Explizite Angabe der Lösungsmenge

Wir gehen weiterhin aus von einem Gleichungssystem

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

mit Polynomen $f_1, \ldots, f_m$ in n Variablen $X_1, \ldots, X_n$ über einem Körper k; dazu betrachten wir einen algebraisch abgeschlossenen Erweiterungskörper K (mit überabzählbar vielen Elementen). Wir betrachten das Ideal $I = (f_1, \ldots, f_m)$ in $k[X_1, \ldots, X_n]$ sowie das von den gleichen Polynomen in $K[X_1, \ldots, X_n]$ erzeugte Ideal $\bar{I}$. Wir wollen annehmen, daß $V_K(I)$ endlich ist. Wie wir in der letzten Vorlesung gesehen haben, ist das äquivalent dazu, daß der Faktorring $A = k[X_1, \ldots, X_n]/I$ als k-Vektorraum endlichdimensional ist, was wir leicht nachprüfen können, wenn wir eine GRÖBNER-Basis von I bezüglich *irgendeiner* Monomordnung berechnen: A ist genau dann endlichdimensional, wenn diese GRÖBNER-Basis für jede Variable X_i ein Element enthält, dessen führendes Monom eine Potenz von X_i ist. Leider führt diese GRÖBNER-Basis im Allgemeinen nicht zu einer expliziten Darstellung der Lösungsmenge.

Etwas besser sieht es aus, wenn wir die GRÖBNER-Basis bezüglich der lexikographischen Ordnung (mit irgendeiner Anordnung der Variablen) berechnet haben: Dann kann ein Polynom, dessen führendes Monom eine Potenz von X_i ist, kein Monom enthalten, in dem eine Variable vorkommt, die in der gewählten Anordnung vor X_i steht. Für ein Polynom, dessen führender Term eine Potenz der letzten Variablen ist, kann also keine andere Variable vorkommen, und wir haben ein Polynom in nur einer Veränderlichen.

Bei einem Basiselement, dessen führender Term eine Potenz der vorletzten Variable ist, kann entsprechend außer dieser Variablen nur noch die letzte vorkommen, und so weiter. Wenn wir mit der Anordnung $X_1 > X_2 > \cdots > X_n$ arbeiten, haben wir daher zu jedem i ein Polynom in der Basis, das nur die Variablen $X_i, \ldots, X_n$ enthält. Für $i = n$ haben wir also ein Polynom nur in X_n, für $i = n - 1$ eines in X_{n-1} und X_n, und so weiter. Die GRÖBNER-Basis enthält somit ein Gleichungssystem in Treppengestalt, und durch sukzessives Lösen

von Polynomgleichungen in einer Veränderlichen können wir, ähnlich wie beim GAUSS-Algorithmus, schrittweise die gesamte Lösungsmenge berechnen. Bei Polynomgleichungen höheren Grades kann freilich die Nullstellenbestimmung problematisch sein.

Am einfachsten wäre die Situation, wenn alle Polynome, die mehr als eine Variable enthalten, von der Form $X_i - g_i$ mit einem Polynom $g_i \in k[X_j]$ für eine in der Anordnung nach X_i kommende Variable X_j wären. In diesem Fall müßten wir nur eine Polynomgleichung höheren Grades lösen, die für die letzte Variable, und ansonsten könnten wir uns mit der Auswertung der Polynome g_i an bekannten Werten begnügen.

Definition: Eine GRÖBNER-Basis hat die Form gemäß des *Shape*-Lemmas, wenn sie genau ein Polynom in nur einer Variablen X enthält und jedes andere Basiselement von der Form $Y - g_Y(X)$ ist mit einer Variablen $Y \neq X$ und einem Polynom $g_Y \in k[X]$.

Wir wollen uns überlegen, wann wir so eine GRÖBNER-Basis bekommen können.

Wir gehen der Einfachheit halber wieder aus von der Standardanordnung $X_1 > X_2 > \cdots > X_n$. Wenn wir eine GRÖBNER-Basis der gewünschten Art haben, ist offensichtlich jeder Lösungspunkt $(x_1, \ldots, x_n) \in V_K(I)$ durch seine X_n-Koordinate eindeutig bestimmt; wenn das nicht der Fall ist, haben wir keine Chance. Die lineare Funktion X_n muß daher separierend für $V_K(I)$ sein im Sinne der Definition aus der letzten Vorlesung. Wie wir dort gesehen haben (Schritt 4 im Beweis des Satzes), gibt es stets eine separierende Linearform, und der Beweis zeigt auch, daß dies (einen unendlichen Grundkörper k vorausgesetzt) sogar für *fast alle* Linearformen gilt: Die Koeffizienten von denen, für die es nicht gilt, müssen Polynomgleichungen erfüllen und liegen daher in einer Menge niedrigerer Dimension. Daher haben wir durchaus Chancen, daß vielleicht eine der Variablen separierend ist – es sei denn, natürlich, das Koordinatensystem wäre speziell an die Lösungsmenge angepaßt. In diesem Fall würde uns aber eine zufällig gewählte lineare Koordinatentransformation mit großer Wahrscheinlichkeit mindestens eine separierende Koordinate liefern.

Nehmen wir also ein, die Variable X_n sei separierend. Da die Menge $V_K(I)$ endlich ist, gibt es auf jeden Fall ein Polynom $g \in K[X_n]$, das genau in den X_n-Koordinaten der Punkte aus $V_K(I)$ verschwindet. Fassen wir g auf als Polynom aus $K[X_1, \ldots, X_n]$, verschwindet g auf ganz $V_K(I) = V_K(\bar{I})$; nach der starken Form des HILBERTschen Nullstellensatzes muß eine Potenz von g in $\bar{I}$ liegen, und natürlich ist auch diese Potenz ein Polynom nur in X_n und hat genau die X_n-Koordinaten der Punkte aus $V_K(I)$ als Nullstellen.

Da wir die Variable X_n als separierend angenommen haben, sind die restlichen Komponenten der Lösungspunkte durch die X_n-Komponente eindeutig bestimmt. Da es nur endlich viele Lösungspunkte gibt, können wir daher für jedes $i < n - 1$ ein Interpolationspolynom $g_i \in K[X_n]$ finden, so daß für jedes $(x_1, \ldots, x_n) \in V_K(I)$ gilt: $x_i = g_i(x_n)$. Damit verschwindet auch das Polynom $X_i - g_i$ auf ganz $V_K(I)$. Leider folgt daraus nicht, daß $X_i - g_i$ in $\bar{I}$ liegt; der HILBERTsche Nullstellensatz garantiert uns wieder nur, daß eine Potenz von $X_i - g_i$ in $\bar{I}$ liegt, und die kann deutlich unangenehmer aussehen.

Wir müssen daher zusätzlich annehmen, daß das Ideal $I = (f_1, \ldots, f_m)$ sein eigenes Radikal ist, also ein sogenanntes Radikalideal. Damit haben wir alle notwendigen Voraussetzungen zusammen und können zeigen, daß wir eine GRÖBNER-Basis der gewünschten Form konstruieren können.

Satz: Ist I ein Radikalideal mit endlicher Lösungsmenge, und ist X_n separierend für $V_K(I)$, so gibt es Polynome $g_1, \ldots, g_n \in k[X_n]$ derart, daß

$$\{X_1 - g_1, \ldots, X_{n-1} - g_{n-1}, g_n\}$$

die reduzierte GRÖBNER-Basis von I ist bezüglich jeder lexikographischen Ordnung, die X_n an die letzte Stelle setzt.

Zum *Beweis* müssen wir uns nur überlegen, daß es eine reduzierte GRÖBNER-Basis dieser Gestalt gibt; da reduzierte GRÖBNER-Basen durch die Monomordnung eindeutig bestimmt sind, folgt dann die Behauptung. Wir überlegen uns zunächst, daß $\bar{I}$ eine GRÖBNER-Basis dieser Form hat mit $g_i \in K[X_n]$. Das Argument ist im wesentlichen das gleiche wie oben: $V_K(I)$ ist eine endliche Menge; sie

enthalte die r Elemente $(x_1^{(\nu)}, \ldots, x_n^{(\nu)})$ für $j = 1, \ldots, r$. Da X_n separierend ist, sind die $x_n^{(\nu)}$ paarweise verschieden; das Polynom $g_n = (X_n - x_n^{(1)}) \cdots (X_n - x_n^{(r)})$ hat also lauter verschiedene Nullstellen und verschwindet, wenn wir es als Polynom in $X_1, \ldots, X_n$ betrachten, auf $V_K(I)$. Da $\bar{I}$ ein Radikalideal ist, liegt g_n somit in $\bar{I}$.

Für $i < n$ ist die X_i-Koordinate eines Punktes aus $V_K(I)$ durch die X_n-Koordinate eindeutig bestimmt; wir können daher, beispielsweise nach LAGRANGE oder NEWTON, ein Interpolationspolynom $g_i \in K[X_n]$ vom Grad höchstens $r - 1$ für die r-Punkte $(x_n^{(\nu)}, x_i^{(\nu)})$ finden. Die Polynome

$$X_1 - g_1, X_2 - g_2, \ldots, X_{n-1} - g_{n-1}, g_n$$

haben die führenden Monome $X_1, X_2, \ldots, X_{n-1}$ und X_n^r, die offensichtlich alle teilerfremd zueinander sind. Damit lassen sich alle S-Polynome auf Null reduzieren, d.h. die angegebenen Polynome bilden nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis von $\bar{I}$ bilden.

Die Polynome $X_i - g_i$ für $i = 1, \ldots, n-1$ und g_n haben allesamt den führenden Koeffizienten eins. Da ihre führenden Monome sogar teilerfremd sind, ist insbesondere keines davon Teiler eines anderen, so daß diese GRÖBER-Basis minimal ist. Sie ist sogar reduziert, denn da die g_i für $i < n$ höchstens Grad $r - 1$ haben, ist keines ihrer Monome durch $\mathrm{FM}(g_n) = X^r$ teilbar. Damit haben wir also eine GRÖBNER-Basis der gewünschten Form für $\bar{I}$ gefunden. Nach allem was wir bisher wissen, können die Koeffizienten der Polynome allerdings beliebige Elemente von K sein.

Nun berechnen wir nach dem BUCHBERGER-Algorithmus, ausgehend von den Polynomen $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$, eine GRÖBNER-Basis von $\bar{I}$ in $k[X_1, \ldots, X_n]$ bezüglich der gleichen Monomordnung und machen daraus eine reduzierte GRÖBNER-Basis. Bei keinem der dabei durchgeführten Rechenschritte verlassen wir den Polynomring $k[X_1, \ldots, X_n]$, so daß auch alle Elemente der so berechneten reduzierten GRÖBNER-Basis dort liegen müssen. Wegen der Eindeutigkeit der reduzierten GRÖBNER-Basis bei gegebener Monomordnung muß das Ergebnis gleich dem obigen sein, die Polynome $X_i - g_i$ für $i < n$ und g_n liegen also in $k[X_1, \ldots, X_n]$, und insbesondere liegen

alle g_i in $k[X_n]$. Da die Bestimmung der reduzierten GRÖBNER-Basis für das von $f_1, \ldots, f_m$ erzeugte Ideal nach dem BUCHBERGER-Algorithmus in $k[X_1, \ldots, X_n]$ genauso verläuft wie in $K[X_1, \ldots, X_n]$, ist die angegebene GRÖBNER-Basis auch eine von I, womit der Satz vollständig bewiesen ist. ∎

Der gerade bewiesene Satz hat zwei Voraussetzungen, die dem Gleichungssystem schwer anzusehen sind: Einmal haben wir vorausgesetzt, daß die Variable X_n separierend ist, und dann auch noch, daß die gegebenen Polynome ein Radikalideal erzeugen.

Die erste Voraussetzung ist ganz offensichtlich nicht immer erfüllt. Wenn sie erfüllt ist und wir ein Radikalideal haben, sagt uns der Satz aber, daß die reduzierte GRÖBNER-Basis bezüglich einer lexikographischen Ordnung mit X_n an letzter Stelle dann eine Form gemäß dem *Shape*-Lemma hat, so daß wir im Nachhinein erkennen, ob X_n separierend ist oder nicht. Falls nein, können wir versuchen, die Rechnung mit einer lexikographischen Ordnung mit einer anderen Variablen an letzter Stelle zu wiederholen in der Hoffnung, damit mehr Erfolg zu haben. Leider ist es durchaus möglich, daß keine der n Variablen separierend ist.

Alternativ können wir einen Koordinatenwechsel durchführen. Im vierten Schritt des Beweises, daß $V_K(I)$ genau dann endlich ist, wenn $k[X_1, \ldots, X_n]/I$ als Vektorraum endliche Dimension hat, haben wir gesehen, daß es bei einer endlichen Lösungsmenge $V_K(I)$ höchstens $n - 1$ Elemente $a \in K$ gibt, für die

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

nicht separierend ist. Genauso folgt natürlich, daß es auch höchstens $n - 1$ Elemente $b \in K$ gibt, für die

$$Y = X_n + bX_{n-1} + b^2X_{n-2} + \cdots + b^{n-1}X_1$$

nicht separierend ist, und offensichtlich ist

$$k[X_1, \ldots, X_n] = k[X_1, \ldots, X_{n-1}, Y]\,,$$

denn

$$X_n = Y - bX_{n-1} - b^2X_{n-2} - \cdots - b^{n-1}X_1\,.$$

Wenn X_n nicht separierend ist, wenn also $b = 0$ einer der Ausnahmewerte sein sollte, ist daher die Chance sehr gut, daß ein anderes $b \in k$ auf ein separierendes Y führt, und spätestens beim n-ten Wert von b ist der Erfolg garantiert.

Die zweite Voraussetzung, daß $f_1, \ldots, f_m$ ein Radikalideal erzeugen müssen, wird auch nicht immer erfüllt sein; wie wir in der nächsten Vorlesung sehen werden, können wir aber ausgehend von $f_1, \ldots, f_m$ ein Erzeugendensystem von $\sqrt{I}$ berechnen und dann mit diesem arbeiten. Die Nullstellenmengen von I und $\sqrt{I}$ sind natürlich nach dem HILBERTschen Nullstellensatz identisch.