Kapitel 2
Systeme von nichtlinearen Polynomgleichungen

GRÖBNER-Basen haben eine Vielzahl von Anwendungen in der Algebra; wir wollen uns hier vor allem damit beschäftigen, wie sie direkt oder im Zusammenspiel mit anderen Methoden zur expliziten Lösung nichtlinearer Gleichungssysteme führen können. Explizit angebbar sind die Lösungen meist nur, wenn die Lösungsmenge endlich ist; daher werden wir uns meist auf solche Systeme beschränken und interessieren uns daher auch für Kriterien, wie wir einem Gleichungssystem die Endlichkeit seiner Lösungsmenge ansehen können.

§1: Gröbner-Basen für nichtlineare Gleichungssysteme

Wir gehen 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

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

Diese wird allerdings oft leer sein; für $f_1 = X^2 - 2$ und $f_2 = Y^2 - 3$ aus $\mathbb{Q}[X]$ etwa ist diese Menge leer, da die Lösungen $(\pm\sqrt{2}, \pm\sqrt{3})$ nicht in $\mathbb{Q}^2$ liegen. Wir betrachten daher meist noch einen zweiten Körper K, der k enthält, und interessieren uns allgemeiner für die Lösungsmenge in K^n:

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

$$V_K(I) = \left\{(x_1, \ldots, x_n) \in K^n \;\middle|\; f(x_1, \ldots, x_n) = 0 \text{ für alle } f \in I\right\}.$$

b) Für $I = (f_1, \cdots, f_m)$ schreiben wir auch kurz $V_K(f_1, \ldots, f_m)$ an Stelle von $V_K(I)$.

Der Körper k sollte dabei möglichst klein sein, denn mit den Elementen dieses Körpers müssen wir rechnen, und je größer der Körper, desto aufwendiger sind seine Rechenoperationen. In konkreten Beispielen werden wir uns meist auf $k = \mathbb{Q}$ beschränken und – soweit möglich – sogar versuchen, unsere Konstruktionen in $\mathbb{Z}[X]$ durchzuführen.

Der Körper K hingegen sollte so groß sein, daß er für ein Gleichungssystem, daß in irgendeinem Körper eine nichtleere endliche Lösungsmenge hat, diese Lösungsmenge enthält. Wir werden meist $K = \mathbb{C}$ betrachten.

Wie wir bereits aus §1 des vorigen Kapitels wissen, hängt die Lösungsmenge des Gleichungssystems nur ab vom Ideal $I = (f_1, \ldots, f_m)$; wir suchen ein Erzeugendensystem $\{g_1, \ldots, g_r\}$ dieses Ideals, aus dem wir mehr über die Mengen

$$V_K(I) = V_K(f_1, \ldots, f_m) = V_K(g_1, \ldots, g_r)$$

ablesen können. Wir erwarten natürlich, daß wir hier vor allem im Falle einer geeigneten GRÖBNER-Basis $\{g_1, \ldots, g_r\}$ eventuell Erfolg haben.

Viele Lösungsansätze für Gleichungssysteme in mehreren Veränderlichen beruhen auf der Elimination von Variablen: Im ℓ-ten Schritt suchen wir nach Bedingungen, die ein $(n - \ell)$-Tupel $(x_{\ell+1}, \ldots, x_n)$ erfüllen muß, wenn es ein ℓ-Tupel $(x_1, \ldots, x_\ell)$ gibt, so daß $(x_1, \ldots, x_n)$ in $V(I)$ liegt. Eine solche Bedingung ist trivial: Für jedes Polynom $f \in I$, in dem die Variablen $X_1, \ldots, X_\ell$ nicht vorkommen, muß $f(x_{\ell+1}, \ldots, x_n) = 0$ sein.

Definition: *a)* Das ℓ-te *Eliminationsideal* eines Ideal $I \lhd k[X_1, \ldots, X_n]$ ist $I_\ell = I \cap k[X_{\ell+1}, \ldots, X_n]$.
b) Eine Monomordnung $<$ heißt *Eliminationsordnung* für $X_1, \ldots, X_\ell$, wenn jedes Monom, das mindestens eine der Variablen $X_1, \ldots, X_\ell$ enthält, größer ist als alle Monome, die nur $X_{\ell+1}, \ldots, X_n$ enthalten.

Die lexikographische Ordnung mit $X_1 > X_2 > \cdots > X_{n-1} > X_n$ ist offensichtlich für jedes ℓ eine Eliminationsordnung für $X_1, \ldots, X_\ell$, die

graduiert lexikographische aber nicht, da bezüglich dieser beispielsweise $X_1 < X_n^2$ ist.

Satz: Ist G eine GRÖBNER-Basis von I bezüglich einer Eliminationsordnung für $X_1, \ldots, X_\ell$, so ist $G \cap I_\ell$ eine GRÖBNER-Basis von I_ℓ.

Beweis: Die Elemente von $G = \{g_1, \ldots, g_m\}$ seien so angeordnet, daß $G \cap I_\ell = \{g_1, \ldots, g_r\}$ ist. Wir müssen zeigen, daß sich jedes $f \in I_\ell$ als Linearkombination von $g_1, \ldots, g_r$ mit Koeffizienten aus $k[X_{\ell+1}, \ldots, X_n]$ darstellen läßt.

Der Divisionsalgorithmus bezüglich der gewählten Ordnung gibt uns eine Darstellung $f = h_1 g_1 + \cdots + h_m g_m$ von f als Element von I. Die Polynome $g_{r+1}, \ldots, g_m$ enthalten jeweils mindestens eine der Variablen $X_1, \ldots, X_\ell$, und da wir eine Eliminationsordnung verwenden, muß auch das führende Monom eine dieser Variablen enthalten. Da kein Monom von f eine dieser Variablen enthält, kann im Divisionsalgorithmus das führende Monom eines dieser Polynome nie Teiler des führenden Monoms des jeweils betrachteten Polynoms p sein, Somit ist $h_{r+1} = \cdots = h_m = 0$, und in keinem der Polynome $h_1, \ldots, h_r$ kann eine der Variablen $X_1, \ldots, X_\ell$ auftreten. Dies zeigt, daß f im von $g_1, \ldots, g_r$ erzeugten Ideal von $k[X_{\ell+1}, \ldots, X_n]$ liegt, d.h. dieses Ideal wird von $g_1, \ldots, g_r$ erzeugt.

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 $g_1, \ldots, g_r$ 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, d.h. $S(g_i, g_j)$ ist als Linearkombination von $g_1, \ldots, g_r$ mit Koeffizienten aus $k[g_1, \ldots, g_r]$ darstellbar. ∎

Daraus ergibt sich eine Strategie zur Lösung nichtlinearer Gleichungssysteme nach Art des GAUSS-Algorithmus: Wir gehen aus von der lexikographischen Ordnung, die ja für jedes ℓ eine Eliminationsordnung für $X_1, \ldots, X_\ell$ ist, und bestimmen eine (reduzierte) GRÖBNER-Basis für das von den Gleichungen erzeugte Ideal des Polynomrings $k[X_1, \ldots, X_n]$.

Dann 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 (in K) 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. Diese erhalten wir, indem wir bei allen Erzeugenden des Eliminationsideals I_{n-2} für X_n nacheinander die Werte aus $V_K(I_{n-1}) \subset k$ einsetzen. Nachdem wir so $V_K(I_{n-2}) \subset K^2$ bestimmt haben, können wir analog die Mengen $V_K(I_{n-3}) \subset K^3$ und so weiter bis $V_K(I) \subset K^n$ bestimmen.

Betrachten wir noch einmal das Beispiel gegen Ende von §5 des vorigen Kapitels mit

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

Dort hatten wir die reduzierte GRÖBNER-Basis bezüglich der graduiert lexikographischen Ordnung berechnet; sie besteht aus

$$g_1 = X^2, \quad g_2 = XY \quad \text{und} \quad g_3 = Y^2 - \frac{X}{2}\,.$$

Da die graduiert lexikographische Ordnung keine Eliminationsordnung für X ist, können wir nicht erwarten, daß $\{g_1, g_2, g_3\} \cap k[Y]$ ein Erzeugendensystem des Eliminationsideals $(f_1, f_2) \cap k[Y]$ liefert, und in der Tat liegt keines der g_i in $k[Y]$. Zufälligerweise liegt aber $g_1 = X^2$ in $k[X]$, wir wissen also, daß für jede Lösung (x, y) des Gleichungssystems $x = 0$ sein muß. $g_2 = XY$ verschwindet für alle solche Punkte automatisch, und $g_3 = Y^2 - X/2$ verschwindet genau dann, wenn auch $y = 0$ ist. Somit ist $V_K(f_1, f_2) = \{(0,0)\}$ für jeden Erweiterungskörper K von k.

Wenn wir das Gleichungssystem mit dem hier vorgestellten Verfahren lösen wollen. können wir zum Beispiel mit der lexikographischen Ordnung arbeiten. Da die führenden Terme von f_1 und f_2 bei beiden Ordnungen gleich sind und viele der zu berechnenden S-Polynome nur aus

einem Term bestehen, ändert sich zunächst nichts: Wie bei der graduiert lexikographischen Ordnung kommen wir auf

$$f_3 = S(f_1, f_2) = -X^2, \quad f_4 = S(f_1, f_3) = -2XY \quad \text{und}$$
$$f_5 = S(f_2, f_3) = X - 2Y^2 .$$

Auch $S(f_1, f_4) = -2XY^2 = Y f_4$ kann wie dort auf Null reduziert werden, bei der Berechnung von $S(f_1, f_5)$ ist jetzt aber nicht mehr Y^2, sondern X das führende Monom. Somit ist

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

das S-Polynom läßt sich also modulo $\{f_1, f_2, f_3, f_4, f_5\}$ nicht auf Null reduzieren und wir müssen $f_6 = 4Y^3$ als neues Element in die Basis aufnehmen. Erst jetzt zeigt eine mühsame Rechnung, die man am besten seinem Computer überläßt, daß $S(f_i, f_j)$ für alle $1 \leq i < j \leq 6$ modulo $\{f_1, f_2, f_3, f_4, f_5, f_6\}$ auf Null reduziert werden kann, womit wir eine GRÖBNER-Basis gefunden haben.

Die führenden Monome der sechs Basiselemente bezüglich der lexikographischen Ordnung sind

$$\begin{array}{lll} \mathrm{FM}(f_1) = X^3 , & \mathrm{FM}(f_2) = X^2Y , & \mathrm{FM}(f_3) = -X^2 , \\ \mathrm{FM}(f_4) = -2XY , & \mathrm{FM}(f_5) = X, , & \mathrm{FM}(f_6) = 4Y^3 ; \end{array}$$

wir können also f_1 bis f_4 eliminieren. Die reduzierte GRÖBNER-Basis bedeutet besteht somit aus $g_1 = X - 2Y^2$ und $g_2 = Y^3$.

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

Es war ein Zufall, daß wir dieses Ergebnis auch der GRÖBNER-Basis bezüglich der graduiert lexikographischen Ordnung ansehen konnten; bei komplizierteren Systemen wird dort oft jedes Basiselement alle Variablen enthalten, so daß wir nichts sehen können. Trotzdem kann die graduiert lexikographische Ordnung zur Lösung nichtlinearer Gleichungssysteme nützlich sein: 1993 publizierten J.C. FAUGÈRE, P. GIANNI, D. LAZARD und T. MORA einen heute nach ihren Anfangsbuchstaben

als FGLM benannten Algorithmus, der für ein Ideal I mit endlicher Nullstellenmenge $V(I)$ effizient eine GRÖBNER-Basis bezüglich der lexikographischen Ordnung bestimmt auf dem Umweg über die graduiert lexikographische Ordnung. Wir werden später sehen, daß wir im Falle einer endlichen Lösungsmenge diese auch ausgehend von einer beliebigen GRÖBNER-Basis mit alternativen Techniken bestimmen können.

Nun kann es beim obigen Verfahren für nichtlineare Gleichungssysteme 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 eines hyperbolischen und eines elliptischen Zylinders. 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.

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

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.

Fast genauso können wir auch zu einer vorgegebenen endlichen Menge von Punkten ein Gleichungssystem konstruieren, das genau diese Menge als Lösungsmenge hat; dies spielt beispielsweise in der algebraischen Statistik eine Rolle, wenn zu einem vorgegebenen Design die damit schätzbaren Modelle identifiziert werden sollen.

Wir gehen aus von r Punkten

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

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

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

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

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

so erzeugen die Polynome

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

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

Ist umgekehrt $Q = (t_1, \ldots, t_r, x_1, \ldots, x_n) \in k^{r+n}$ 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 X_j-Koordinate, so ist $X_j - x_j^{(i)}$ in Q in Q von Null verschieden; $\left(X_j - x_j^{(i)}\right) T_i$ kann daher nur verschwinden, wenn $t_i = 0$ ist. Dies kann aber nicht für alle i der Fall sein, denn die Summe der t_i ist eins, da $T_1 + \cdots + T_r - 1$ verschwindet. Somit liegt Q nicht in $V(J)$.

Damit haben wir ein Ideal $J \lhd k[T_1, \ldots, T_r, X_1, \ldots, X_n]$ gefunden, dessen Nullstellen genau die Punkte $Q_1, \ldots, Q_r \in k^{r+n}$ 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. Wir erhalten ein Erzeugendensystem dieses Ideals, indem wir bezüglich einer Eliminationsordnung für $T_1, \ldots, T_r$ eine GRÖBNER-Basis von J berechnen und davon nur die Polynome betrachten, die keine der Variablen T_i enthalten.

§2: Der Hilbertsche Nullstellensatz

Wie wir wissen, stimmen die Lösungsmengen zweier Gleichungssysteme

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

und

$$g_1(x_1, \ldots, x_n) = \cdots = g_p(x_1, \ldots, x_n) = 0$$

überein, wenn die Ideale $(f_1, \ldots, f_m)$ und $(g_1, \ldots, g_p)$ übereinstimmen. Umgekehrt folgt aber nicht aus der Gleichheit der Lösungsmengen, daß auch die Ideale gleich sein müssen. In diesem Paragraphen wollen wir genauer untersuchen, was hier gilt.

Dazu betrachten wir als erstes den Fall von Polynomen in nur einer Veränderlichen X. Hier können wir uns mit einer einzigen Gleichung begnügen, denn es gilt

Lemma: Der Polynomring $R = k[X]$ über einem Körper k ist ein Hauptidealring.

Beweis: Wir müssen zeigen, daß jedes Ideal I von R ein Hauptideal ist, also von einem einzigen Polynom f erzeugt werden kann. Sei also I ein beliebiges Ideal in R. Falls I nur aus der Null besteht, ist es das von der Null erzeugte Hauptideal, andernfalls wählen wir ein Polynom f minimalen Grades aus I und wollen zeigen, daß $I = (f)$ ist. Dazu sei g ein beliebiges Polynom aus I. Wir dividieren es durch f:

$$g : f = q \text{ Rest } r \quad \text{oder} \quad g = qf + r\,,$$

wobei entweder $r = 0$ ist oder $\deg r < \deg f$. Da mit f und g auch $r = g - qf$ in I liegt, kann letzteres nicht sein: Nach Konstruktion enthält I kein Polynom vom Grad kleiner $\deg f$. Also ist $r = 0$ und $g = qf$ liegt in (f).

■

Sind also I und J zwei Ideale in $k[X]$, so gibt es Polynome $f, g \in k[X]$, für die $I = (f)$ und $J = (g)$ ist. Da für jedes $c \in k \setminus \{0\}$ die Polynome f und cf dasselbe Ideal erzeugen, können wir dabei annehmen, daß sowohl f als auch g den führenden Koeffizienten eins haben. Dann ist $I = J$ genau dann, wenn $f = g$ ist.

Um zu sehen, was es bedeutet, daß $V_K(I) = V_K(J)$ ist, betrachten wir zunächst den Fall, daß $k = K = \mathbb{Q}$ ist. Offensichtlich ist dann

$$V_{\mathbb{Q}}(X^2 - 2) = V_{\mathbb{Q}}(X^2 - 3) = V_{\mathbb{Q}}(X^2 + 1) = V_{\mathbb{Q}}(X^2 + 5) = \emptyset\,,$$

ohne daß irgendwelche zwei der betrachteten Polynome gleich wären. Es ist dabei unerheblich, daß die Nullstellenmengen jeweils leer sind: Hätten wir jedes der vier betrachteten Polynome noch mit $X - 1$ multipliziert, hätten wir vier neue Polynome erhalten, die allesamt die Eins als einzige rationale Nullstelle haben und trotzdem verschieden sind. Über einem hinreichend großen Körper, etwa dem der kompklexen Zahlen, haben freilich alle betrachteten Polynome verschiedene Nullstellenmengen.

Aber auch über $\mathbb{C}$ gilt nicht, daß aus $V_{\mathbb{C}}(f) = V_{\mathbb{C}}(g)$ die Gleichheit der Ideale (f) und (g) folgt: Beispielsweise ist

$$V_{\mathbb{C}}\big(X(X-1)^2\big) = V_{\mathbb{C}}\big(X^2(X-1)\big) = \{0, 1\}\,,$$

aber keines der beiden Polynome liegt auch nur im vom anderen erzeugten Ideal. Allgemein ist offenbar für r komplexe Zahlen $z_1, \ldots, z_r$ und r natürliche Zahlen $e_1, \ldots, e_r$ stets

$$V_{\mathbb{C}}\Big((X - z_1)^{e_1} \cdots (X - z_r)^{e^r}\Big) = V_{\mathbb{C}}\big((X - z_1) \cdots (X - z_r)\big)\,,$$

und sofern nicht alle $e_i = 1$ sind, erzeugen die beiden Polynome verschiedene Ideale.

Nach dem sogenannten *Fundamentalsatz der Algebra* hat jedes nichtkonstante Polynom f mit komplexen Koeffizienten mindestens eine komplexe Nullstelle. Da der Körper der komplexen Zahlen überabzählbar und damit für praktische Rechnungen zu groß ist, betrachten wir auch kleinere Körper mit einer entsprechenden Eigenschaft und definieren allgemein:

Definition: Ein Körper K heißt *algebraisch abgeschlossen,* wenn jedes nichtkonstante Polynom $f \in K[X]$ mindestens eine Nullstelle in K hat.

Durch Polynomdivision folgt leicht induktiv:

Lemma: Ist K algebraisch abgeschlossen, so läßt sich jedes Polynom vom Grad d aus $K[X]$ schreiben als

$$f = c(X - x_1) \cdots (X - x_d) \quad \text{mit} \quad c \in K \setminus \{0\} \text{ und } x_1, \ldots, x_d \in K\,.$$

Die x_i müssen dabei nicht notwendigerweise verschieden sein. ∎

Im folgenden betrachten wir Polynome über einem beliebigen Körper k; in den Beispielen wird das fast immer der Körper $\mathbb{Q}$ sein. Zusätzlich betrachten wir einen Körper K, der k enthält. Im Falle von $\mathbb{Q}$ kann man zeigen, daß es einen abzählbaren algebraisch abgeschlossenen Körper $\overline{\mathbb{Q}} \subset \mathbb{C}$ gibt, der $\mathbb{Q}$ enthält; er besteht aus allen *algebraischen* Zahlen, d.h. allen komplexen Zahlen z, für die es ein Polynom $0 \neq f \in \mathbb{Q}[X]$ gibt mit $f(z) = 0$.

Um die Beweise der folgenden Sätze etwas zu vereinfachen, wollen wir dort zusätzlich annehmen, daß der Körper K überabzählbar viele Elemente enthält. Dies ist aber nicht notwendig; mit etwas größerem Aufwand lassen sich die Beweise so führen, daß sie auch für abzählbare algebraisch abgeschlossene Körper gelten.

Sei also für den Rest dieses Paragraphen k irgendein Körper, und K sei ein algebraisch abgeschlossener Körper mit überabzählbar vielen Elementen, der k enthält.

Als erstes wollen wir uns mit der Frage beschäftigen, für welche Ideale $I \lhd k[X_1, \ldots, X_n]$ die Lösungsmenge $V_K(I)$ in K^n leer ist. Ein Beispiel ist offensichtlich: Natürlich ist $I = k[X_1, \ldots, X_n]$ ein Ideal, und da es insbesondere die Konstante eins enthält, ist $V_K(I) = \emptyset$. Eine (schwache) Form des HILBERTschen Nullstellensatzes besagt, daß dies das einzige Beispiel ist. Zur Vorbereitung des Beweises definieren wir

Definition: R sei ein Ring.
a) $I \lhd R$ ist ein *echtes* Ideal, falls $I \neq R$.
b) Ein echtes Ideal $\mathfrak{m} \lhd R$ heißt *maximales* Ideal, wenn R das einzige Ideal ist, das $\mathfrak{m}$ als echte Teilmenge enthält.
c) Ein echtes Ideal $\mathfrak{p} \lhd R$ heißt *Primideal,* wenn gilt: Liegt für zwei Elemente $f, g \in R$ das Produkt fg in $\mathfrak{p}$, so liegt mindestens einer der Faktoren f, g in $\mathfrak{p}$.

Wie aus der Zahlentheorie bekannt, teilt eine Primzahl p genau dann das Produkt zweier Zahlen a, b, wenn sie mindestens einen der beiden Faktoren teilt; in $\mathbb{Z}$ sind also die von den Primzahlen erzeugten Hauptideale Primideale. Dazu kommt wegen der Nullteilerfreiheit auch noch das Nullideal.

Durch vollständige Induktion beweist man leicht

Lemma: Ist $\mathfrak{p}$ ein Primideal und liegt ein Produkt $f_1 \cdots f_n$ von Elementen $f_i \in R$ in $\mathfrak{p}$, so liegt mindestens einer der Faktoren f_i in $\mathfrak{p}$. ∎

Lemma: Jedes maximale Ideal $\mathfrak{m} \lhd R$ ist ein Primideal.

Beweis: Das Produkt fg zweier Elemente $f, g \in R$ liege in $\mathfrak{m}$. Falls $f \in \mathfrak{m}$ sind wir fertig; andernfalls ist $\mathfrak{m}+(f) = R$ wegen der Maximalität von $\mathfrak{m}$. Es gibt daher Elemente $m \in \mathfrak{m}$ und $h \in R$, so daß $m + hf = 1$ ist. Damit ist $g = mg + hfg \in \mathfrak{m}$, denn $m \in \mathfrak{m}$ und $fg \in \mathfrak{m}$. ∎

Lemma: Jedes echte Ideal $I \lhd k[X_1, \ldots, X_n]$ liegt in einem maximalen Ideal $\mathfrak{m} \lhd k[X_1, \ldots, X_n]$.

Beweis: Falls I selbst maximal ist, sind wir fertig; andernfalls gibt es ein echtes Ideal I_1, das I als echte Teilmenge enthält. Auch wenn I_1 ein maximales Ideal ist, sind wir fertig; andernfalls gibt es ein echtes Ideal I_2, das I_1 als echte Teilmenge enthält, und so weiter. Wenn dieses Verfahren nach endlich vielen Schritten abbricht, haben wir ein maximales Ideal gefunden, das I enthält. Andernfalls gibt es eine unendliche aufsteigende Folge von Idealen $I \subset I_1 \subset I_2 \subset \cdots$. Die Vereinigung aller I_j ist selbst ein Ideal in $k[X_1, \ldots, X_n]$ und hat damit nach dem HILBERTschen Basissatz ein endliches Erzeugendensystem $\{f_1, \ldots, f_m\}$. Jedes f_i liegt in einem der Ideale I_j und damit auch in allen I_ℓ mit $\ell > j$. Wegen der Endlichkeit des Erzeugendensystems gibt es daher einen Index r derart, daß alle f_i in I_r liegen. Dann ist aber $I = I_r = I_{r+1} = \cdots$, im Widerspruch zu der Annahme, daß jedes I_j echte Teilmenge von I_{j+1} ist. Somit bricht das Verfahren nach endlich vielen Schritten ab und liefert ein maximales Ideal $\mathfrak{m}$, in dem I enthalten ist. ∎

(Tatsächlich gilt auch dieses Lemma für beliebige Ringe; da dort der HILBERTsche Basissatz nicht gelten muß, beweist man es im allgemeinen Fall mit Hilfe des ZORNschen Lemmas.)

Für ein Ideal I eines Rings R können wir eine Äquivalenzrelation $\sim$ auf R definieren durch

$$f \sim g \Longleftrightarrow f - g \in I \,.$$

Die Menge der Äquivalenzhlassen bezeichnen wir als den *Faktorring* R/I, und die Äquivalenzklasse eines Elements $f \in R$ mit $f + I$. Man überlegt sich leicht, daß R/I wirklich ein Ring ist, daß also insbesondere im Fall $f+I = f'+I$ und $g+I = g'+I$ auch $(f+g)+I = (f'+g')+I$ ist und $fg + I = f'g' + I$.

Speziell für $R = k[X_1, \ldots, X_n]$ ist R auch ein k-Vektorraum, und auch jedes Ideal $I \lhd R$ ist ein solcher. In diesem Fall ist R/I als Vektorraum einfach der Faktorraum dieser beiden Vektorräume. Wir können dann also insbesondere auch von der k-Dimension $\dim_k R/I$ reden. Diese wird im folgenden häufiger eine Rolle spielen.

Ist etwa $R = k[X]$ und $I = (f)$ für ein Polynom f vom Grad $d > 0$, so ist X^d modulo f äquivalent zu einem Polynom vom Grad höchstens $d - 1$ in X, so daß die Restklassen der Eins und der Potenzen X^e mit $1 \leq e < d$ eine k-Vektorraumbasis von R/I bilden. Somit ist hier $\dim_k R/I = d$.

Für ein Ideal I des Polynomrings $R = k[X_1, \ldots, X_n]$ definieren die Elemente von R/I als Funktionen $V_K(I) \to K$, die jedem Punkt $(x_1, \ldots, x_n) \in V_K(I)$ das Körperelement $f(x_1, \ldots, x_n) \in K$ zuordnen, wobei f irgendein Element der Restklasse ist. Ist nämlich g ein anderes Element derselben Restklasse, so liegt $f - g$ in I, verschwindet also auf allen Elementen von $V_K(I)$, so daß die Werte von f und von g dort übereinstimmen. Da das Ideal I durch $V_K(I)$ nicht eindeutig bestimmt ist, wissen wir allerdings noch nicht, unter welchen Bedingungen wir wir R/I mit dem Ring aller (mengentheoretischer) Abbildungen $V_K(I) \to I$ identifizieren können. Einen ersten Schritt in diese Richtung geben die folgenden Sätze, die HILBERT in seiner 1893 erschienenen Arbeit *Ueber die vollen Invariantensysteme* (Mathematische Annalen **36**, S. 313–373) veröffentlicht hat, und die auch für viele andere Fragen

fundamental sind. Sie alle werden unter dem Namen *Hilbertscher Nullstellensatz* zusammengefaßt; eine erste Version ist die folgende:

Schwache Form des Hilbertschen Nullstellensatzes: Für ein echtes Ideal $I \lhd k[X_1, \ldots, X_n]$ ist $V_K(I) \neq \emptyset$.

Beweis: Nach dem HILBERTschen Basissatz hat jedes Ideal I ein endliches Erzeugendensystem $\{f_1, \ldots, f_m\}$. Wir betrachten das von den f_i erzeugte Ideal $\bar{I}$ in $K[X_1, \ldots, X_n]$. Da eine Basis des k-Vektorraums $k[X_1, \ldots, X_n]/I$ auch Basis des K-Vektorraums $K[X_1, \ldots, X_n]/\bar{I}$ ist, muß auch $\bar{I}$ ein echtes Ideal von $K[X_1, \ldots, X_n]$ sein und liegt somit in einem maximalen Ideal $\mathfrak{m} \lhd K[X_1, \ldots, K_n]$. Der Satz folgt daher aus der folgenden alternativen Version des HILBERTschen Nullstellensatzes:

Satz: Die maximalen Ideale $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ sind genau die Ideale

$$\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n) \quad \text{mit} \quad (x_1, \ldots, x_n) \in K^n \, .$$

Beweis: $\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n)$ ist der Kern der Abbildung

$$\begin{cases} K[X_1, \ldots, X_n] \to K \\ \qquad\qquad f \mapsto f(x_1, \ldots, x_n) \end{cases} .$$

Ist daher I ein Ideal, das $\mathfrak{m}$ echt enthält, so muß der Vektorraum $K[X_1, \ldots, X_n]/I$ ein echter Untervektorraum von $K[X_1, \ldots, X_n]/\mathfrak{m}$ sein. Da letzterer nach dem Homomorphiesatz isomorph zum eindimensionalen Vektorraum K ist, muß dies der Nullraum sein. Somit ist $I = K[X_1, \ldots, X_m]$, d.h. $\mathfrak{m}$ ist ein maximales Ideal.

Umgekehrt sei $\mathfrak{m}$ ein maximales Ideal. Wenn wir zeigen können, daß es Elemente $x_1, \ldots, x_n$ gibt, für die $X_i - x_i$ in $\mathfrak{m}$ liegt, ist $(X_1 - x_1, \ldots, X_n - x_n) \subseteq \mathfrak{m}$, und da links ein maximales Ideal steht, müssen beide Seiten gleich sein.

Angenommen, es gibt ein $i \in \{1, \ldots, n\}$, für das $X_i - x$ für kein $x \in K$ im Ideal $\mathfrak{m}$ liegt. Wegen der Maximalität von $\mathfrak{m}$ ist dann

$$\mathfrak{m} + (X_i - x) = K[X_1, \ldots, X_n] \quad \text{für alle } x \in K \, .$$

Somit gibt es für jedes $x \in K$ ein Polynom $f_x \in \mathfrak{m}$ sowie ein Polynom $h_x \in K[X_1, \ldots, X_n]$ derart, daß $f_x + h_x \cdot (X_i - x) = 1$ ist. Da 1 nicht

in $\mathfrak{m}$ liegt, ist $h_x \neq 0$. Wir wählen für jedes $x \in K$ ein festes Polynom h_x (und damit auch f_x), das obige Gleichung erfüllt, und setzen $K_d = \{x \in K \,|\, \deg h_x = d\}$ für jedes $d \in \mathbb{N}_0$. Da K nach Voraussetzung überabzählbar viele Elemente enthält und K die Vereinigung der K_d ist, muß mindestens eine der Mengen K_d unendlich viele Elemente enthalten. (Nur an dieser Stelle geht die Voraussetzung der Überabzählbarkeit ein, und wie bereits erwähnt, gibt es alternative Beweise, die ohne diese Voraussetzung auskommen.)

Wir wählen eine solche Menge K_d und betrachten den Vektorraum $K[X_1, \ldots, K_n]_d$ aller Polynome vom Grad höchstens d. Da es nur endlich viele Monome vom Grad höchstens d gibt, ist dies ein endlichdimensionaler K-Vektorraum. Wir wählen eine natürliche Zahl r, die größer ist als seine Dimension, und dazu r Elemente $x^{(1)}, \ldots, x^{(r)} \in K$ mit $h_{x^{(i)}} \in k[X_1, \ldots, X_n]_d$. Zwischen diesen Polynomen muß dann eine kineare Abhängigkeit bestehen. Es gibt daher Elemente $\lambda_1, \ldots, \lambda_r \in K$, die nicht allesamt verschwinden, so daß

$$\lambda_1 h_{x^{(1)}} + \cdots + \lambda_r h_{x^{(r)}} = 0$$

ist. Dazu definieren wir

$$g = \sum_{j=1}^{r} \lambda_j \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) \in K[X_i]\,.$$

Dieses Polynom liegt auch in $\mathfrak{m}$, denn wegen

$$1 = f_{x^{(j)}} + h_{x^{(j)}} \left(X_i - x^{(j)}\right) \quad \text{für } j = 1, \ldots, r$$

ist

$$\begin{aligned} g &= \sum_{j=1}^{r} \lambda_j \left(f_{x^{(j)}} + h_{x^{(j)}} \left(X_i - x^{(j)}\right)\right) \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) \in K[X_i] \\ &= \sum_{j=1}^{r} \lambda_j f_{x^{(j)}} \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) + \left(\sum_{j=1}^{r} \lambda_j h_{x^{(j)}}\right) \prod_{\ell=1}^{n} \left(X_i - x^{(\ell)}\right) \\ &= \sum_{j=1}^{r} \lambda_j \prod_{\ell \neq j} \left(X_i - x^{(\ell)}\right) f_{x^{(j)}} \in \mathfrak{m}\,, \end{aligned}$$

da $\sum_{j=1}^{r} \lambda_j h_{x^{(j)}}$ verschwindet und alle $f_{x^{(j)}}$ in $\mathfrak{m}$ liegen.

g ist nicht das Nullpolynom, denn für jeden Index ν ist

$$g\big(x^{(\nu)}\big) = \sum_{j=1}^{r} \lambda_j \prod_{\ell \neq j} \big(x^{(\nu)} - x^{(\ell)}\big) = \lambda_\nu \prod_{\ell \neq \nu} \big(x^{(\nu)} - x^{(\ell)}\big) \,.$$

Da die $x^{(\ell)}$ paarweise verschieden sind und mindestens ein λ_ν nicht verschwindet, muß mindestens einer dieser Werte von Null verschieden sein.

Da g in $\mathfrak{m}$ liegt, kann g auch keine von Null verschiedene Konstante sein, hat also einen positiven Grad e. Über dem algebraisch abgeschlossenen Körper K zerfällt g daher in Linearfaktoren:

$$g = c\,(X_i - z_1)\ldots(X_i - z_e) \quad \text{mit} \quad c \in K \smallsetminus \{0\},\ z_1, \ldots z_e \in K \,.$$

g liegt in $\mathfrak{m}$, aber nach Voraussetzung liegt keiner der Faktoren $X_i - z_j$ in $\mathfrak{m}$, und die Konstante $c \neq 0$ natürlich auch nicht. Dies ist ein Widerspruch, denn als maximales Ideal ist $\mathfrak{m}$ insbesondere ein Primideal. ∎

Somit hat also jedes echte Ideal $I \lhd k[X_1, \ldots, X_n]$ zumindest in einem Erweiterungskörper K von k mindestens eine Nullstelle. Damit folgt umgekehrt

Satz: Das Gleichungssystem

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

mit $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ ist genau dann in jedem Erweiterungskörper K von k unlösbar, wenn es Polynome $h_1, \ldots, h_m$ in $X_1, \ldots, X_n$ gibt, so daß $h_1 f_1 + \cdots + h_m f_m = 1$ ist.

Beweis: Im Falle der Unlösbarkeit ist das von $f_1, \ldots, f_m$ erzeugte Ideal der ganze Polynomring, enthält also insbesondere die Eins. Da

$$(f_1, \ldots, f_m) = \big\{ h_1 f_1 + \cdots + h_m f_m \;\big|\; h_1, \ldots, h_m \in k[X_1, \ldots, X_n] \big\} \,,$$

hat auch die Eins eine Darstellung der verlangten Form.

Ist umgekehrt $h_1 f_1 + \cdots + h_m f_m = 1$ für irgendwelche Polynome $h_1, \ldots, h_m$, so ist für jeden Erweiterungskörper K von k und jedes n-Tupel $(x_1, \ldots, x_n) \in K^n$

$$h_1(x_1, \ldots, x_n) f_1(x_1, \ldots, x_n) + \cdots + h_m(x_1, \ldots, x_n) f_m(x_1, \ldots, x_n) = 1 \,,$$

so daß nicht alle $f_j(x_1, \ldots, x_n)$ verschwinden können.

■

Wenn wir eine GRÖBNER-Basis eines Ideals I kennen, ist es einfach zu entscheiden, ob $I = k[X_1, \ldots, X_n]$ ist (oder äquivalent, ob $1 \in I$): Da der führende Term eines jeden Polynoms aus I 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.

Aus dem gerade bewiesenen Satz folgt mit einem 1929 von J.L. RABINOWITSCH gefundenen Trick die von HILBERT 1893 ab Seite 320 unten der zitierten Arbeit bereits anders bewiesene

Starke Form des Hilbertschen Nullstellensatzes: k sei ein beliebiger Körper und K ein überabzählbarer algebraisch abgeschlossener Erweiterungskörper von k. Falls für ein Ideal $I \lhd k[X_1, \ldots, X_n]$ ein Polynom $f \in k[X_1, \ldots, X_n]$ auf ganz $V_K(I)$ verschwindet, gibt es ein $q \in \mathbb{N}$, so daß f^q in I liegt.

Beweis: Wir erweitern den Polynomring $k[X_1, \ldots, X_n]$ mit einer neuen Variablen X_{n+1} zu $k[X_1, \ldots, X_{n+1}]$ und betrachten dort für ein Erzeugendensystem $\{f_1, \ldots, f_m\}$ von I das Gleichungssystem

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 1 - x_{n+1} f(x_1, \ldots, x_n) = 0 \,.$$

Für jeden Punkt $(x_1, \ldots, x_n, x_{n+1}) \in K^{n+1}$, für den die $f_j(x_1, \ldots, x_n)$ verschwinden, verschwindet auch $f(x_1, \ldots, x_n)$, d.h.

$$1 - x_{n+1} f(x_1, \ldots, x_n) = 1 \,.$$

Somit haben diese $n+1$ Gleichungen keine gemeinsame Nullstelle; es gibt also Polynome $h_1, \ldots, h_{m+1} \in k[X_1, \ldots, X_{n+1}]$ derart, daß

$$h_1 f_1 + \cdots + h_m f_m + h_{m+1}(1 - X_{n+1} f) = 1$$

ist. Diese Gleichung bleibt gültig, wenn wir überall für X_{n+1} ein Polynom oder eine rationale Funktion in $X_1, \ldots, X_n$ einsetzen; wir setzen $X_{n+1} = 1/f$. Die h_j werden dann zu rationalen Funktionen in $X_1, \ldots, X_n$, wobei alle Nenner Potenzen von f sind. Ist f^q die höchste dieser Potenzen, so erhalten wir nach Multiplikation mit f^q eine Gleichung der Form

$$\widetilde{h}_1 f_1 + \cdots + \widetilde{h}_m f_m = f^q$$

mit $\widetilde{h}_j = f^q h_j\big(X_1, \ldots, X_n, 1/f\big) \in k[X_1, \ldots, X_n]$. Dies zeigt, daß f^q in $I = (f_1, \ldots, f_m)$ liegt.

■

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

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

Ist $I = \sqrt{I}$, so bezeichnen wir I als ein *Radikalideal.*

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 $f^p \in I$ und $g^q \in I$, so sind in

$$(f+g)^{p+q} = \sum_{\ell=0}^{p+q} \binom{p+q}{\ell} f^{p+q-\ell} g^{\ell}$$

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

Mit diesem neuen Begriff können wir den obigen Satz umformulieren:

Satz: Ein Polynom $f \in k[X_1, \ldots, X_n]$ verschwindet genau dann auf $V_K(I)$, wenn $f \in \sqrt{I}$.

■

Anders ausgedrückt heißt dies

Satz: Für zwei Ideale $I, J \lhd k[X_1, \ldots, X_n]$ ist $V_K(I) = V_K(J)$ genau dann, wenn $\sqrt{I} = \sqrt{J}$ ist.
■

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. Im nächsten Paragraphen wollen wir uns überlegen, wie man ähnliche Ergebnisse auch für Systeme von Polynomgleichungen in mehreren Veränderlichen finden kann.

§3: Gleichungssysteme mit endlicher Lösungsmenge

Auch hier gehen wir wieder aus von einem beliebigen Körper k sowie einem algebraisch abgeschlossenen Erweiterungskörper K mit überabzählbar vielen Elementen. Letztere Bedingung ist nur notwendig, weil wir sie im Beweis des HILBERTschen Nullstellensatzes verwendet haben; wie bereits dort erwähnt, gibt es auch Beweise für den Fall, daß K ein beliebiger algebraisch abgeschlossener Körper ist, so daß alle Sätze dieses Paragraphen tatsächlich auch ohne die Voraussetzung der Überabzählbarkeit von K gelten.

Satz: I sei ein Ideal im Polynomring $k[X_1, \ldots, X_n]$ über dem Körper k, und K sei ein überabzählbarer algebraisch abgeschlossener Körper, in dem k enthalten sei. Dann gilt: $V_K(I)$ ist genau dann endlich, wenn der Faktorring $A = k[X_1, \ldots, X_n]/I$ 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 und somit in I liegt. Für jeden Punkt aus $V_K(I)$ muß daher 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: $\bar{I}$ sei das von I in $K[X_1, \ldots, X_n]$ erzeugte Ideal. 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 $\{b_1, \ldots, b_r\}$ und zu jedem Basiselement b_i ein Polynom $B_i \in k[X_1, \ldots, X_n]$, das modulo I gleich b_i ist. Zusammen mit einer Basis von I als k-Vektorraum bilden die B_i dann eine k-Vektorraumbasis von $k[X_1, \ldots, X_n]$. Über K wird die Basis von I zu einer K-Vektorraumbasis von $\bar{I}$, da sich jedes Element von $\bar{I}$ als eine K-Linearkombination von Elementen aus I schreiben läßt. Zusammen mit den B_i, die wir auch als Elemente von $K[X_1, \ldots, X_n]$ aufâãlfassen können, erhalten wir sowohl über k als auch über K eine Basis des ganzen jeweiligen Polynomrings, und damit ist klar, daß die Restklassen der B_i modulo $\bar{I}$ den Faktorring $\bar{A}$ erzeugen. Somit ist dieser als K-Vektorraum endlichdimensional.

Die Gleichheit von $\dim_k A$ und $\dim_K \bar{A}$ folgt, falls wir zeigen können, daß die Restklassen der B_i modulo $\bar{I}$ linear unabhängig sind.

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. $\lambda_1 B_1 + \cdots + \lambda_r B_r$ liegt daher in 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

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

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. Seine Lösungsmenge über k ist ein k-Vektorraum, für den uns der GAUSS-Algorithmus eine Basis liefert. Da der GAUSS-Algorithmus nirgends aus dem Körper hinausführt, in dem die Koeffizienten liegen, ist dies auch eine Basis des Lösungsraums über K; die beiden Vektorräume haben also dieselbe Dimension. Da wir wissen, daß es über K eine nichttriviale Lösung gibt, muß es daher auch über k eine geben.

Es gibt somit 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 über k, also ist A endlichdimensional.

Im nächsten Schritt wollen wir das Zählen der Lösungen zurückführen auf das Zählen von Nullstellen eines Polynoms einer Veränderlichen.

Definition: Ein Polynom $u \in K[X_1, \ldots, X_n]$ heißt *separierend,* wenn es für keine zwei Elemente von $V_K(I)$ denselben Wert annimmt.

4. Schritt: Falls $V_K(I)$ endlich ist, gibt es ein separierendes homogenes lineares Polynom $u = c_1X_1 + \cdots c_nX_n$. Wir können dabei für u eines der speziellen Polynome

$$u_a = X_1 + aX_2 + a^2X_3 + \cdots + a^{n-1}X_n$$

wählen, wobei a in einer beliebig vorgebbaren Teilmenge von K mit mehr als $(n-1)\binom{s}{2} = \frac{1}{2}s(s-1)(n-1)$ Elementen liegt.

Für je zwei verschiedene Punkte $z, w \in V_K(I)$ ist $u_a(z) = u_a(w)$ genau dann, wenn

$$(z_1 - w_1) + (z_2 - w_2)a + (z_3 - w_3)a^2 + \cdots + (z_n - w_n)a^{n-1}$$

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. Ist $s = \#V_K(I)$ endlich, so gibt es $\binom{s}{2}$ Paare aus voneinander verschiedenen Elementen; somit gibt es höchstens $(n-1)\binom{s}{2}$ Elemente $a \in K$, für die $u_a(z) = u_a(w)$ für *irgendwelche* voneinander verschiedene Elemente von $V_K(I)$.

(Hier haben wir benutzt, daß jeder algebraisch abgeschlossene Körper unendlich ist. Falls bereits k unendlich ist, etwa $k = \mathbb{Q}$, können wir sogar ein $a \in k$ finden 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. Im hier meistens betrachteten Fall $k = \mathbb{Q}$ können wir etwa eine ganze Zahl a mit $0 \leq a \leq (n-1)\binom{s}{2}$ wählen.

5. Schritt: Die Elementanzahl s 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 4. 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 $\bar{A}$ und wollen uns überlegen, daß die Elemente $1, \tilde{u}, \ldots, \tilde{u}^{s-1} \in \bar{A}$ linear unabhängig sind: Angenommen, es gibt eine Relation der Form $\sum_{\ell=0}^{s-1} \lambda_\ell \tilde{u}^\ell = 0$ mit $\lambda_\ell \in K$. Das Polynom $\sum_{\ell=0}^{s-1} \lambda_\ell u^\ell \in K[X_1, \ldots, X_n]$ liegt dann in $\bar{I}$, verschwindet also für jedes der s Elemente von $V_K(I)$. Da u für jedes dieser Elemente einen anderen Wert annimmt, hat das Polynom $\sum_{\ell=0}^{r-1} \lambda_\ell U^\ell \in k[U]$ einerseits mindestens s verschiedene Nullstellen in K, andererseits ist sein Grad kleiner als s. Das ist nur für das Nullpolynom möglich; somit verschwinden alle Koeffizienten λ_ℓ, was die behauptete lineare Unabhängigkeit beweist. Damit enthält $\bar{A}$ mindestens s linear unabhängige Elemente, d.h. $r = \dim_K \bar{A} \geq s = \#V_K(I)$. Damit ist die Behauptung und auch der gesamte Satz bewiesen.

∎

Betrachten wir als Beispiel das von $f = X^2 + Y^2 - 1$ und $g = X - Y$ erzeugte Ideal $I \lhd \mathbb{Q}[X, Y]$. Seine Lösungsmenge ist, geometrisch gesehen, der Schnitt des Einheitskreises mit der ersten Winkelhalbierenden, besteht also aus den beiden Punkten $\left(\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{2}\right)$ und $\left(-\frac{1}{2}\sqrt{2}, -\frac{1}{2}\sqrt{2}\right)$.

Der Polynomring $\mathbb{Q}[X, Y]$ hat als $\mathbb{Q}$-Vektorraum eine Basis bestehend aus allen Monomen $X^a Y^b$ mit $a, b \in \mathbb{N}_0$. Modulo I sind X und Y äquivalent, und damit ist $X^a Y^b \sim X^{a+b}$. Außerdem ist $2X^2$ äquivalent zu $X^2 + Y^2$, und das wiederum ist wegen f äquivalent zu 1, d.h. $X^2 \sim \frac{1}{2}$. Daher ist jedes Monom äquivalent entweder zu einer Konstanten (falls $a+b$ gerade) oder einem skalaren Vielfachen von X. Da I kein Polynom der Form $\lambda X + \mu$ enthält, sind X und 1 modulo I linear unabhängig; somit bilden ihre Restklassen eine Basis des Vektorraums $\mathbb{Q}[X, Y]/I$.

Ersetzen wir in diesem Beispiel g durch $X^2 - Y^2 = (X + Y)(X - Y)$, so schneiden wir den Kreis mit beiden Winkelhalbierenden und haben

nun eine vierelementige Lösungsmenge

$$V_{\mathbb{C}}(I) = \left\{ \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right), \left(\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right), \left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right), \left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right) \right\}.$$

Modulo dem neuen Ideal I sind X und Y nicht mehr äquivalent, sondern nur noch X^2 und Y^2. Jedes Monom ist somit äquivalent entweder zu einer X-Potenz oder zu einem Monom der Form $X^a Y$. Da auch hier $X^2 \sim \frac{1}{2}$, ist es somit äquivalent zu einem skalaren Vielfachen eines der Monome $1, X, Y$ oder XY. Da keine Linearkombination dieser vier Monome in I liegt, bilden ihre Restklassen eine Basis von $\mathbb{Q}[X, Y]/I$.

In diesen beiden Beispielen waren sowohl die Lösungsmengen als auch Basen der Faktorringe einfach zu finden; im Allgemeinen ist das eher nicht der Fall. Wenn wir eine GRÖBNER-Basis des Ideals I kennen, können wir leicht eine Vektorraumbasis des Faktorrings konstruieren:

Definition: $I \lhd k[X_1, \ldots, X_n]$ sei ein Ideal und G sei eine GRÖBNER-Basis bezüglich irgendeiner Monomordnung auf $k[X_1, \ldots, X_n]$. Ein Monom in $X_1, \ldots, X_n$ heißt *Standardmonom* (bezüglich G), wenn es für kein $g \in G$ durch das führende Monom von g teilbar ist.

(Tatsächlich sollte man von Standardmonomen bezüglich einer Monomordnung reden, denn eine Menge G kann durchaus GRÖBNER-Basis bezüglich zweier verschiedener Monomordnungen sein, und zumindest einige ihrer Elemente können bezüglich dieser Monomordnungen verschiedene führende Monome haben, so daß ein Standardmonom bezüglich der einen Monomordnung keines bezüglich der anderen sein muß.)

Satz: Für jede GRÖBNER-Basis G eines Ideals $I \lhd k[X_1, \ldots, X_n]$ bilden die Restklassen der Standardmonome eine Vektorraumbasis von $k[X_1, \ldots, X_n]/I$.

Beweis: Zunächst sind diese Restklassen linear unabhängig, denn jede nichttriviale Linearkombination der Null entspräche einem Polynom h aus I, dessen sämtliche Monome Standardmonome sind. Da die führenden Monome der Elemente von G das Ideal FM(I) erzeugen, müßte

daher FM(h) Vielfaches eines FM(g) mit $g \in G$ sein, was der Definition eines Standardmonoms widerspricht.

Für ein beliebiges $f \in k[X_1, \ldots, X_n]$ liefert uns der Divisionsalgorithmus eine Darstellung

$$f = \sum_{g \in G} a_g g + r \quad \text{mit} \quad a_g, r \in k[X_1, \ldots, X_n] \,,$$

wobei r eine k-Linearkombination von Standardmonomen ist. Da die Summe der $a_g g$ in I liegt, ist f also äquivalent zu einer k-Linearkombination von Standardmonomen, so daß seine Restklasse die entsprechende Linearkombination von deren Restklassen ist. ∎

Dieser Satz gilt unabhängig davon, ob $k[X_1, \ldots, X_n]/I$ als Vektorraum endlichdimensional ist; er liefert uns auch ein einfaches Kriterium dafür, wann er endliche Dimension hat und wann somit die Lösungsmenge $V_K(I)$ endlich ist:

Lemma: G sei eine GRÖBNER-Basis eines Ideals $I \lhd k[X_1, \ldots, X_n]$ bezüglich irgendeiner Monomordnung. $V_K(I)$ ist genau dann endlich, wenn G für jedes i ein Polynom enthält, dessen führendes Monom eine X_i-Potenz ist.

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 Standardmonome. 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. ∎

Für den Fall, daß $V_K(I)$ endlich ist, läßt der obige Satz noch wie folgt verschärfen:

Satz: Ist $D = V_K(I)$ endlich und τ eine Monomordnung, so gibt es zu jeder Funktion $\varphi\colon D \to K$ eine K-Linearkombination f von Standardmonomen bezüglich τ derart, daß $f(x) = \varphi(x)$ für alle $x \in D$. Insbesondere ist die Dimension von $k[X_1, \ldots, X_n]/I$ größer oder gleich der Elementanzahl von D. Die beiden Zahlen sind genau dann gleich, wenn I das Ideal $I(D)$ aller auf D verschwindender Polynome ist, was wiederum dazu äquivalent ist, daß I ein Radikalideal ist.

Beweis: Zunächst sollten wir uns überlegen, daß es überhaupt ein Polynom $\widetilde{f} \in K[X_1, \ldots, X_n]$ gibt mit $\widetilde{f}(x) = \varphi(x)$ für alle $x \in D$. Im Eindimensionalen können wir $\widetilde{f}$ nach LAGRANGE oder NEWTON als Interpolationspolynom konstruieren, und den allgemeinen Fall können wir wie folgt darauf zurückführen: Wie wir im vierten Schritt des Beweises in §3 gesehen haben, gibt es ein homogenes lineares Polynom $\ell \in k[X_1, \ldots, X_n]$, das auf den verschiedenen Punkten von D verschiedene Werte annimmt. Dazu betrachten wir das Interpolationspolynom aus $K[T]$, das für jeden Punkt $x \in D$ an der Stelle $t = \ell(x)$ den Wert $\varphi(x)$ annimmt. Setzen wir ℓ in dieses Polynom ein, erhalten wir ein Polynom $\widetilde{f}$ aus $k[X_1, \ldots, X_n]$, das für jedes $x \in D$ an der Stelle x den Wert $\varphi(x)$ annimmt. Da die Restklassen der Standardmonome eine Basis des Restklassenrings bilden, gibt es dazu eine Linearkombination f von Standardmonomen, die sich nur durch ein Polynom aus $\bar{I}$ von $\widetilde{f}$ unterscheidet, d.h. $f(x) = \widetilde{f}(x) = \varphi(x)$ für alle $x \in D$.

Die Funktionen $\phi\colon D \to K$ bilden offensichtlich einen K-Vektorraum, den wir für $D = \{x^{(1)}, \ldots, x^{(r)}$ identifizieren können mit dem Vektorraum aller Tupel $\big(\varphi(x^{(1)}, \ldots, x^{(r)})\big)$, also mit K^r. Die Dimension des Vektorraums aller dieser Funktionen ist somit gleich der Elementanzahl von D.

Diese Dimensionen ist genau dann gleich der Vektorraumdimension des Faktorrings, wenn die obige Linearkombination f durch φ eindeutig bestimmt ist. Sind f_1 und f_2 zwei verschiedene solche Linearkombinationen, so verschwindet $f_1 - f_2$ auf ganz D, liegt also im Ideal $I(D)$.

Genau dann, wenn dieses mit I übereinstimmt, können wir daraus folgern, daß $f_1 = f_2$ ist, und das ist nach dem HILBERTschen Nullstellensatz genau dann der Fall, wenn I ein Radikalideal ist.

■

In §1 haben wir gesehen, wie man zu jeder endlichen Teilmenge $D \subset k^n$ ein Ideal $I \lhd k[X_1, \ldots, X_n]$ finden kann, für das $D = V_K(I)$ ist. Mit dem gerade bewiesenen Satz können wir nun sehen, daß das dort konstruierte Ideal gleich $I(D)$ ist:

Für $D = \{x^{(1)}, \ldots, x^{(r)}\} \subset k^n$ mit $x^{(i)} = (x_1^{(i)}, \ldots, x_n^{(i)})$ hatten wir die Punkte

$$y^{(i)} = (0, \ldots, 0, 1, 0, \ldots, 0, x_1^{(i)}, \ldots, x_n^{(i)}) \in k^{r+n}$$

betrachtet, wobei die Eins bei $y^{(i)}$ an der i-ten Stelle steht; die Menge dieser Punkte sei $\widetilde{D}$. Wie wir gesehen hatten, ist $\widetilde{D}$ die Nullstellenmenge jenes Ideals $J \lhd k[T_1, \ldots, T_r, X_1, \ldots, X_n]$, das erzeugt wird von den Polynomen $f_{ij} = T_i(X_j - x_j^{(i)})$ und dem Polynom $g = T_1 + \cdots + T_r - 1$. Wir wollen uns als erstes überlegen, daß J das Ideal *aller* auf $\widetilde{D}$ verschwindenden Funktionen ist: Da $f_{ij} \in J$, ist jedes Monom $T_i X_j$ modulo J äquivalent zu einem skalaren Vielfachen von T_i. Induktiv folgt, daß für jedes nichtkonstante Monom M in den X_j das Monom $T_i M$ äquivalent ist zu einem skalaren Vielfachen von T_i. Da g in J liegt, ist M selbst äquivalent zu $T_1 M + T_2 M + \cdots + T_r M$ und damit zu einem linearen Polynom in den T_i. Somit ist jedes Polynom aus $k[T_1, \ldots, T_r, X_1, \ldots, X_n]$ äquivalent zu einem Polynom nur in den T_i.

Für zwei verschiedene Punkte $x^{(i)}$ und $x^{(\ell)}$ aus D gibt es mindestens einen Index j, für den $x_j^{(i)} \neq x_j^{(\ell)}$ ist. Mit f_{ij} und $f_{\ell j}$ enthält J auch das Polynom

$$T_\ell f_{ij} - T_i f_{\ell j} = T_\ell T_i X_j - T_\ell T_i x_j^{(i)} - T_i T_\ell X_j + T_i T_\ell x^{(\ell)} = T_i T_\ell \left(x_j^{(\ell)} - x_j^{(i)}\right)$$

und damit das Produkt $T_i T_\ell$, so daß jedes Monom, das zwei verschiedene T_i enthält, modulo J verschwindet. Außerdem liegt für jedes T_i auch das Polynom $T_i g = T_i T_1 + \cdots + T_i T_r - T_i$ in J, d.h. modulo J ist T_i äquivalent zu $T_i T_1 + \cdots + T_i T_r$. Da alle $T_i T_\ell$ mit $\ell \neq i$ in J liegen, ist T_i damit auch äquivalent zu T_i^2 und damit auch zu jeder höheren T_i-Potenz. Somit ist jedes Polynom äquivalent zu einem linearen Polynom

in den T_i, wobei wir dieses homogen wählen können, da 1 äquivalent ist zur Summe der T_i.

Dies zeigt, daß der Restklassenring modulo J als k-Vektorraum höchstens die Dimension r hat. Diese Dimension hat auch der Vektorraum aller Funktionen $\widetilde{D} \to K$. Damit folgt aus dem gerade bewiesenen Satz, daß J ein Radikalideal sein muß. Dann ist aber auch $I = J \cap k[X_1, \ldots, X_n]$ ein Radikalideal, d.h. $I = I(D)$.