es gibt inzwischen auch zahlreiche nicht offensichtliche Verbesserungen und Optimierungen; wir wollen uns aber mit dem Prinzip begnügen und für den Rest des Semesters lieber einige Anwendungen betrachten.

Der BUCHBERGER-Algorithmus hat den Nachteil, daß er das vorgegebene Erzeugendensystem in jedem Schritt größer macht ohne je ein Element zu streichen. Dies ist weder beim GAUSS-Algorithmus noch beim EUKLIDischen Algorithmus der Fall, bei denen jeweils eine Gleichung durch eine andere *ersetzt* wird. Obwohl wir sowohl die Eliminationsschritte des GAUSS-Algorithmus als auch die einzelnen Schritte der Polynomdivisionen beim EUKLIDischen Algorithmus durch S-Polynome ausdrücken können, *müssen* wir im allgemeinen Fall zusätzlich zu g und $S(f, g)$ auch noch das Polynom f beibehalten; andernfalls kann sich die Lösungsmenge ändern:

Als Beispiel können wir das Gleichungssystem

$$f(X,Y) = X^2Y + XY^2 + 1 = 0 \quad \text{und} \quad g(X,Y) = X^3 - XY - Y = 0$$

betrachten. Wenn wir mit der lexikographischen Ordnung arbeiten, sind hier die einzelnen Monome bereits der Größe nach geordnet, insbesondere stehen also die führenden Monome an erster Stelle und

$$S(f,g) = Xf(X,Y) - Yg(X,Y) = X^2Y^2 + XY^2 + X + Y^2 .$$

Der führende Term X^2Y^2 ist durch den führenden Term X^2Y von f teilbar; subtrahieren wir Yf vom S-Polynom, erhalten wir das nicht weiter reduzierbare Polynom

$$h(X,Y) = -XY^3 + XY^2 + X + Y^2 - Y .$$

Sowohl $g(X,Y)$ als auch $h(X,Y)$ verschwinden im Punkt $(0,0)$; dieser ist aber keine Lösung des Ausgangssystems, da $f(0,0) = 1$ nicht verschwindet.

Aus diesem Grund werden die nach dem BUCHBERGER-Algorithmus berechneten GRÖBNER-Basen oft sehr groß und unhandlich. Betrachten wir dazu als Beispiel das System aus den beiden Gleichungen

$$f_1 = X^3 - 2XY \quad \text{und} \quad f_2 = X^2Y - 2Y^2 + X$$

und berechnen eine GRÖBNER-Basis bezüglich der graduiert lexikographischen Ordnung. Dann ist

$$S(f_1,f_2) = Yf_1 - Xf_2 = -X^2$$

weder durch den führenden Term von f_1 noch den von f_2 teilbar, muß also als neues Element f_3 in die Basis aufgenommen werden.

$$S(f_1,f_3) = f_1 + Xf_3 = -2XY$$

kann wieder mit keinem der f_i reduziert werden, muß also als neues Element f_4 in die Basis. Genauso ist es mit

$$f_5 = S(f_2,f_3) = f_2 + Yf_3 = -2Y^2 + X .$$

Im so erweiterten Erzeugendensystem bestehend aus den Polynomen

$$f_1 = X^3 - 2XY, \quad f_2 = X^2Y - 2Y^2 + X, \quad f_3 = -X^2,$$
$$f_4 = -2XY \quad \text{und} \quad f_5 = -2Y^2 + X$$

sind die S-Polynome

$$S(f_1, f_2) = f_3, \quad S(f_1, f_3) = f_4 \quad \text{und} \quad S(f_2, f_3) = f_5$$

trivialerweise auf Null reduzierbar, die anderen Kombinationen müssen wir nachrechnen:

$$S(f_1, f_4) = Y f_1 - \frac{X}{2} f_4 = -2XY^2 = Y f_4$$

$$S(f_1, f_5) = Y^2 f_1 + \frac{X^3}{2} f_5 = -2XY^3 + \frac{X^4}{2} = \frac{X}{2} f_1 + f_2 + Y^2 f_4 - f_5$$

$$S(f_2, f_4) = f_2 + \frac{X}{2} f_4 = -2Y^2 + X = f_5$$

$$S(f_2, f_5) = Y f_2 + \frac{X^2}{2} f_5 = \frac{X^3}{2} + XY - 2Y^3 = \frac{1}{2} f_1 - \frac{1}{2} f_4 + Y f_5$$

$$S(f_3, f_4) = -Y f_3 - \frac{X}{2} f_4 = 0$$

$$S(f_3, f_5) = -Y^2 f_3 - \frac{X^2}{2} f_5 = \frac{1}{2} f_1 - \frac{1}{2} f_4$$

$$S(f_4, f_5) = -\frac{Y}{2} f_4 - \frac{X}{2} f_5 = \frac{X^2}{2} = -\frac{1}{2} f_3$$

Somit bilden diese fünf Polynome eine GRÖBNER-Basis des von f_1 und f_2 erzeugten Ideals.

Zum Glück brauchen wir aber nicht alle fünf Polynome. Das folgende Lemma gibt ein Kriterium, wann man auf ein Erzeugendes verzichten kann, und illustriert gleichzeitig das allgemeine Prinzip, wonach bei einer GRÖBNER-Basis alle wichtigen Eigenschaften anhand der führenden Termen ablesbar sein sollten:

Lemma: G sei eine GRÖBNER-Basis des Ideals $I \lhd k[X_1, \ldots, X_n]$, und $g \in G$ sei ein Polynom, dessen führendes Monom im von den führenden Monomen der restlichen Basiselemente erzeugten monomialen Ideal liegt. Dann ist auch $G \setminus \{g\}$ eine GRÖBNER-Basis von I.

Beweis: $G \setminus \{g\}$ ist nach Definition genau dann eine GRÖBNER-Basis von I, wenn die führenden Terme der Basiselemente das Ideal FT(I)

erzeugen. Da G eine GRÖBNER-Basis von I ist und die führenden Terme egal ob mit oder ohne FT(g) dasselbe monomiale Ideal erzeugen, ist das klar. ∎

Im obigen Beispiel haben wir die führenden Monome

$$\mathrm{FM}(f_1) = X^3, \quad \mathrm{FM}(f_2) = X^2Y, \quad \mathrm{FM}(f_3) = X^2,$$
$$\mathrm{FM}(f_4) = XY \quad \text{und} \quad \mathrm{FM}(f_5) = Y^2;$$

offensichtlich sind FM(f_1) und FM(f_2) durch FM(f_3) teilbar, so daß wir auf f_1 und f_2 verzichten können: Auch die Polynome f_3, f_4 und f_5 bilden eine GRÖBNER-Basis des von f_1 und f_2 erzeugten Ideals. Zur weiteren Normierung können wir noch durch die führenden Koeffizienten teilen und erhalten dann die *minimale* GRÖBNER-Basis

$$\widetilde{f}_3 = X^2, \quad \widetilde{f}_4 = XY \quad \text{und} \quad \widetilde{f}_5 = Y^2 - \frac{X}{2}.$$

Definition: Eine minimale GRÖBNER-Basis von I ist eine GRÖBNER-Basis von I mit folgenden Eigenschaften:

1.) Alle $g \in G$ haben den führenden Koeffizienten eins

2.) Für kein $g \in G$ liegt FT(g) im von den führenden Termen der übrigen Elemente erzeugten Ideal.

Es ist klar, daß jede GRÖBNER-Basis zu einer minimalen GRÖBNER-Basis verkleinert werden kann: Durch Division können wir alle führenden Koeffizienten zu eins machen ohne etwas an der Erzeugung zu ändern, und nach obigem Lemma können wir nacheinander alle Elemente eliminieren, die die zweite Bedingung verletzen.

Wir können aber noch mehr erreichen: Wenn nicht das führende sondern einfach *irgendein* Monom eines Polynoms $g \in G$ im von den führenden Termen der übrigen Elemente erzeugten Ideal liegt, ist dieses Monom teilbar durch das führende Monom eines anderen Polynoms $h \in G$. Wir können den Term mit diesem Monom daher zum Verschwinden bringen, indem wir g ersetzen durch g minus ein Vielfaches von h. Da sich dabei nichts an den führenden Termen der Elemente von G ändert, bleibt G eine GRÖBNER-Basis. Wir können somit aus den Elementen einer minimalen GRÖBNER-Basis Terme eliminieren, die durch den führenden

Term eines anderen Elements teilbar sind. Was dabei schließlich entstehen sollte, ist eine *reduzierte* GRÖBNER-Basis:

Definition: Eine reduzierte GRÖBNER-Basis von I ist eine GRÖBNER-Basis von I mit folgenden Eigenschaften:
1.) Alle $g \in G$ haben den führenden Koeffizienten eins
2.) Für kein $g \in G$ liegt ein Monom von g im von den führenden Termen der übrigen Elemente erzeugten Ideal.

Die minimale Basis im obigen Beispiel ist offenbar schon reduziert, denn außer $\widetilde{f}_5$ bestehen alle Basispolynome nur aus dem führendem Term, und bei $\widetilde{f}_5$ ist der zusätzliche Term linear, kann also nicht durch die quadratischen führenden Terme der anderen Polynome teilbar sein.

Reduzierte GRÖBNER-Basis haben eine für das praktische Rechnen mit Idealen sehr wesentliche zusätzliche Eigenschaft:

Satz: Jedes Ideal $I \lhd k[X_1, \ldots, X_n]$ hat eine eindeutig bestimmte reduzierte GRÖBNER-Basis.

Beweis: Wir gehen aus von einer minimalen GRÖBNER-Basis G und ersetzen nacheinander jedes Element $g \in G$ durch seinen Rest bei der Polynomdivision durch $G \setminus \{g\}$. Da bei einer minimalen GRÖBNER-Basis kein führendes Monom eines Element das führende Monom eines anderen teilen kann, ändert sich dabei nichts an den führenden Termen, G ist also auch nach der Ersetzung eine minimale GRÖBNER-Basis. In der schließlich entstehenden Basis hat kein $g \in G$ mehr einen Term, der durch den führenden Term eines Elements von $G \setminus \{g\}$ teilbar wäre, denn auch wenn wir bei der Reduktion der einzelnen Elemente durch eine eventuell andere Menge geteilt haben, hat sich doch an den führenden Termen der Basiselemente nichts geändert. Also gibt es eine reduzierte GRÖBNER-Basis.

Nun seien G und G' zwei reduzierte GRÖBNER-Basen von I. Jedes Element $f \in G'$ liegt insbesondere in I, also ist $\overline{f}^G = 0$. Insbesondere muß der führende Term von f durch den führenden Term eines $g \in G$ teilbar sein. Umgekehrt ist aber auch $\overline{g}^{G'} = 0$, d.h. der führende Term von g muß durch den führenden Term eines Elements von $f' \in G'$ teilbar

sein. Dieser führende Term teilt dann insbesondere den führenden Term von f, und da G' als reduzierte GRÖBNER-Basis minimal ist, muß $f' = f$ sein. Somit gibt es zu jedem $g \in G$ genau ein $f \in G'$ mit FT(f) = FT(g); insbesondere haben G und G' dieselbe Elementanzahl. Tatsächlich muß sogar $f = g$ sein, denn $f - g$ liegt in I, enthält aber keine Term, der durch den führenden Term irgendeines Elements von G teilbar wäre. Also ist $f - g = 0$.

■

§6: Anwendungen von Gröbner-Basen

Die Eindeutigkeit der reduzierten GRÖBNER-Basis bedeutet, daß wir Ideale des Polynomrings durch endlich viele Daten eindeutig beschreiben können; insbesondere können wir entscheiden, ob zwei Mengen von Polynomen dasselbe Ideal erzeugen. Dies ist der Ausgangspunkt für zahlreiche Anwendungen von GRÖBNER-Basen in der kommutativen Algebra, algebraischen Geometrie, Kontrolltheorie und so weiter.

Wir wollen uns hier mit zwei einfacheren Anwendungen begnügen, zunächst dem Hauptproblem dieser Vorlesung, der Lösung algebraischer Gleichungen und Gleichungssysteme.

Wir gehen also aus von m Polynomgleichungen

$$f_i(x_1, \ldots, x_n) = 0 \quad \text{mit} \quad f_i \in k[X_1, \ldots, X_n] \quad \text{für} \quad i = 1, \ldots, m$$

und suchen die Lösungsmenge

$$V(I) = \left\{ (x_1, \ldots, x_n) \in k^n \;\middle|\; f_i(x_1, \ldots, x_n) = 0 \text{ für } i = 1, \ldots, m \right\}.$$

Wir verwenden die lexikographische Ordnung mit $X_1 > \cdots > X_n$ und betrachten das von den f_i erzeugte Ideal $I \lhd k[X_1, \ldots, X_n]$.

Zur Lösung des Gleichungssystems wollen wir, wie von linearen Gleichungssystemen gewohnt, nacheinander die Variablen eliminieren; dazu definieren wir

Definition: Das k-te Eliminationsideal eines Ideal $I \lhd k[X_1, \ldots, X_n]$ ist $I_k = I \cap k[X_{k+1}, \ldots, X_n]$.

Satz: Ist G eine GRÖBNER-Basis von I bezüglich der lexikographischen Ordnung, so ist $G \cap I_k$ eine GRÖBNER-Basis von I_k.

Beweis: Die Elemente von $G = \{g_1, \ldots, g_m\}$ seien so angeordnet, daß $G \cap I_k = \{g_1, \ldots, g_r\}$ ist. Wir müssen zeigen, daß sich jedes $f \in I_k$ als Linearkombination von $g_1, \ldots, g_r$ darstellen läßt.

Der Divisionsalgorithmus bezüglich der lexikographischen Ordnung gibt uns eine Darstellung $f = h_1 g_1 + \cdots + h_n g_n$ von f als Element von I. Dabei mußten alle h_i mit $i > r$ verschwinden, denn da f in I_k liegt, kann bei der Division kein führender Term eines $g_i \notin I_k$ je den führenden Term des Dividenden teilen. Somit ist $G \cap I_k$ eine Basis von I_k. Um zu zeigen, daß es sich dabei sogar um eine GRÖBNER-Basis handelt, können wir zum Beispiel zeigen, daß alle $S(g_i, g_j)$ mit $i, j \leq r$ ohne Rest durch $G \cap I_k$ teilbar sind. Da G nach Voraussetzung eine GRÖBNER-Basis ist, sind sie auf jeden Fall ohne Rest durch G teilbar, und wieder kann bei der Division nie der führende Term eines Dividenden durch den eines g_i mit $i > r$ teilbar sein.

■

Ist I das von den Gleichungen eines nichtlinearen Gleichungssystems erzeugte Ideal, so ist jede Lösung $(x_1, \ldots, x_n)$ Nullstelle aller Polynome aus I, insbesondere also auch derer aus I_k. Für jede Lösung ist daher das Tupel $(x_{k+1}, \ldots, x_n)$ Nullstelle der Polynome aus I_k.

Daraus ergibt sich eine Strategie zur Lösung nichtlinearer Gleichungssysteme nach Art des GAUSS-Algorithmus: Wir bestimmen zunächst eine (reduzierte) GRÖBNER-Basis für das von den Gleichungen erzeugte Ideal des Polynomrings $k[X_1, \ldots, X_n]$ und betrachten als erstes das Eliminationsideal I_{n-1}. Dieses besteht nur aus Polynomen in X_n; falls wir mit einer reduzierten GRÖBNER-Basis arbeiten, gibt es darin höchstens ein solches Polynom.

Falls es ein solches Polynom gibt, muß jede Lösung des Gleichungssystem als letzte Komponente eine von dessen Nullstellen haben. Wir bestimmen daher diese Nullstellen und setzen sie nacheinander in das restliche Gleichungssystem ein. Dadurch erhalten wir Gleichungssysteme in $n-1$ Unbekannten, wo wir nach Gleichungen nur in X_{n-1} suchen können, und so weiter.

Im obigen Beispiel etwa besteht die reduzierte GRÖBNER-Basis bezüglich der lexikographischen Ordnung aus den beiden Polynomen

$$g_1 = X - 2Y^2 \quad \text{und} \quad g_2 = Y^3 .$$

Das Eliminationsideal I_1 wird also erzeugt von $g_2 = Y^3$, d.h. für jede Lösung (x, y) muß y verschwinden. Setzen wir $y = 0$ in g_1, so sehen wir, daß auch x verschwinden muß, der Nullpunkt ist also die einzige Lösung.

Nun kann es natürlich vorkommen, daß I_{n-1} das Nullideal ist; falls unter den Lösungen des Systems unendlich viele Werte für die letzte Variable vorkommen, muß das sogar so sein. Es kann sogar vorkommen, daß *alle* Eliminationsideale außer $I_0 = I$ das Nullideal sind. In diesem Fall führt die gerade skizzierte Vorgehensweise zu nichts.

Bevor wir uns darüber wundern, sollten wir uns überlegen, was wir überhaupt unter der Lösung eines nichtlinearen Gleichungssystems verstehen wollen. Im Falle einer endlichen Lösungsmenge ist das klar: Dann wollen wir eine Auflistung der sämtlichen Lösungstupel. Bei einer unendlichen Lösungsmenge ist das aber nicht mehr möglich. Im Falle eines linearen Gleichungssystems wissen wir, daß die Lösungsmenge ein affiner Raum ist; wir können sie daher auch wenn sie unendlich sein sollte durch endlich viele Daten eindeutig beschreiben, zum Beispiel durch eine spezielle Lösung und eine Basis des Lösungsraums des zugehörigen homogenen Gleichungssystems.

Bei nichtlinearen Gleichungssystemen gibt es im allgemeinen keine solche Beschreibung unendlicher Lösungsmengen: Die Lösungsmenge des Gleichungssystems

$$X^2 + 2Y^2 + 3Z^2 = 100 \quad \text{und} \quad 2X^2 + 3Y^2 - Z^2 = 0$$

etwa ist die Schnittmenge eines Ellipsoids mit einem elliptischen Kegel; sie besteht aus zwei ovalen Kurven höherer Ordnung. Die GRÖBNER-Basis besteht in diesem Fall aus den beiden Polynomen

$$X^2 - 11Z^2 + 300 \quad \text{und} \quad Y^2 + 7Z^2 - 200 ,$$

stellt uns dieselbe Menge also dar als Schnitt zweier elliptischer Zylinder. Eine explizitere Beschreibung der Lösungsmenge ist schwer vorstellbar.

Auf der Basis von STURMschen Ketten, dem Lemma von THOM und Verallgemeinerungen davon hat die semialgebraische Geometrie Methoden entwickelt, wie man auch allgemeinere Lösungsmengen nichtlinearer Gleichungssysteme durch eine sogenannte zylindrische Zerlegung qualitativ beschreiben kann; dazu wird der $\mathbb{R}^n$ in Teilmengen zerlegt, in denen die Lösungsmenge entweder ein einfaches qualitatives Verhalten hat oder aber leeren Durchschnitt mit der Teilmenge. Dadurch kann man insbesondere feststellen, in welchen Regionen des $\mathbb{R}^n$ Lösungen zu finden sind; diese Methoden sind Gegenstand der reell-algebraischen Geometrie.

In manchen Fällen lassen sich Lösungsmengen parametrisieren; wie man mit Methoden der algebraischen Geometrie zeigen kann, ist das aber im allgemeinen nur bei Gleichungen kleinen Grades der Fall und kommt daher für allgemeine Lösungsalgorithmen nicht in Frage.

Stets möglich ist das umgekehrte Problem, d.h. die Beschreibung einer parametrisch gegebenen Menge in impliziter Form. Hier haben wir also Gleichungen der Form

$$x_1 = \varphi_1(t_1, \ldots, t_m), \quad \ldots, \quad x_n = \varphi_n(t_1, \ldots, t_m)$$

und suchen Polynome $f_1, \ldots, f_r$ aus $k[X_1, \ldots, X_n]$, die genau auf der Menge aller jener $(x_1, \ldots, x_n)$ verschwinden, für die es eine solche Darstellung gibt.

Dazu wählen wir eine lexikographische Ordnung auf dem Polynomring $k[T_1, \ldots, T_m, X_1, \ldots, X_n]$, bei der alle T_i größer sind als die X_j, und bestimmen eine GRÖBNER-Basis für das von den Polynomen $X_i - \varphi_i(T_1, \ldots, T_m)$ erzeugte Ideal. Dessen Schnitt mit $k[X_1, \ldots, X_n]$ ist ein Eliminationsideal, hat also als Basis genau die Polynome aus der GRÖBNER-Basis, in denen keine T_i vorkommen.

Eine weitere Anwendung von Eliminationsidealen ist die Suche nach einem Gleichungssystem mit vorgegebener (endlicher) Lösungsmenge; dies spielt beispielsweise in der algebraischen Statistik eine Rolle, wenn zu einem vorgegebenen Design die damit schätzbaren Modelle identifiziert werden sollen.

Wir gehen also aus von r Punkten

$$P_i = (x_1^{(i)}, \ldots, x_n^{(i)}) \in k^n, \quad i = 1, \ldots, r,$$

und suchen ein Ideal $I \lhd k[X_1, \ldots, X_n]$, dessen Elemente in den Punkten P_i verschwinden. Im Falle nur eines Punktes P_i können wir einfach das Ideal

$$I_i = (X_1 - x_1^{(i)}, \ldots, X_n - x_n^{(i)})$$

nehmen; bei mehreren Punkten brauchen wir den Durchschnitt der Ideale I_1 bis I_r, für den wir kein offensichtliches Erzeugendensystem haben.

Betrachten wir stattdessen die Punkte

$$Q_i = (x_1^{(i)}, \ldots, x_n^{(i)}, t_1^{(i)}, \ldots, t_r^{(i)}) \in k^{n+r} \quad \text{mit} \quad t_j^{(i)} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases},$$

so erzeugen die Polynome

$$T_i(X_j - x_j^{(i)}) \in k[X_1, \ldots, X_n, T_1, \ldots, T_r]$$

für $i = 1, \ldots, n$ und $j = 1, \ldots, r$ zusammen mit dem Polynom $T_1 + \cdots + T_r - 1$ ein Ideal, das alle Q_i als Nullstellen hat, denn $T_i(X_j - x_j^{(i)})$ verschwindet, da $x_j^{(i)}$ die j-te Koordinate von Q_i ist, und für $\ell \neq i$ verschwindet $T_\ell(X_j - x_j^{(i)})$, da $t_\ell = 0$ ist.

Ist umgekehrt $Q \in k^{n+r}$ keiner der Punkte Q_i, so gibt es für jedes i mindestens eine Koordinate, in der sich Q von Q_i unterscheidet. Ist dies etwa die j-te Koordinate, so ist $X_j - x_j^{(i)}$ in Q von null verschieden; $T_i(X_j - x_j^{(i)})$ kann daher nur verschwinden, wenn $t_i = 0$ ist. Dies kann aber nicht aber alle i der Fall sein, denn die Summe der t_i ist eins. Somit liegt Q nicht in $V(J)$.

Damit haben wir ein Ideal $J \lhd k[X_1, \ldots, X_n, T_1, \ldots, T_r]$ gefunden, dessen Nullstellen genau die Punkte $Q_1, \ldots, Q_r \in k^{n+r}$ sind. Die Punkte $P_1, \ldots, P_r$ sind die Projektionen der Q_i von k^{n+r} nach k^n; deshalb ist klar, daß alle Polynome aus

$$I \underset{\text{def}}{=} J \cap k[X_1, \ldots, X_n]$$

in den Punkten P_i verschwinden.

§7: Der Hilbertsche Nullstellensatz

In diesem Paragraphen wollen wir Kriterien für die Lösbarkeit eines nichtlinearen Gleichungssystems sowie für die Endlichkeit der Lösungsmenge herleiten. Außerdem überlegen wir uns, wann ein Polynom g auf der Lösungsmenge eines nichtlinearen Gleichungssystems verschwindet. Natürlich muß es dann verschwinden, wenn es im von den Gleichungen erzeugten Ideal liegt, aber die Umkehrung dazu gilt nicht: Die Nullstellenmenge des System mit der einzigen Gleichung $(X - Y)^3 = 0$ etwa besteht genau aus den Punkten (x, y) mit $x = y$, und dort verschwindet auch das lineare Polynom $X - Y$, das schon aus Gradgründen nicht im von $(X - Y)^3$ erzeugten Ideal liegen kann.

Wenn wir über einem endlichen Körper arbeiten, beispielsweise dem Körper $\mathbb{F}_p$, haben wir das zusätzliche Problem, daß es Polynome gibt, die auf ganz $\mathbb{F}_p^n$ verschwinden: Nach dem kleinen Satz von FERMAT ist beispielsweise $x^p - x = 0$ für alle $x \in \mathbb{F}_p$, und daraus lassen sich leicht Polynome in n Variablen konstruieren, die auf ganz $\mathbb{F}_p^n$ verschwinden. Wir wollen uns als erstes überlegen, daß dieses Phänomen bei unendlichen Körpern nicht auftreten kann:

Lemma: k sei ein unendlicher Körper und $f \in k[X_1, \ldots, X_n]$ sei nicht das Nullpolynom. Dann gibt es $a_1, \ldots, a_n \in k$ derart, daß $f(a_1, \ldots, a_n)$ nicht verschwindet.

Wir führen den *Beweis* durch Induktion nach n: Für Polynome einer Veränderlichen folgt dies aus der Tatsache, daß ein vom Nullpolynom verschiedenes Polynom höchstens so viele Nullstellen haben kann, wie sein Grad angibt, also auch jeden Fall endlich viele. In einem unendlichen Körper muß es daher Elemente geben, für die das Polynom nicht verschwindet.

Für $n > 1$ schreiben wir $f = f_d X_n^d + f_{d-1} X_n^{d-1} + \cdots + f_1 X_n + f_0$ als Polynom in X_n mit Koeffizienten $f_i \in k[X_1, \ldots, X_{n-1}]$, wobei wir annehmen können, daß der führende Koeffizient f_d nicht das Nullpolynom ist. Nach Induktionsannahme gibt es dann $a_1, \ldots, a_{n-1} \in k$, für die $f_d(a_1, \ldots, a_{n-1})$ nicht verschwindet. Setzen wir $X_1, \ldots, X_{n-1}$ auf

diese Werte, ist daher $f(a_1, \ldots, a_{n-1}, X_n) \in k[X_n]$ nicht das Nullpolynom, hat also nur endlich viele Nullstellen. Wählen wir für $a_n \in k$ irgendein Element, das keine Nullstelle ist, muß $f(a_1, \ldots, a_{n-1}, a_n)$ von Null verschieden sein. ∎

Korollar: Das Polynom $f \in k[X_1, \ldots, X_n]$ über dem unendlichen Körper k habe den Gesamtgrad d. Dann gibt es Elemente $\lambda_i \in k$, für die das Polynom $f(Y_1 + \lambda_1 Y_n, \ldots, Y_{n-1} + \lambda_{n-1} Y_n, Y_n)$ aus dem Polynomring $k[Y_1, \ldots, Y_n] = k[Y_1, \ldots, Y_{n-1}][Y_n]$ als Polynom in Y_n den führenden Term cY_n^d hat mit einem $c \neq 0$ aus k.

Den *Beweis* führen wir wieder durch Induktion nach n: Für $n = 1$ ist $Y_1 = X_1$, und die Behauptung trivial; sei also $n > 1$. Wir schreiben

$$\begin{aligned} g(Y_1, \ldots, Y_n) &\underset{\text{def}}{=} f(Y_1 + \lambda_1 Y_n, \ldots, Y_{n-1} + \lambda_{n-1} Y_n, Y_n) \\ &= \sum_e a_e(\lambda_1, \ldots, \lambda_{n-1}) Y^e \end{aligned}$$

als Polynom in den Y_i mit Koeffizienten aus $k[\lambda_1, \ldots, \lambda_{n-1}]$; die Summe Läuft also über gewisse n-Tupel $e \in \mathbb{N}_0^n$ vom Grad höchstens d. Da wir in f für jedes X_i einen in Y_n linearen Ausdruck eingesetzt haben, führt jedes Monom von f nach Einsetzen und Ausmultiplizieren zu einer Summe, in der ein Term mit Y_n^d vorkommt; der Koeffizient von Y_n^d ist also nicht das Nullpolynom aus $k[\lambda_1, \ldots, \lambda_{n-1}]$. Nach dem gerade bewiesenen Lemma gibt es daher $\lambda_i \in k$, für die dieser Koeffizient von Null verschieden ist, und mit diesen λ_i gilt die Behauptung. ∎

Dieses eher technische Korollar sagt also, daß wir durch eine lineare Koordinatentransformation immer erzwingen können, daß eine der Variablen mit dem Gesamtgrad als Exponenten auftritt. Dies benutzen wir, um zu untersuchen, wann ein Gleichungssystem unlösbar ist.

Dabei wollen wir die *Unlösbarkeit* in einem starken Sinn interpretieren: Die Gleichung $X^2 + 1 = 0$ hat beispielsweise zwar keine reelle Lösung, aber sie hat die beiden komplexen Lösungen $x = \pm i$. So eine Gleichung wollen wir nicht als unlösbar betrachten. Wir definieren

Definition: *a)* Ist I ein Ideal in $k[X_1, \ldots, X_n]$ und ist k' ein Körper, der k enthält, setzen wir

$$V_{k'}(I) = \left\{(z_1, \ldots, z_n) \in k'^n \;\middle|\; f(z_1, \ldots, z_n) = 0 \text{ für alle } f \in I\right\}.$$

b) Erzeugen die Polynome $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ das Ideal I, so sei $V_{k'}(f_1, \ldots, f_m) = V_{k'}(I)$.

Schwache Form des Hilbertschen Nullstellensatzes: k sei ein Körper, K ein algebraisch abgeschlossener Körper, der k enthält, und I sei ein Ideal im Polynomring $k[X_1, \ldots, X_n]$ über k. Dann ist $V_K(I) = \emptyset$ genau dann, wenn das Ideal I die Eins enthält.

In Gleichungen ausgedrückt heißt dies, daß das Gleichungssystem

$$f_i(x_1, \ldots, x_n) = 0 \quad \text{für } i = 1, \ldots, m$$

genau dann keine Lösung in K hat, wenn es $g_1, \ldots, g_m \in k[X_1, \ldots, X_n]$ gibt, für die $g_1 f_1 + \cdots + g_m f_m = 1$ ist.

Der *Beweis* erfolgt auch hier wieder durch vollständige Induktion nach der Anzahl der Variablen:

Für $n = 1$ ist jedes Ideal $I \lhd k[X]$ ein Hauptideal; es sei erzeugt von $f \in k[X]$. Nach Definition eines algebraisch abgeschlossenen Körpers hat f genau dann keine Nullstelle in K, wenn f konstant ist, und das ist äquivalent dazu, daß I die Eins enthält.

Für $n > 1$ betrachten wir ein Erzeugendensystem $f_1, \ldots, f_m$ von I. Nach dem obigen Korollar können wir annehmen, daß f_1 den Term X_n^d enthält, wobei d den Grad von f_1 bezeichnet: Eine lineare Koordinatentransformation ändert schließlich nichts daran, ob $V_K(I)$ leer ist oder nicht und auch nichts daran, ob I die Eins enthält oder nicht.

Wir führen eine neue Variable U ein und betrachten das Polynom

$$h = f_2 + U f_3 + \cdots + U^{m-2} f_m \in k[X_1, \ldots, X_n, U]$$

sowie die Resultante $\mathrm{Res}_{X_n}(f_1, h) \in k[X_1, \ldots, X_{n-1}, U]$. Wir schreiben sie als Polynom

$$\mathrm{Res}_{X_n}(f_1, h) = a_\ell(X_1, \ldots, X_{n-1})U^\ell + \cdots + a_0(X_1, \ldots, X_{n-1})$$

in U mit Koeffizienten aus $k[X_1, \ldots, X_{n-1}]$.

Wie wir am Ende von §1 gesehen haben, läßt sich die Resultante zweier Polynome als Linearkombination dieser Polynome darstellen; es gibt daher Polynome $p, q \in k[X_1, \ldots, X_n, U]$, so daß gilt

$$\mathrm{Res}_{X_n}(f_1, h) = pf_1 + qh = pf_1 + qf_2 + quf_3 + \cdots + qu^{m-2}f_m\,.$$

Vergleichen wir dies mit obiger Darstellung der Resultante als Polynom in U, sehen wir, daß die Koeffizientenpolynome $a_i(X_1, \ldots, X_{n-1})$ im Ideal $I = (f_1, \ldots, f_m)$ liegen müssen.

Wenn wir zeigen können, daß diese Polynome keine gemeinsame Nullstelle in K^{n-1} haben, wissen wir nach Induktionsannahme, daß sich die Eins in $k[X_1, \ldots, X_{n-1}]$ als Linearkombination der a_i darstellen läßt; da diese Polynome in I liegen, liegt die Eins somit erst recht in I, und wir sind fertig.

Angenommen, die a_i hätten eine gemeinsame Nullstelle $(z_1, \ldots, z_{n-1})$ in K^{n-1}. Dann wäre $\mathrm{Res}_{X_n}(f_1, h)(z_1, \ldots, z_{n-1}, U) \in k[U]$ das Nullpolynom. Somit hätten die beiden Polynome

$$f_1(z_1, \ldots, z_{n-1}, X_n) \in k[X_n] \quad \text{und}$$
$$h(z_1, \ldots, z_{n-1}, X_n, U] \in k[X_n, U]$$

einen nichtkonstanten gemeinsamen Faktor. In K gäbe es dann eine Nullstelle z_n von $f_1(z_1, \ldots, z_{n-1}, X_n)$, für die $h(z_1, \ldots, z_{n-1}, z_n, U)$ das Nullpolynom wäre. Nach Definition von h verschwänden dann nicht nur $f_1(z_1, \ldots, z_n)$, sondern auch alle $f_j(z_1, \ldots, z_n)$ für $j = 2, \ldots, m$. Damit läge $(z_1, \ldots, z_n)$ in $V_K(I)$, was wir aber als leer vorausgesetzt haben. Damit ist klar, daß die a_i keine gemeinsame Nullstelle haben können, und der Satz ist bewiesen.

∎

Ob ein Ideal die Eins enthält oder nicht, kann man seiner GRÖBNER-Basis leicht ansehen: Da der führende Term eines jeden Polynoms aus dem Ideal durch den führenden Term eines Elements der GRÖBNER-Basis teilbar sein muß, enthält diese im Falle eines Ideals, das die Eins enthält, ein Polynom, dessen führendes Monom die Eins ist. Da diese bezüglich jeder Monomordnung das kleinste Monom ist, muß somit die GRÖBNER-Basis eine Konstante enthalten. Die zugehörige minimale und erst recht die reduzierte GRÖBNER-Basis besteht in diesem Fall nur aus der Eins.

Kriterium: Ein nichtlineares Gleichungssystem ist genau dann unlösbar selbst über einem algebraisch abgeschlossenen Körper, der k enthält, wenn seine reduzierte GRÖBNER-Basis nur aus der Eins besteht. ∎

Die starke Form des HILBERTschen Nullstellensatzes sagt uns allgemein, welche Polynome auf der Nullstellenmenge eines Ideals verschwinden:

Hilbertscher Nullstellensatz: $I \lhd k[X_1, \ldots, X_n]$ sei ein Ideal, und das Polynom $g \in k[X_1, \ldots, X_n]$ verschwinde in jedem Punkt von $V_K(I)$, wobei K ein algebraisch abgeschlossener Körper sei, der k enthält. Dann gibt es eine natürliche Zahl r, so daß g^r in I liegt.

Beweis: $f_1, \ldots, f_m$ sei ein Erzeugendensystem von I und

$$J = (f_1, \ldots, f_m, Tg - 1) \lhd k[X_1, \ldots, X_n, T] .$$

Für einen Punkt $(z_1, \ldots, z_n, t) \in V_K(J)$ müßte einerseits gelten

$$f_j(z_1, \ldots, z_n) = 0 \quad \text{für alle } j = 1, \ldots, m ,$$

so daß $(z_1, \ldots, z_n)$ in $V_K(I)$ läge; andererseits wäre auch

$$tg(z_1, \ldots, z_n) - 1 = 0 .$$

Da g in allen Punkten aus $V_K(I)$ verschwindet, ist das nicht möglich, also ist $V_K(J) = \emptyset$. Nach der schwachen Form des HILBERTschen Nullstellensatzes muß somit die Eins in J liegen; es gibt also Polynome $a_0, \ldots, a_m \in k[X_1, \ldots, X_n, T]$, so daß

$$a_1 f_1 + \cdots + a_n f_n + a_0(Tg - 1) = 1$$

ist. Im Quotientenkörper von $k[X_1, \ldots, X_n]$ können wir in dieser Identität $T = 1/g$ einsetzen. Dadurch können die Summanden Potenzen von g in ihre Nenner bekommen; durch Multiplikation mit der höchsten auftretenden Potenz g^r erhalten wir eine Polynomgleichung der Form

$$b_1 f_1 + \cdots + b_m f_m = g^r \quad \text{mit} \quad b_j \in k[X_1, \ldots, X_n] .$$

Dies beweist die Behauptung. ∎

Definition: R sei ein Ring und $I \lhd R$ ein Ideal von R. Das *Radikal* von I ist die Menge

$$\sqrt{I} \underset{\text{def}}{=} \left\{ f \in R \;\middle|\; \exists n \in \mathbb{N} : f^n \in I \right\} .$$

Das Radikal besteht also aus allen Ringelementen, die eine Potenz in I haben. Es ist selbst ein Ideal, denn sind $f, g \in \sqrt{I}$ zwei Elemente mit $f^n \in I$ und $g^m \in I$, so sind in

$$(f+g)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} f^{n+m-k} g^k$$

die ersten m Summanden Vielfache von f^n, und die restlichen n sind Vielfache von g^m. Somit liegt jeder Summand in I, also auch die Summe. Für ein beliebiges $r \in R$ liegt natürlich auch ra in $\sqrt{I}$, denn seine n-te Potenz $(ra)^n = r^n a^n$ liegt in I.

Falls ein Ideal mit seinem Radikal übereinstimmt, enthält es *alle* Polynome, die auf $V_K(I)$ verschwinden; zwei Polynome nehmen genau dann in jedem Punkt von $V_K(I)$ denselben Wert an, wenn ihre Differenz in I liegt, wenn sie also modulo I dieselbe Restklasse definieren.

Wenn das Ideal I nicht mit seinem Radikal übereinstimmt, gilt zwar nicht mehr *genau dann,* aber wir können trotzdem die Elemente des Faktorvektorraums $A = k[X_1, \ldots, X_n]/I$ auffassen als Funktionen von $V_K(I)$ nach K: Für jede Restklasse und jeden Punkt aus $V_K(I)$ nehmen wir einfach irgendein Polynom aus der Restklasse und setzen die Koordinaten des Punkts ein. Da die Differenz zweier Polynome aus derselben Restklasse in I liegt, wird sie nach Einsetzen des Punktes zu Null, der Wert hängt also nicht ab von der Wahl des Polynoms. Auch Polynome aus $K[X_1, \ldots, X_n]$ definieren in dieser Weise Funktionen $V_K(I) \to K$; hinreichend (aber nicht notwendig) dafür, daß zwei Polynome dieselbe Funktion definieren ist, daß ihre Differenz im von I erzeugten Ideal $\bar{I} \lhd K[X_1, \ldots, X_n]$ liegt.

Im Falle von Polynomen einer Veränderlichen ist jedes Ideal von $k[X]$ ein Hauptideal; ist $I = (f)$ mit einem Polynom $f \neq 0$ vom Grad d, so können wir die Restklassen repräsentieren durch die Polynome vom Grad höchstens $d - 1$, denn jedes Polynom $g \in k[X]$ hat dieselbe Restklasse wie sein Divisionsrest bei der Polynomdivision durch f. Somit ist $A = k[X]/I$ in diesem Fall ein d-dimensionaler Vektorraum. Da $V_K(I)$ gerade aus den Nullstellen von f in K besteht, von denen es höchstens d verschiedene gibt, liefert die Dimension von A eine obere

Schranke für die Elementanzahl von $V_K(I)$; wenn wir die Nullstellen mit ihrer Vielfachheit zählen, ist die Dimension von A sogar *gleich* der Gesamtzahl der Nullstellen.

Dies gilt auch für Polynome mehrerer Veränderlicher, ist allerdings schwerer zu beweisen. Vielfachheiten werden wir erst im nächsten Paragraphen betrachten; hier begnügen wir uns mit dem folgenden

Satz: I sei ein Ideal im Polynomring $k[X_1, \ldots, X_n]$ über dem Körper k, und K sei ein algebraisch abgeschlossener Körper, in dem k enthalten sei. Dann gilt: $V_K(I)$ ist genau dann endlich, wenn $A = k[X_1, \ldots, X_n]/I$ ein endlichdimensionaler k-Vektorraum ist. In diesem Fall ist die Dimension von A eine obere Schranke für die Elementanzahl von $V_K(I)$.

Den recht umfangreichen *Beweis* führen wir in mehreren Schritten:

1. Schritt: Wenn der Vektorraum A endliche Dimension hat, ist $V_K(I)$ endlich.

Bezeichnet nämlich d die Dimension von A, so sind für jedes i die Potenzen $1, X_i, \ldots, X_i^d$ linear abhängig; es gibt also ein Polynom aus $k[X_i]$, das modulo I zur Null wird. Nach dem HILBERTschen Nullstellensatz liegt eine Potenz davon in I; daher muß für jeden Punkt aus $V_K(I)$ die i-te Koordinate eine Nullstelle dieses Polynoms sein. Damit kann die i-te Koordinate nur endlich viele Werte annehmen, und da dies für alle i gilt, ist $V_K(I)$ endlich.

2. Schritt: Wenn $V_K(I)$ endlich ist, hat der K-Vektorraum $\bar{A} = K[X_1, \ldots, X_n]/\bar{I}$ endliche Dimension.

Besteht $V_K(I)$ nur aus endlich vielen Punkten, so nimmt jede der Koordinatenfunktionen $X_1, \ldots, X_n$ auf $V_K(I)$ nur endlich viele Werte an; es gibt also für jedes i ein Polynom aus $K[X_i]$, das auf ganz $V_K(I)$ verschwindet. Nach dem HILBERTschen Nullstellensatz muß eine Potenz dieses Polynoms in $\bar{I}$ liegen, es gibt also auch in $\bar{I}$ für jedes i ein Polynom nur in X_i. Somit gibt es einen Grad d_i derart, daß sich X_i^e für $e \geq d_i$ modulo $\bar{I}$ durch die endlich vielen X_i-Potenzen $1, X_i, \ldots, X_i^{d_i - 1}$ ausdrücken läßt. Damit läßt sich auch jedes Monom aus $K[X_1, \ldots, X_n]$

modulo $\bar{I}$ durch jene Monome ausdrücken, bei denen jede Variable X_i höchstens mit Exponent $d_i - 1$ auftritt. Da es nur endlich viele solche Monome gibt, ist $K[X_1, \ldots, X_n]/\bar{I}$ ein endlichdimensionaler K-Vektorraum.

3. Schritt: A ist genau dann endlichdimensional, wenn $\bar{A}$ endlichdimensional ist; in diesem Fall haben beide dieselbe Dimension.

Ist A endlichdimensional, so wählen wir eine Basis und zu jedem Basiselement ein Polynom aus $k[X_1, \ldots, X_n]$, das modulo I gleich diesem Element ist. Diese Polynome liegen erst recht in $K[X_1, \ldots, X_n]$, und es ist klar, daß ihre Restklassen modulo $\bar{I}$ den Vektorraum $\bar{A}$ erzeugen. Somit ist auch $\bar{A}$ endlichdimensional. Die Gleichheit von $\dim_k A$ und $\dim_K \bar{A}$ folgt, falls wir zeigen können, daß dieses Erzeugendensystem linear unabhängig ist.

Dazu zeigen wir die folgende, etwas allgemeinere Aussage: Sind $B_1, \ldots, B_r$ Polynome aus $k[X_1, \ldots, X_n]$ mit Restklassen $b_1, \ldots, b_r$ modulo I und Restklassen $\bar{b}_1, \ldots, \bar{b}_r$ modulo $\bar{I}$, so sind die b_i genau dann linear abhängig, wenn es die $\bar{b}_i$ sind.

Die eine Richtung ist einfach: Falls die b_i linear abhängig sind, gibt es Skalare $\lambda_i \in k$, die nicht alle verschwinden, so daß $\lambda_1 b_1 + \cdots + \lambda_r b_r$ der Nullvektor aus A ist. $\bar{\lambda}_1 B_1 + \cdots + \bar{\lambda}_r B_r$ liegt daher in $\bar{I}$, also erst recht in $\bar{I}$, so daß auch $\lambda_1 \bar{b}_1 + \cdots + \lambda_r \bar{b}_r$ der Nullvektor aus $\bar{A}$ ist.

Wenn die $\bar{b}_i$ linear abhängig sind, gibt es $\lambda_i \in K$, so daß $\lambda_1 \bar{b}_1 + \cdots + \lambda_r \bar{b}_r$ der Nullvektor aus $\bar{A}$ ist, d.h. $\lambda_1 B_1 + \cdots + \lambda_r B_r$ liegt in $\bar{I}$. Da die λ_i nicht in k liegen müssen, nützt und das noch nichts, um etwas über die b_i auszusagen.

Um trotzdem deren lineare Abhängigkeit zu beweisen, wählen wir ein endliches Erzeugendensystem $f_1, \ldots, f_m$ des Ideals I; wir wissen dann, daß es Polynome $g_1, \ldots, g_m$ aus $K[X_1, \ldots, X_n]$ gibt mit

$$\lambda_1 B_1 + \cdots + \lambda_r B_r = g_1 f_1 + \cdots + g_m f_m \,.$$

ist. Die Polynome g_j sind K-Linearkombinationen von Monomen $M_{j\ell}$ in den Variablen X_i. Die obige Gleichung ist also äquivalent zu einer

Gleichung der Form

$$\lambda_1 B_1 + \cdots + \lambda_r B_r - \sum_{j=1}^{m} \sum_{\ell=1}^{r_j} \mu_{j\ell} M_{j\ell} f_j = 0$$

mit Elementen $\mu_{j\ell} \in K$, die von den g_j abhängen. Sortieren wir diese Gleichung nach Monomen, können wir dies so interpretieren, daß ein (recht großes) lineares Gleichungssystem in den Variablen λ_i und $\mu_{j\ell}$ eine nichttriviale Lösung hat. Da die B_i und die f_j Polynome mit Koeffizienten aus k sind, ist dies ein homogenes lineares Gleichungssystem mit Koeffizienten aus k. Es hat genau dann nichttriviale Lösungen über k, wenn der Rang seiner Matrix kleiner ist als die Anzahl der Variablen, was man durch das Verschwinden gewisser Determinanten charakterisieren kann.

Da k in K enthalten ist, können wir dieses Gleichungssystem auch über K betrachten; an den Bedingungen für die Lösbarkeit ändert sich dadurch nichts, denn eine Determinante mit Einträgen aus k verschwindet natürlich in K genau dann, wenn sie in k verschwindet.

Somit muß das Gleichungssystem auch eine nichttriviale Lösung über k haben, es gibt also bereits Elemente $\lambda_i' \in k$ und $\mu_{j\ell} \in k$, die das Gleichungssystem lösen. Damit ist dann

$$\lambda_1' B_1 + \cdots + \lambda_r' B_r = g_1' f_1 + \cdots + g_m' f_m$$

mit Polynomen $g_j' \in k[X_1, \ldots, X_n]$, die linke Seite liegt also im Ideal I. Somit ist $\lambda_1' b_1 + \cdots + \lambda_r' b_r$ der Nullvektor in A. Die λ_i' können nicht allesamt verschwinden, denn ansonsten müßte mindestens ein $\mu_{j\ell} \neq 0$ sein, Null wäre also gleich einer nichttrivialen Linearkombination von Monomen, was absurd ist. Also sind auch die b_i linear abhängig.

Bleibt noch zu zeigen, daß A endlichdimensional ist, wenn $\bar{A}$ endlichdimensional ist. Das folgt sofort aus der gerade gezeigten Äquivalenz der linearen Abhängigkeit über k und über K: Hat $\bar{A}$ die endliche Dimension d, so ist jede Teilmenge von $\bar{A}$ mit mehr als d Elementen linear abhängig. Damit ist, wie wir gerade gesehen haben, auch jede Teilmenge von mehr als d Elementen aus A linear abhängig, also A endlichdimensional.

4. Schritt: Falls $V_K(I)$ endlich ist, gibt es ein homogenes lineares Polynom $u = c_1X_1 + \cdots c_nX_n$ aus $K[X_1, \ldots, X_n]$, das für jeden Punkt aus $V_K(I)$ einen anderen Wert annimmt.

Wir betrachten die Polynome $u_a = X_1 + aX_2 + \cdots + a^{n-1}X_n$ zu den verschiedenen Elementen $a \in K$. Für je zwei verschiedene Punkte $z, w \in V_K(I)$ ist $u_a(z) = u_a(w)$ genau dann, wenn

$$(z_1 - w_1) + (z_2 - w_2)a + \cdots + (z_n - w_n)a^{n-1}$$

verschwindet. Die Koordinaten z_i, w_i von z und w sind Elemente von K; die $a \in K$, für die $u_a(z) = u_a(w)$ ist, sind also die Nullstellen eines Polynoms in einer Veränderlichen über K vom Grad höchstens $n - 1$. Daher gibt es höchstens $n - 1$ Werte $a \in K$, für die $u_a(z) = u_a(w)$ ist. Wenn $V_K(I)$ endlich ist, gibt es auch nur endlich viele verschiedene Paare aus voneinander verschiedenen Elementen; somit gibt es nur endlich viele $a \in K$, für die $u_a(z) = u_a(w)$ sein kann für *irgendwelche* voneinander verschiedene Elemente von $V_K(I)$. Da K als algebraisch abgeschlossener Körper unendlich sein muß, gibt es somit Polynome u_a, die für je zwei verschiedene Elemente von $V_K(I)$ verschiedene Werte annehmen. Falls bereits k ein unendlicher Körper ist, können wir sogar entsprechende $a \in k$ finden; in diesem Fall gibt es also schon in $k[X_1, \ldots, X_n]$ solche Polynome.

5. Schritt: Die Elementanzahl r von $V_K(I)$ ist höchstens gleich der Dimension von A.

Da wir im 3. Schritt gesehen haben, daß $\dim_k A = \dim_K \bar{A}$ ist, können wir auch mit dieser Dimension argumentieren. Aus dem 5. Schritt wissen wir, daß es ein Polynom $u \in K[X_1, \ldots, X_n]$ gibt, das für jedes Element von $V_K(I)$ einen anderen Wert annimmt. Wir ersetzen u durch seine Restklasse $\tilde{u}$ modulo $\bar{I}$ in $\bar{A}$. Wir wollen uns überlegen, daß die Elemente $1, \tilde{u}, \ldots, \tilde{u}^{r-1} \in \bar{A}$ linear unabhängig sind, wenn $V_K(I)$ mindestens r Elemente enthält: Falls es eine Relation der Form $\sum_{\ell=0}^{r-1} \lambda_\ell \tilde{u}^\ell = 0$ gäbe mit $\lambda_\ell \in k$, so läge das Polynom $\sum_{\ell=0}^{r-1} \lambda_\ell u^\ell$ in $\bar{I}$, würde also für jedes der r Elemente von $V_K(I)$ verschwinden. Da u für jedes dieser Elemente einen anderen Wert annimmt, ist dies bei einem Polynom vom Grad r nur möglich, wenn alle Koeffizienten λ_ℓ verschwinden, was die behauptete

lineare Unabhängigkeit beweist. Somit enthält $\bar{A}$ mindestens r linear unabhängige Elemente, d.h. $\dim_K \bar{A} \geq r$. Damit ist die Behauptung und auch der gesamte Satz bewiesen.

■

In der Computeralgebra interessieren wir uns nicht in erster Linie für abstrakte Sätze über Nullstellenmenge und Ideale; wir wollen die Lösungsmengen eines Systems von Polynomgleichungen möglichst explizit angeben. Die beste Chance dazu haben wir, wenn die Lösungsmenge endlich ist; daher interessieren wir uns für möglichst einfache Kriterien dafür, daß $V_K(I)$ eine endliche Menge ist. (Die eigentlich sehr viel interessantere Frage nach der Endlichkeit von $V_k(I)$ ist um soviel schwieriger zu beantworten, daß sie jenseits unserer Ambitionen bleiben muß; halbwegs allgemeine Resultate hierzu sind zumindest derzeit unbekannt.)

Wie wir gerade gesehen haben, ist diese Endlichkeit äquivalent zur Endlichdimensionalität des Vektorraums A; wir suchen daher Kriterien, die dies garantieren. Da wir uns im Kapitel über GRÖBNER-Basen befinden, sollten diese auch damit etwas zu tun haben.

Wir betrachten daher zwar weiterhin ein Gleichungssystem der Form

$$f_j(x_1, \ldots, x_n) = 0 \quad \text{für } j = 1 \ldots, m \quad \text{mit} \quad f_j \in k[X_1, \ldots, X_n]\,,$$

nehmen aber an, daß wir eine GRÖBNER-Basis G des von den Polynomen $f_j \in k[X_1, \ldots, X_n]$ erzeugten Ideals I bezüglich irgendeiner Monomordnung kennen.

Wir müssen dann entscheiden, ob der Vektorraum $A = k[X_1, \ldots, X_n]/I$ endliche Dimension hat. Im eindimensionalen Fall ist das einfach: I ist dann ein Hauptideal, eine reduzierte GRÖBNER-Basis besteht nur aus einem Element, und wenn dieses ein Polynom vom Grad d ist, hat $A = k[x]/I$ die Restklassen der Elemente $1, X, \ldots, X^{d-1}$ als Basis.

Ähnlich können wir auch im Falle mehrerer Veränderlicher argumentieren: Wenden wir den Divisionsalgorithmus an auf ein beliebiges Polynom und die GRÖBNER-Basis, erhalten wir eine Darstellung des Polynoms als Summe einer Linearkombination mit Koeffizienten aus $k[X_1, \ldots, X_n]$ von Elementen der GRÖBNER-Basis und einem Rest.

Dieser ist eine k-Linearkombination von Monomen, die durch kein führendes Monom eines Elements der GRÖBNER-Basis teilbar sind. Somit bilden diese Monome eine Basis des Vektorraums A; falls es nur endlich viele davon gibt, ist A endlichdimensional.

Einfacher ist das folgende Kriterium:

Lemma: $V_K(I)$ ist genau dann endlich, wenn die GRÖBNER-Basis von I (bezüglich irgendeiner Monomordnung) für jedes i ein Polynom mit einer X_i-Potenz als führenden Term enthält.

Beweis: Falls die GRÖBNER-Basis für jedes i ein Polynom mit führendem Monom $X_i^{d_i}$ enthält, ist jedes Monom, in dem ein X_i mit einem Exponenten größer oder gleich d_i vorkommt, durch das führende Monom eines Elements der GRÖBNER-Basis teilbar. Die Monome, für die das nicht der Fall ist, haben für jedes i einen Exponenten echt kleiner d_i; es gibt also nur endlich viele solche Monome. Somit hat A endliche Dimension, und $V_K(I)$ ist endlich.

Ist umgekehrt $V_K(I)$ endlich, so enthält $\bar{I}$ für jedes i ein Polynom aus $K[X_i]$ – siehe Schritt 2 im Beweis des obigen Satzes. Da die GRÖBNER-Basis von I gleichzeitig eine GRÖBNER-Basis von $\bar{I}$ ist, muß das führende Monom eines ihrer Elemente die höchste X_i-Potenz in diesem Polynom teilen, muß also selbst eine Potenz von X_i sein. ∎

§8: Multiplizitäten

Um, wie im eindimensionalen Fall, statt einer Ungleichung eine Gleichung für die Anzahl der Nullstellen zu bekommen, müssen wir diesen eine Vielfachheit oder, wie man auch sagt, Multiplizitäten zuordnen. Im Falle von Polynomen einer Veränderlichen können wir diese mit Hilfe von Ableitungen definieren; falls wir über den reellen Zahlen arbeiten, reicht zur Bestimmung der Multiplizität daher die Kenntnis einer beliebig kleinen ε-Umgebung.

In der Algebra haben wir keine ε-Umgebungen, aber wir können uns auch mit algebraischen Methoden auf die Umgebung eines Punktes

konzentrieren: Wir betrachten einfach an Stelle von Polynomen beliebige rationale Funktionen, von denen wir nur verlangen, daß der Nenner im betrachteten Punkt nicht verschwindet.

Sei zunächst $f \in k[X]$ ein Polynom einer Veränderlichen, das im Punkt z eine r-fache Nullstelle habe. Dann ist $f = (X-z)^r g$ mit einem Polynom $g \in k[X]$, das an der Stelle z nicht verschwindet. Der im vorigen Paragraphen eingeführte Faktorraum $\bar{A} = K[X]/(f)$ hat als Basis die Potenzen X^ℓ mit $0 \le \ell < \deg f$; alternativ können wir natürlich auch die entsprechenden Potenzen $(X-z)^\ell$ nehmen. Dann verschwindet ein Element von A genau dann im Punkt z, wenn es im von den $(X-z)^\ell$ mit $\ell > 0$ aufgespannten Untervektorraum liegt.

Wenn wir alle anderen Elemente von A als Nenner zulassen, sollte man zunächst erwarten, daß A dadurch größer wird. Tatsächlich aber ist das Gegenteil der Fall: Wenn wir von den üblichen Regeln der Bruchrechnung ausgehen, ist beispielsweise

$$(X-z)^r = \frac{(X-z)^r}{1} = \frac{(X-z)^r g}{g} = \frac{f}{g} = \frac{0}{g} = 0\,,$$

denn wir rechnen ja modulo f, und g ist als Nenner zugelassen, da $g(z)$ nicht verschwindet. Entsprechendes gilt für alle $(X-z)^\ell$ mit $\ell \ge r$, nicht aber für die mit $\ell < r$, denn hier bräuchten wir ja noch mindestens einen Faktor $(X-z)$, um im Zähler auf f zu kommen, und Funktionen, die in z verschwinden, sind im Nenner nicht erlaubt. Durch das Einführen solcher Nenner verringert sich also die Dimension von A; der neue Vektorraum hat nur noch die Dimension r, was gleich der Vielfachheit der Nullstelle z ist. Wir können ihn über die Basis aus den $(X-z)^\ell$ mit $\ell < r$ identifizieren mit einem r-dimensionalen Untervektorraum von $\bar{A}$, und die Dimensionen der so definierten Unterräume zu den verschiedenen Nullstellen von f ergänzen sich zur Dimension von $\bar{A}$.

Für Polynome einer Veränderlichen ist das sicherlich eine sehr umständliche Art der Betrachtung; sie hat aber den Vorteil, daß sie sich auf Polynome in mehreren Veränderlichen verallgemeinern läßt.

Als erstes müssen wir klar definieren, was oben kurz als die „Einführung von Nennern“ bezeichnet wurde:

Definition: R sei ein (kommutativer) Ring.
a) Eine Teilmenge $S \subseteq R \setminus \{0\}$ heißt *multiplikativ abgeschlossen,* wenn sie mit je zwei Elementen $f, g \in S$ auch deren Produkt enthält.
b) Die *Lokalisierung* von R nach der multiplikativ abgeschlossenen Menge S ist die Menge aller Paare $(f, g) \in R \times S$ modulo der folgenden Äquivalenzrelation:

$$(f, g) \sim (f', g') \Longleftrightarrow \exists h \in R \setminus \{0\} : h(fg' - f'g) = 0\,.$$

Die Äquivalenzklasse des Paars (f, g) wird mit $\frac{f}{g}$ bezeichnet, die Menge aller Äquivalenzklassen mit $S^{-1}R$. Sie wird zum Ring durch die Verknüpfungsdefinitionen

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'} \quad \text{und} \quad \frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}\,.$$

Man sollte sich kurz überlegen, daß diese Verknüpfungen wohldefiniert sind, daß das Ergebnis also nicht von der Wahl spezieller Repräsentanten (f, g) und (f', g') abhängt; im wesentlichen ist dies die gleiche Rechnung wie bei der Einführung des Quotientenkörpers in Kapitel 2§6.

Falls R nullteilerfrei ist, können wir in der Definition der Äquivalenzrelation auf des Element h verzichten, denn wenn $h(fg' - f'g)$ für ein $h \neq 0$ verschwindet, muß der zweite Faktor Null sein. Da unsere Ringe A und $\bar{A}$ im allgemeinen nicht nullteilerfrei sind, ist – wie wir gerade am Beispiel der Polynome einer Veränderlichen gesehen haben – die Möglichkeit zur Erweiterung mit Nullteilern wesentlich.

Die größte multiplikativ abgeschlossene Teilmenge eines Integritätsbereichs R ist $S = R \setminus \{0\}$; in diesem Fall ist $S^{-1}R$ der Quotientkörper. Falls R Nullteiler enthält, d.h. Elemente $g \neq 0$, zu denen es ein $h \neq 0$ gibt mit $gh = 0$, ist $R \setminus \{0\}$ nicht mehr multiplikativ abgeschlossen: Zwar liegen g und h in $R \setminus \{0\}$, nicht aber deren Produkt. In diesem Fall besteht die größte multiplikativ abgeschlossene Teilmenge $S \subset R$ aus allen $f \in R$, für die es kein $g \neq 0$ gibt mit $fg = 0$, wir müssen also außer der Null auch noch alle Nullteiler ausschließen. Die Menge $S^{-1}R$ wird in diesem Fall als *vollständiger Quotientenring* von R bezeichnet. Man beachte, daß sich R in so einem Fall nicht injektiv in

$S^{-1}R$ einbetten läßt: Für einen Nullteiler h und ein $g \neq 0$ mit $hg = 0$ ist $h/1 = hg/g = 0/g = 0$.

Weitere typische Beispiele multiplikativ abgeschlossener Teilmengen eines Rings sind die Potenzen eines Nichtnullteilers oder auch das Komplement eines Primideals: Ein Ideal $I \lhd R$ heißt *Primideal* wenn für je zwei Elemente $f, g \in R$ mit $fg \in I$ mindestens einer der beiden Faktoren f, g in I liegt. Dies ist offensichtlich äquivalent dazu, daß die Menge $R \setminus I$ multiplikativ abgeschlossen ist.

Wir interessieren uns für Ideale $I \lhd k[X_1, \ldots, X_n]$, für die $V_K(I)$ eine endliche Menge ist; dabei bezeichnet K wie üblich einen algebraisch abgeschlossenen Körper, der k enthält. Die Elemente der Vektorräume $A = k[X_1, \ldots, X_n]/I$ und $\bar{A} = K[X_1, \ldots, X_n]/\bar{I}$ können wir als Funktionen auf $V_K(I)$ mit Werten in K interpretieren. Da sich Funktionen miteinander multiplizieren lassen, sind auch A und $\bar{A}$ Ringe, deren Multiplikation offensichtlich mit der im Polynomring kompatibel ist. Für jedes $z \in V_K(I)$ ist die Menge

$$S_z = \left\{ f \in \bar{A} \;\middle|\; f(z) \neq 0 \right\}$$

multiplikativ abgeschlossen, denn die Funktionswerte liegen ja im (nullteilerfreien) Körper K. Diese Lokalisierungen wollen wir im folgenden genauer untersuchen.

Definition: *a)* $\bar{A}_z \underset{\text{def}}{=} S_z^{-1}\bar{A}$
b) Die *Vielfachheit* oder *Multiplizität* einer Nullstelle $z \in V_K(I)$ ist die Dimension von $\bar{A}_z$ als K-Vektorraum.

Wie wir oben gesehen haben, entspricht dies für Polynome einer Veränderlichen der gewohnten Vielfachheit; wir wollen uns überlegen, daß sich die Vielfachheiten der verschiedenen Elemente von $V_K(I)$ auch im Falle von Polynomen mehrerer Veränderlichen zu $\dim_K \bar{A}$ addieren.

Dazu benötigen wir noch einen Begriff aus der Linearen Algebra:

Definition: $V_1, \ldots, V_r$ seien Vektorräume über dem Körper k. Die direkte Summe

$$\bigoplus_{i=1}^{r} V_i = V_1 \oplus \cdots \oplus V_r$$

ist als Menge gleich dem kartesischen Produkt $V_1 \times \cdots V_r$ der Vektorräume; die Vektorraumaddition ist definiert durch

$$(v_1, \ldots, v_r) + (w_1, \ldots, w_r) = (v_1 + w_1, \ldots, v_r + w_r)\,,$$

und für die Multiplikation mit einem Skalar $\lambda \in k$ setzen wir

$$\lambda(v_1, \ldots, v_n) = (\lambda v_1, \ldots, \lambda v_n)\,.$$

Die Vektorräume V_i können identifiziert werden mit jenen Untervektorräumen von $\oplus_{i=1}^{r} V_i$, in denen alle Komponenten außer eventuell der i-ten gleich dem Nullvektor sind.

Wenn alle Räume V_i endliche Dimensionen haben, ist die Dimension ihrer direkten Summe offensichtlich einfach die Summe dieser Dimensionen: Wählen wir in jedem der Vektorräume V_i eine Basis und fassen wir V_i auf als Untervektorraum der direkten Summe, so ist die Vereinigung der Basen der V_i offensichtlich eine Basis des Summenraums. Insbesondere ist jeder endlichdimensionale k-Vektorraum mit einer Basis $b_1, \ldots, b_n$ isomorph zur direkten Summe der eindimensionalen Untervektorräume kb_i.

Satz: Ist $V_K(I)$ endlich, so ist $\bar{A} \cong \bigoplus_{z \in V_K(I)} \bar{A}_z$

Beweis: Wie wir aus dem vorigem Paragraphen wissen (4. Schritt im Beweis des letzten Satzes), gibt es ein homogenes lineares Polynom über K, das für jeden Punkt aus $V_K(I)$ einen anderen Wert annimmt. Durch einen linearen Koordinatenwechsel können wir erreichen, daß x_1 diese Eigenschaft hat. Wir bezeichnen die x_1-Koordinate eines Punktes $z \in V_K(I)$ mit z_1 und betrachten die LAGRANGE-Polynome

$$s_z = \frac{\prod_{w \in V_K(I) \setminus \{z\}} (X_1 - w_1)}{\prod_{w \in V_K(I) \setminus \{z\}} (z_1 - w_1)} \in K[X_1]\,;$$

offensichtlich ist $s_z(z) = 1$ und $s_z(w) = 0$ für alle $w \neq z$ aus $V_K(I)$. Somit verschwindet das Produkt $s_z s_w$ zweier solcher Funktionen in jedem Punkt von $V_K(I)$; nach dem HILBERTschen Nullstellensatz liegt daher eine Potenz von $s_z s_w$ im Ideal $\bar{I}$. Bezeichnet r den größten Exponenten, den wir für eines der Produkte $s_z s_w$ brauchen, haben daher die

Polynome $t_z = s_z^r$ die Eigenschaft, daß $t_z t_w$ für $z \neq w$ in $\bar{I}$ liegt, und $t_z(z) = 1$.

Wir betrachten nun das Ideal J von $K[X_1, \ldots, X_n]$, das von I und den sämtlichen t_z erzeugt wird. Es hat offensichtlich keine gemeinsame Nullstelle, denn die gemeinsamen Nullstellen von $\bar{I}$ sind die $z \in V_K(I)$, und für jedes dieser z ist $t_z(z) = 1$. Nach der schwachen Form des HILBERTschen Nullstellensatzes enthält J daher die Eins; es gibt also Polynome $p_z \in K[x_1, \ldots, x_n]$ und ein Polynom $p \in \bar{I}$, so daß

$$\sum_{z \in V_K(I)} p_z t_z + p = 1$$

ist. Die Restklassen $e_z \in \bar{A}$ von $p_z t_z$ modulo $\bar{I}$ erfüllen die Gleichungen

1.) $\sum_{z \in V_K(I)} e_z = 1$
2.) $e_z^2 = e_z$
3.) $e_z(z) = 1$
4.) $e_z e_w = 0$ für $z \neq w$ aus $V_K(I)$

Die einzige noch nicht gezeigte Aussage ist 2.); sie folgt aus der Gleichung

$$e_z - e_z^2 = e_z(1 - e_z) = e_z \sum_{w \neq z} e_w = \sum_{w \neq z} e_z e_w = 0 .$$

Elemente e eines Rings R mit der Eigenschaft $e^2 = e$ bezeichnet man als *Idempotente;* sie haben die Eigenschaft, daß das Ideal $(e) = Re$ selbst ein Ring ist mit e als der Eins, denn $(ae)(be) = abe^2 = abe$ für alle $a, b \in R$.

Wir wollen uns als nächstes überlegen, daß der Ring $\bar{A}e_z$ isomorph ist zur Lokalisierung von $\bar{A}$ bei z; der Isomorphismus ist gegeben durch

$$\begin{cases} \bar{A}e_z \to \bar{A}_z \\ f e_z \mapsto \dfrac{f}{1} \end{cases} .$$

Zum Nachweis der Bijektivität konstruieren wir eine Umkehrabbildung $\bar{A}_z \to \bar{A}e_z$ wie folgt: Zu jedem $g \in \bar{A}$ mit $g(z) \neq 0$ setzen wir

$$\tilde{g} \underset{\text{def}}{=} \frac{g}{g(z)} - 1 \in \bar{A}_z, \quad \text{d.h.} \quad g = g(z)(1 + \tilde{g}) .$$

Da $\tilde{g}(z)$ verschwindet und $e_z(w) = 0$ für alle $w \neq z$, verschwindet $\tilde{g}e_z$ auf ganz $V_K(I)$. Nach dem HILBERTschen Nullstellensatz gibt es somit eine Potenz eines Repräsentanten, die in $\bar{I}$ liegt, d.h. es gibt eine natürliche Zahl N, so daß $\big(\tilde{g}e_z\big)^N = \tilde{g}^N e_z$ die Null von $\bar{A}$ ist. Dann ist

$$(1+\tilde{g})e_z \cdot \big(1 - \tilde{g} + \tilde{g}^2 - \cdots + (-1)^{N-1}\tilde{g}^{N-1}\big)e_z = (1 - \tilde{g}^N)e_z = e_z\,;$$

im Ring $\bar{A}_z$ hat also $1+\tilde{g}$ ein Inverses und damit auch $ge_z = g(z)(1+\tilde{g})e_z$. Wir bilden daher den Bruch $f/g \in \bar{A}_z$ ab auf

$$f \cdot \frac{1}{g(z)} \cdot \big(1 - \tilde{g} + \tilde{g}^2 - \cdots + (-1)^{N-1}\tilde{g}^{N-1}\big)e_z \in \bar{A}_z\,,$$

und mit Hilfe der gerade durchgeführten Rechnung folgt leicht, daß die beiden Abbildungen zueinander invers, also Isomorphismen sind.

Zum Beweis des Satzes fehlt nun nur noch, daß $\bar{A}$ die direkte Summe der Ringe $\bar{A}e_z$ ist; das ist klar, da die Summe der e_z gleich eins ist und $e_z e_w = 0$ für $z \neq w$.

■

Weiteres über den Umgang mit Multiplizitäten und die Lösung nichtlinearer Gleichungssysteme mit endlicher Lösungsmenge findet man zum Beispiel in dem Übersichtsartikel

LAUREANO GONZALEZ-VEGA, FABRICE ROUILLIER, MARIE-FRANÇOISE ROY: Symbolic Recipes for Polynomial System Solving *in:* ARJEH M. COHEN, HANS CUYPERS, HANS STERK [EDS.]: Some Tapas of Computer Algebra, *Springer,* 1999,

dessen Anfangsteil ich in diesem und dem vorigen Paragraphen weitgehend folgte.