Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems

B. BUCHBERGER (Innsbruck, Austria)

1970

Sonderdruck aus
aequationes mathematicae
Vol. 4, Fasc. 3, 1970 BIRKHÄUSER VERLAG BASEL Seiten 374–383

Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems

B. BUCHBERGER (Innsbruck, Austria)

1. Problemstellung

Wir gehen vom Polynomring $K[x_1, \ldots, x_n]$ über einem kommutativen Körper K (abgekürzt $K[x_i]$) und einem beliebigen Polynomideal $\mathbf{a}=(f_1,\ldots,f_s)$ ($f_j \in K[x_i]$ für $j=1,\ldots,s$) aus. (Nicht ausdrücklich definierte Begriffe werden genau in dem Sinne verwendet, wie sie in [Gröbner 1] bzw. [Waerden] eingeführt werden.)

Der Restklassenring $\mathbf{o}=K[x_i]/\mathbf{a}$ ist bekanntlich eine (i.a. unendlich dimensionale) Algebra über K. Ist $\mathbf{a}$ nulldimensional, so ist $\mathbf{o}$ von endlicher Dimension über K und umgekehrt. Die Restklassen der Potenzprodukte (abgekürzt PP) $x_1^{i_1}\ldots x_n^{i_n}$ bilden eine (im Falle $\mathbf{a}\neq(0)$ linear abhängige) Basis der Algebra. (Da wir im Folgenden oft von der Basis eines Ideals und der Basis der zugehörigen Restklassenalgebra sprechen werden, vereinbaren wir zur Vermeidung von Zweideutigkeiten folgenden Sprachgebrauch: wir sagen einfach *Basis*, wenn wir die Basis der Restklassenalgebra meinen, andernfalls *Idealbasis*.)

Ziel der vorliegenden Untersuchung ist es, einen Algorithmus zu entwickeln, der bei gegebener Idealbasis $(f_1,\ldots,f_s)$ aus der Menge aller Restklassen von PP eine linear unabhängige Basis für $\mathbf{o}$ ausscheidet und für zwei beliebige Elemente dieser Basis eine Darstellung ihres Produktes als Linearkombination von Basiselementen zu berechnen gestattet (d.h. im endlich dimensionalen Fall die vollständige Multiplikationstafel liefert). Für nulldimensionale Ideale gab W. Gröbner einen derartigen Algorithmus an, von dem noch nicht entschieden war, wann er im konkreten Fall abgebrochen werden konnte ([Gröbner 3]). Bei der Untersuchung dieser letzten Frage ergab sich die Berechtigung des hier angegebenen Algorithmus, der auf beliebige Polynomideale angewendet werden kann. Nach Anwendung des Algorithmus ist eine Aussage über die Existenz einer Nullstelle für das Ideal sowie über die Dimension des Ideals möglich.

2. Beschreibung des Algorithmus

2.1. *Definitionen*

Für die Zwecke unserer Untersuchung ordnen wir die PP nach aufsteigendem Grad und innerhalb desselben Grades lexikographisch in dem Sinne, dass $x_1^{i_1}\ldots x_n^{i_n}$ vor $x_1^{i'_1}\ldots x_n^{i'_n}$ kommt, wenn $i_1>i'_1$ oder $i_t=i'_t$ (für $t=1,\ldots,k$ und $1\leqslant k<n$) und

Eingegangen am 27.3.1969, und in verbesserter Form am 11.8.1969.

$i_{k+1} > i'_{k+1}$. Den so geordneten PP ordnen wir, bei $x_1^0 \dots x_n^0$ beginnend, der Reihe nach die Zahlen 1, 2, 3, ... als die *Nummern der entsprechenden PP* zu. Das PP, das unter den in einem Polynom vorkommenden PP die grösste Nummer hat, nennen wir *GPP dieses Polynoms.*

Die Basispolynome des vorgegebenen Polynomideals $\mathbf{a}=(f_1,\dots,f_s)$ seien

$$f_j = x_1^{I_{j,1}} \dots x_n^{I_{j,n}} + \sum a_{i_1 \dots i_n}^{(j)} x_1^{i_1} \dots x_n^{i_n} \quad (j=1,\dots,s). \tag{1}$$

$pp_j = x_1^{I_{j,1}} \dots x_n^{I_{j,n}}$ sei dass GPP von f_j, die anderen Glieder von f_j sind in (1) unter dem Summenzeichen zusammengefasst. O.B.d.A. haben wir den Koeffizienten bei pp_j mit 1 angenommen. Wegen (1) gilt:

$$x_1^{I_{j,1}+v_1} \dots x_n^{I_{j,n}+v_n} \leftrightarrow - \sum a_{i_1 \dots i_n}^{(j)} x_1^{i_1+v_1} \dots x_n^{i_n+v_n} \tag{2}$$

($j=1,\dots,s$ und $v_t=0,1,2,\dots$ für $t=1,\dots,n$. „$\leftrightarrow$" sei das Symbol für *kongruent modulo* **a**).

Ein PP $x_1^{i_1} \dots x_n^{i_n}$ heisse *Vielfaches* des PP $x_1^{k_1} \dots x_n^{k_n}$, wenn $i_t \geqslant k_t$ für $t=1,\dots,n$. PP, die Vielfaches wenigstens eines pp_j ($j=1,\dots,s$), d.h. wenigstens einmal auf der linken Seite von (2) vorkommen, werden wir *MPP in bezug auf die Idealbasis* $(f_1,\dots,f_s)$ nennen. Andernfalls soll ein PP *NPP in bezug auf die Idealbasis* $(f_1,\dots,f_s)$ heissen. Wenn keine Zweideutigkeit möglich ist, werden wir den Zusatz „in bezug auf die Idealbasis $(f_1,\dots,f_s)$" weglassen. Polynome, in denen nur NPP vorkommen und Glieder, die dasselbe PP enthalten, zusammengefasst sind, wollen wir *NPP-Polynome* (in bezug auf die Idealbasis $(f_1,\dots,f_s)$) nennen.

Ein vorgegebenes Polynom (von dem wir nicht voraussetzen wollen, dass Glieder, die das gleiche PP enthalten, zusammengefasst sind) kann durch sukzessives Ersetzen aller vorkommenden MPP durch die entsprechenden rechten Seiten von (2) und durch Zusammenfassen gleicher Glieder in beliebigen Stadien dieses Reduktionsvorganges (den wir *M-Reduktion* nennen) stets in ein, i.a. nicht eindeutig bestimmtes, kongruentes NPP-Polynom übergeführt werden. Es bilden also bereits die Restklassen der NPP eine i.a. jedoch noch linear abhängige Basis für **o**.

2.2. *Hilfssatz*

Es gilt nun der folgende

HILFSSATZ. *Hat eine Idealbasis $(f_1,\dots,f_s)$ die Eigenschaft, dass alle möglichen M-Reduktionen eines Polynoms zu demselben Resultat führen, so bilden die Restklassen der NPP in bezug auf diese Idealbasis eine linear unabhängige Basis für* **o**.

Beweis. Einer linearen Abhängigkeit zwischen Restklassen von NPP würde ein NPP-Polynom q in **a** entsprechen, das eine Darstellung

$$q \equiv \sum_{j=1}^{s} h_j \cdot f_j \quad \text{mit} \quad h_j \in K[x_i] \quad \text{für} \quad j=1,\dots,s \tag{3}$$

besässe. Ausmultiplizieren der $h_j \cdot f_j$ $(j=1,\ldots,s)$ ohne Zusammenfassen von Gliedern, die Gleiche PP enthalten, liefert auf der rechten Seite von (3) ein Polynom, das im Widerspruch zur Voraussetzung des Hilfssatzes einerseits durch eben dieses Zusammenfassen auf $q \neq 0$, andererseits trivialerweise durch Abziehen von $\sum_{j=1}^{s} h_j \cdot f_j$ und nachheriges Zusammenfassen gleicher Glieder auf 0 M-reduziert werden kann. (Man beachte, dass beide Vorgangsweisen die Definition einer M-Reduktion erfüllen!)

2.3. *Beschreibung eines Teilschrittes des Algorithmus*

In einem Teilschritt des Algorithmus ist folgender Vorgang auszuführen: Bilde das *kleinste gemeinsame Vielfache* (*abgekürzt KGV*) der GPP pp_j und pp_k zweier verschiedener Basispolynome f_j and f_k, nämlich das PP

$$pp_{j,k} = x_1^{L_{j,k,1}} \ldots x_n^{L_{j,k,n}}, \quad \text{wobei} \quad L_{j,k,t} = \max(I_{j,t}, I_{k,t}) \quad (t = 1, \ldots, n).$$

Für $pp_{j,k}$ ergeben sich aus (2) die folgenden beiden Kongruenzen:

$$pp_{j,k} \leftrightarrow - \sum a^{(j)}_{i_1 \ldots i_n} x_1^{i_1 + d_{j,1}} \ldots x_n^{i_n + d_{j,n}} \tag{4}$$

und

$$pp_{j,k} \leftrightarrow - \sum a^{(k)}_{i_1 \ldots i_n} x_1^{i_1 + d_{k,1}} \ldots x_n^{i_n + d_{k,n}}, \tag{5}$$

wobei

$$d_{j,t} = L_{j,k,t} - I_{j,t} \quad \text{und} \quad d_{k,t} = L_{j,k,t} - I_{k,t} \quad (t = 1, \ldots, n).$$

Das Polynom, das durch Subtraktion der rechten Seiten von (4) and (5) entsteht, nennen wir *das zu $pp_{j,k}$ gehörige S-Polynom.* Durch M-Reduktion dieses Polynoms in bezug auf die gerade vorliegende Idealbasis können zwei Situationen entstehen:

1. Das zu $pp_{j,k}$ gehörige S-Polynom wurde auf null M-reduziert. In diesem Fall gehen wir zum nächsten Teilschritt über, so wie in 2.4. angegeben.
2. Das zu $pp_{j,k}$ gehörige S-Polynom wurde auf ein Polynom (6) M-reduziert, das nicht identisch verschwindet:

$$a\, x_1^{I_1} \ldots x_n^{I_n} + \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \quad (a \in K, \quad a \neq 0), \tag{6}$$

wobei wir wieder das GPP dieses Polynoms besonders hervorgehoben und mit $x_1^{I_1} \ldots x_n^{I_n}$ bezeichnet haben. In diesem Fall fügen wir das so erhaltene Polynom in der Form

$$x_1^{I_1} \ldots x_n^{I_n} + \frac{1}{a} \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \tag{7}$$

der Idealbasis bei. Wir vergrössern damit auch die Vielfalt der in (2) erscheinenden Relationen und damit die Anzahl der möglichen M-Reduktionen, die für irgendein Polynom in Zukunft ausgeführt werden können. Wir gehen gemäss 2.4. zum nächsten Teilschritt über.

2.4. *Kombination der Teilschritte*

Die in 2.3. angegebenen Operationen werden hintereinander für alle $pp_{j,k}$ ausgeführt, wobei $j=1,\ldots,s-1$ und $k=j+1,\ldots,s$. Man beachte, dass sich die Anzahl s der erzeugenden Polynome während der Ausführung des Algorithmus i.a. ändert. Es empfiehlt sich für die praktische Rechnung, die $pp_{j,k}$ mit kleineren Nummern zuerst zu bearbeiten, da dadurch die Rechenzeit meist erheblich vermindert werden kann.

Für eine gewisse Kombination der Indizes j und k kann einer der folgenden Spezialfälle eintreten:

S1. $pp_{j,k}=pp_j$ (oder $pp_{j,k}=pp_k$). In diesem Fall kann das Basispolynom f_j (bzw. f_k) aus der Basis gestrichen werden, nachdem die in 2.3. definierten Operationen für $pp_{j,k}$ ausgeführt wurden.

S.2. $pp_{j,k}=pp_j\cdot pp_k$. In diesem Fall brauchen wir die in 2.3. definierten Operationen für $pp_{j,k}$ nicht auszuführen.

Der Algorithmus sei beendet, wenn alle $pp_{j,k}$ nach den Vorschriften von 2.3. behandelt wurden.

Wir haben nun die beiden folgenden Behauptungen zu beweisen:

B1. *Sei* $(g_1,\ldots,g_u)$ *die Idealbasis, die nach Abbrechen des Algorithmus vorliegt. Dann hat* $(g_1,\ldots,g_u)$ *die in der Voraussetzung des Hilfssatzes geforderte Eigenschaft.*

B2. *Der Algorithmus bricht für jedes Ideal nach endlich vielen Schritten ab.*

3. Beweise

3.1. *Beweis von B1*

Die neuen Basispolynome seien

$$g_j = x_1^{S_{j,1}} \ldots x_n^{S_{j,n}} + \sum c^{(j)}_{i_1\ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \quad (j=1,\ldots,u).$$

Für diese spezielle Idealbasis gilt: Wenn wir alle $pp_{j,k}$ ($pp_{j,k}$ sei jetzt das KGV von $x_1^{S_{j,1}}\ldots x_n^{S_{j,n}}$ und $x_1^{S_{k,1}}\ldots x_n^{S_{k,n}}$) noch einmal nach den Vorschriften des Algorithmus behandeln würden ($j=1,\ldots,u-1$ und $k=j+1,\ldots,u$), so könnten wir jetzt alle dabei auftretenden S-Polynome auf wenigstens eine Art auf null M-reduzieren, da wir beim ersten Durchlauf des Algorithmus gerade die dazu notwendigen Polynome der Art (7) in die Idealbasis aufgenommen haben.

Im Falle, dass $pp_{j,k}=pp_j\cdot pp_k$ (pp_j sei jetzt die Abkürzung für $x_1^{S_{j,1}}\ldots x_n^{S_{j,n}}$), hat das zugehörige S-Polynom die Form:

$$-\sum c^{(j)}_{i_1\ldots i_n} x_1^{i_1+S_{k,1}} \ldots x_n^{i_n+S_{k,n}} + \sum c^{(k)}_{k_1\ldots k_n} x_1^{k_1+S_{j,1}} \ldots x_n^{k_n+S_{j,n}}.$$

Die spezielle M-Reduktion, bei der wir jedes

$$x_1^{i_1+S_{k,1}} \ldots x_n^{i_n+S_{k,n}}$$

durch

$$-\sum c^{(k)}_{k_1\ldots k_n} x_1^{k_1+i_1}\ldots x_n^{k_n+i_n}$$

und jedes

$$x_1^{k_1+S_{j,1}}\ldots x_n^{k_n+S_{j,n}}$$

durch

$$-\sum c^{(j)}_{i_1\ldots i_n} x_1^{i_1+k_1}\ldots x_n^{i_n+k_n}$$

ersetzen, macht dieses S-Polynom sofort zu null. In diesem Fall existiert also immer eine M-Reduktion des entsprechenden S-Polynoms auf null, auch wenn für $pp_{j,k}$ die in 2.3. definierten Operationen nicht ausgeführt wurden.

Wir zeigen nun, dass in bezug auf die Idealbasis $(g_1,\ldots,g_u)$ jede M-Reduktion eines gegebenen Polynoms zum gleichen Resultat führt. Wir beweisen mit Induktion und beginnen mit $x_1^0\ldots x_n^0$. $x_1^0\ldots x_n^0$ hat eine eindeutig bestimmte M-reduzierte Form relativ zu jeder Idealbasis, denn es ist entweder ein NPP und damit schon (eindeutig) M-reduziert oder ein MPP und damit auf null M-reduzierbar.

Die Induktionsvoraussetzung lautet: für jedes Polynom, dessen GPP eine nicht grössere Nummer als ein festes PP pp_0 hat, liefert M-Reduktion in bezug auf $(g_1,\ldots,g_u)$ ein eindeutig bestimmtes NPP-Polynom.

Zu zeigen ist: Für ein Polynom

$$f = c_1\cdot x_1^{V_1}\ldots x_n^{V_n}+\cdots+c_p\cdot x_1^{V_1}\ldots x_n^{V_n}+\sum a_{v_1\ldots v_n}x_1^{v_1}\ldots x_n^{v_n},$$

dessen GPP $x_1^{V_1}\ldots x_n^{V_n}$ eine um eins grössere Nummer als pp_0 hat, liefert M-Reduktion ein eindeutig bestimmtes NPP-Polynom. (Man beachte, dass wir die Behauptung für Polynome, in denen eventuell gleiche Glieder noch nicht zusammengefasst sind, zeigen müssen, weil wir sie in dieser Form in 2.2. verwendet haben.)

Wir unterscheiden drei Fälle:

Fall A. $x_1^{V_1}\ldots x_n^{V_n}$ ist NPP. M-Reduktion von f heisst dann: M-Reduktion von

$$\sum a_{v_1\ldots V_n}x_1^{v_1}\ldots x_n^{v_n},$$

was wegen der Induktionsvoraussetzung ein eindeutiges Resultat liefert, und Zusammenfassen der Glieder $c_q\cdot x_1^{V_1}\ldots x_n^{V_n}$ $(q=1,\ldots,p)$, was ebenfalls zu einem eindeutigen Ergebnis führt.

Fall B. $x_1^{V_1}+x_n^{V_n}$ ist Vielfaches genau eines $x_1^{S_{j,1}}\ldots x_n^{S_{j,n}}$ $(1\leqslant j\leqslant u)$. In einem gewissen Stadium der M-Reduktion von f muss jeder Term $c_q\cdot x_1^{V_1}\ldots x_n^{V_n}$ zunächst durch $c_q\cdot\sum(j)$, wobei

$$\sum(j)=\sum c^{(j)}_{i_1\ldots i_n}x_1^{i_1+d_{j,1}}\ldots x_n^{i_n+d_{j,n}}\left(d_{j,t}=V_t-S_{j,t}\quad\text{für}\quad t=1,\ldots,n\right),$$

ersetzt $(q=1,\ldots,p)$ und dann, zusammen mit den anderen Gliedern des Polynoms, weiter M-reduziert werden, was aber wieder auf Grund der Induktionsvoraussetzung zu einem eindeutigen Resultat führt.

Fall C. $x_1^{V_1} \dots x_n^{V_n}$ ist Vielfaches von mehreren $x_1^{S_{j,1}} \dots x_n^{S_{j,n}}$, z.B. $j=j_1,\dots,j_z$ $(1<z\leqslant u)$. Während der M-Reduktion von f wird jedes $c_q \cdot x_1^{V_1} \dots x_n^{V_n}$ $(q=1,\dots,p)$ durch ein Polynom $c_q \cdot \sum(j_{r_q})$ ersetzt werden, wobei $j_{r_q} \in \{j_1,\dots,j_z\}$. Eine fixe Kombination von Indizes $(j_{r_1},\dots,j_{r_p})$ charakterisiert also eine Mannigfaltigkeit von M-Reduktionen von f, die alle diesselben „Anfangsersetzungen" für die Glieder $c_q \cdot x_1^{V_1} \dots x_n^{V_n}$ verwenden und alle dasselbe Resultat liefern, wie wir leicht einsehen, indem wir die Überlegungen bei Fall B. leicht modifizieren. Insbesondere führen alle M-Reduktionen, die durch das p-Tupel $(j_1,j_1,\dots,j_1)$ charakterisiert sind, zum selben NPP-Polynom. Wir sind fertig, wenn wir zeigen können, dass unter den M-Reduktionen, die durch eine gewisse Kombination $(j_{r_1},\dots,j_{r_p})$, und denen, die durch $(j_1,\dots,j_1)$ charakterisiert sind, je eine angegeben werden kann, die zum gleichen Resultat führt. Eine passende M-Reduktion aus der durch $(j_1,\dots,j_1)$ charakterisierten Klasse ersetzt zunächst auf alle Fälle $c_q \cdot x_1^{V_1} \dots x_n^{V_n}$ $(q=1,\dots,p)$ in f durch

$$c_q \cdot \sum c_{i_1 \dots i_n}^{(j_1)} x_1^{V'_1+i_1+d_{j_1,1}} \dots x_n^{V'_n+i_n+d_{j_1,n}}, \tag{8}$$

wobei

$$V'_t = V_t - L_{j_1,j_{r_q},t}, \quad d_{j_1,t} = L_{j_1,j_{r_q},t} - S_{j_1,t},$$
$$L_{j_1,j_{r_q},t} = \max(S_{j_1,t}, S_{j_{r_q},t})$$

(Exponenten des KGV $pp_{j_1,j_{r_q}}$), $t=1,\dots,n$.

Eine geeignete M-Reduktion aus der durch $(j_{r_1},\dots,j_{r_p})$ charakterisierten Klasse ersetzt zunächst $c_q \cdot x_1^{V_1} \dots x_n^{V_n}$ $(q=1,\dots,p)$ durch:

$$c_q \cdot \sum c_{i_1 \dots i_n}^{(j_{r_q})} x_1^{V'_1+i_1+d_{j_{r_q},1}} \dots x_n^{V'_n+i_n+d_{j_{r_q},n}}, \tag{9}$$

wobei

$$d_{j_{r_q},t} = L_{j_1,j_{r_q},t} - S_{j_{r_q},t} \quad (t=1,\dots,n).$$

Die Polynome (8) und (9) sind genau die Polynome, deren Differenz das zu $pp_{j_1,j_{r_q}}$ gehörige S-Polynom ergab, jedoch beide mit $x_1^{V'_1} \dots x_n^{V'_n}$ multipliziert. Aus einer M-Reduktion, die dieses S-Polynom auf null reduziert (und die es auf Grund der Überlegungen zu Beginn dieses Abschnitts in bezug auf $(g_1,\dots,g_u)$ immer gibt), kann man sofort eine M-Reduktion des Polynoms, das aus (8) und (9) durch Differenzbildung entsteht, auf null gewinnen, indem man alle bei der M-Reduktion des S-Polynoms auftretenden PP mit $x_1^{V'_1} \dots x_n^{V'_n}$ multipliziert. Lässt sich aber die Differenz zweier Polynome auf null M-reduzieren, so lassen sich die beiden Polynome für sich auf wenigstens eine Art auf das gleiche Polynom M-reduzieren, wie man sich leicht überlegt. Es gibt also unter den durch $(j_1,\dots,j_1)$ charakterisierten und den durch $(j_{r_1},\dots,j_{r_p})$ charakterisierten M-Reduktion von f mindestens je eine, die zum gleichen NPP-Polynom führt. Damit ist B1 gezeigt.

Es bleibt noch die Rechtfertigung der Behandlung des Spezialfalles S1 offen. Wir können uns jedoch leicht davon überzeugen, dass durch das Streichen eines erzeugenden Polynoms, das die in S1 geforderte Eigenschaft hat, die Mannigfaltigkeit der

ausführbaren M-Reduktionen nicht vermindert wird, sofern wir nur gegebenenfalls das aus dem zugehörigen S-Polynom entstandene NPP-Polynom der Idealbasis beigefügt haben, so wie es der Algorithmus vorschreibt. Die Behauptung, dass alle zu den $pp_{j,k}$ gehörigen S-Polynome in bezug auf die Idealbasis $(g_1, \ldots, g_u)$ auf null M-reduziert werden können, die die Grundlage für den Beweis der Eindeutigkeit der M-Reduktionen eines Polynoms bildet, bleibt also auch nach Streichen eines Basispolynoms auf Grund des Eintretens des Falles S1 noch richtig.

3.2. *Beweis von B2*

Bei der Behandlung eines KGV $pp_{j,k}$ gemäss den Vorschriften des Algorithmus wird die Idealbasis eventuell durch das Hinzufügen eines Polynoms vergrössert, dessen GPP ein NPP relativ zu der bisherigen Idealbasis ist. B2 ist gezeigt, wenn wir den folgenden Satz bewiesen haben:

SATZ: *Eine Folge von PP* $x_1^{I_{j,1}} \ldots x_n^{I_{j,n}}$ $(j=1, 2, 3\ldots)$, *die die Eigenschaft hat, dass* $x_1^{I_{k,1}} \ldots x_n^{I_{k,n}}$ $(k=2, 3\ldots)$ *nicht Vielfaches von irgendeinem* $x_1^{I_{m,1}} \ldots x_n^{I_{m,n}}$ $(m<k)$ *ist, hat nur endlich viele Elemente.*

(Eine Folge von PP mit der obigen Eigenschaft werden wir *M-Folge* nennen.)

Beweis. Der Satz ist für $n=1$ leicht einzusehen. Wir setzen seine Richtigkeit für alle $n<N$ voraus und betrachten eine M-Folge, die mit $x_1^{I_1} \ldots x_N^{I_N}$ beginnt. Sei $x_1^{v_1} \ldots x_N^{v_N}$ ein anderes Element der M-Folge, dann gilt $v_i<I_i$ für mindestens ein i $(1\leqslant i\leqslant N)$. Für eine beliebige Kombination von Indizes $(i_1, \ldots, i_k)$ $(1\leqslant k\leqslant N, 1\leqslant i_j\leqslant N$ für $j=1, \ldots, k, i_j\neq i_m$ für $j\neq m)$ gibt es nur endlich viele k-Tupel $(v_{i_1}, \ldots, v_{i_k})$ positiver ganzer Zahlen (null eingeschlossen), die $v_{i_j}<I_{i_j}$ für $j=1, \ldots, k$ erfüllen. Die PP einer M-Folge gehören also zu endlich vielen Typen, deren jeder durch eine feste Kombination von Exponenten $(v_{i_1}, \ldots, v_{i_k})$ bei gewissen k Variablen $x_{i_1}, \ldots, x_{i_k}$ charakterisiert ist.

In einer M-Folge mit unendlich vielen Elementen müsste wenigstens eine unendliche Teilfolge existieren, deren Elemente alle zum gleichen Typ gehören. Durch Streichen der Variablen $x_{i_1}, \ldots, x_{i_k}$, bei denen die PP dieser Teilfolge die festen Exponenten $v_{i_1}, \ldots, v_{i_k}$ haben mögen, entstehen aus diesen PP solche in $n-k$ Variablen, die ebenfalls – im Widerspruch zu unserer Induktionsvoraussetzung – eine unendliche M-Folge bilden.

Bemerkung. Dieser Beweis zeigt, dass der Algorithmus prinzipiell endlich ist, unabhängig von speziellen Eigenschaften der Ideale (z.B. der Dimension), sagt jedoch nichts über seine Wirtschaftlichkeit. In diesem Zusammenhang erscheint die folgende Tatsache interessant: Bei Anwendung auf ein System linearer Gleichungen geht der Algorithmus in das Gauss'sche Eliminationsverfahren über, wie man unmittelbar nachprüfen kann. Er ist also in einem gewissen Sinne eine Verallgemeinerung des Gauss'schen Algorithmus.

4. Aussagen über die Existenz einer Nullstelle und die Dimension

Bekanntlich hat ein Polynomideal **a** genau dann keine Nullstelle, wenn $\mathbf{a}=(1)$, d.h. der zugehörige Restklassenring **o** nur aus einer Restklasse besteht. Das ist dann und nur dann der Fall, wenn während des Ablaufs des Algorithmus das Polynom $x_1^0 \dots x_n^0$ in die Idealbasis aufgenommen werden muss. (Kommt $x_1^0 \dots x_n^0$ nicht in der Idealbasis vor, die nach Abbrechen des Algorithmus vorliegt, so gibt es mehr als ein NPP und damit mehr als eine Restklasse in **o**!) Wir haben damit:

KRITERIUM 4.1. *Ein Polynomideal hat genau dann keine Nullstelle, wenn während der Ausführung des Algorithmus das Polynom $x_1^0 \dots x_n^0$ in die Idealbasis aufgenommen werden muss.*

Ausserdem können wir die folgende Feststellung über die Dimension des Ideals treffen:

KRITERIUM 4.2. *Ein Polynomideal hat genau dann eine höhere Dimension als null, wenn die Idealbasis $(g_1, \dots, g_u)$, die nach Abbrechen des Algorithmus vorliegt, die folgende Eigenschaft hat: Es gibt ein i $(1 \leqslant i \leqslant n)$, sodass kein PP der Form x_i^h unter den GPP der Basispolynome vorkommt $(h \geqslant 0)$.*

Beweis. Unter Verwendung der Definition der Dimension eines Polynomideals ([Gröbner 1], S. 98) sieht man leicht, dass ein Polynomideal genau dann die Dimension null hat, wenn die Restklassenalgebra endlichdimensional ist. Die Anzahl der Basiselemente der Restklassenalgebra (= die Anzahl der NPP bezüglich $(g_1, \dots, g_u)$) ist aber genau dann unendlich, wenn die im Kriterium 4.2. ausgesprochene Bedingung gilt.

5. Berechnung der Multiplikationstafel der Restklassenalgebra

Seien $\overline{x_1^{i_1} \dots x_n^{i_n}}$ und $\overline{x_1^{k_1} \dots x_n^{k_n}}$ Grössen, die durch den Algorithmus als Basiselemente für **o** konstruiert wurden. (Mit Überstreichen kennzeichnen wir den Übergang zur entsprechenden Restklasse.) Wir erhalten dann eine Darstellung ihres Produktes $\overline{x_1^{i_1+k_1} \dots x_n^{i_n+k_n}}$ als Linearkombination der Restklassen der NPP durch M-Reduktion von $x_1^{i_1+k_1} \dots x_n^{i_n+k_n}$ in bezug auf die Idealbasis, die nach Abbrechen des Algorithmus vorliegt.

6. Bemerkung zur Konstruktion von Nullstellen

Es sei hier noch ein Weg angedeutet, wie bei Kenntnis der Struktur der Restklassenalgebra Nullstellen für das Polynomideal gefunden werden können. Betrachten wir zunächst den nulldimensionalen Fall! Seien $u_1, \dots, u_m$ die PP, deren Restklassen eine Basis für **o** bilden. Unter Verwendung der Multiplikationstafel, können wir nacheinander für alle $\overline{x_1^k}$ $(k=0, 1, \dots)$ Darstellungen als Linearkombinationen der $\overline{u_j}$ $(j=1, \dots$

..., m) finden und für jedes $\overline{x_1^k}$ prüfen, ob es bereits von $1, \overline{x_1}, \ldots, \overline{x_1^{k-1}}$ linear abhängt. Dies sei für $k = m_1$ ($m_1 \leqslant m+1$) das erstemal der Fall, es gelte also

$p_1(\overline{x_1}) = 0$, wobei $p_1(x_1)$ ein Polynom des Grades m_1 aus $K[x_1]$ ist.

Als nächstes bilden wir die Darstellungen der Restklassen der PP, die aus $1, x_1, \ldots, x_1^{m_1-1}$ durch Multiplikation mit $x_2, x_2^2, \ldots$ entstehen, solange bis für eine gewisse Restklasse $\overline{x_1^{i_1} x_2^{i_2}}$ eine lineare Abhängigkeit von früheren PP-Restklassen zu Tage tritt, die sich in der Form

$$p_2(\overline{x_1}, \overline{x_2}) = 0 \quad \text{mit} \quad p_2(x_1, x_2) \in K[x_1, x_2]$$

schreiben lässt.

Entsprechend gehen wir weiter und erhalten so eine Folge von *Polynomen* $p_k(x_1, \ldots, x_k) \in \mathbf{a}$ ($k = 1, \ldots, n$), *die man sukzessive lösen kann.* Alle Nullstellen des Ideals kommen sicher unter den gemeinsamen Nullstellen der p_k vor, das Umgekehrte ist i.a. nicht der Fall. Es müssen noch Vorkehrungen getroffen werden (durch Hinzunahme weiterer Polynome aus **a**), dass überschüssige Nullstellen ausgeschieden werden. Ein genaues Studium der in diesem Zusammenhang auftretenden Fragen geht jedoch über die Zielsetzung der vorliegenden Arbeit hinaus.

Den d-dimensionalen Fall ($d > 0$) kann man durch Einsetzen von numerischen Werten für d in bezug auf **a** unabhängige Variable auf den nulldimensionalen Fall zurückführen und gelangt so wenigstens zu endlich vielen Lösungen. Von jedem Lösungspunkt ausgehend kann man unter gewissen Voraussetzungen z.B. mit Hilfe von Lie-Reihen ([Gröbner 2], S. 72ff.) die Lösungsmannigfaltigkeit in der Umgebung dieses Punktes konstruieren. Hier bleiben aber noch viele Detailfragen zu untersuchen.

7. Beispiel und Bemerkung zur Programmierung

Um die Schritte des Algorithmus weiter zu erläutern, geben wir ein einfaches Beispiel:

$$\mathbf{a} = (x_3^2 - \tfrac{1}{2}x_1^2 - \tfrac{1}{2}x_2^2, x_1x_3 - 2x_3 + x_1x_2, x_1^2 - x_2).$$

Betrachten wir zunächst das $pp_{1,2}$, nämlich $x_1x_3^2$. Das zugehörige S-Polynom ist:

$$S_{1,2} = \tfrac{1}{2}x_1^3 + \tfrac{1}{2}x_1x_2^2 - 2x_3^2 + x_1x_2x_3.$$

M-Reduktion von $S_{1,2}$ liefert:

$$x_1x_2^2 - x_1x_2 + 2x_2 + 2x_2^2 - 4x_2x_3.$$

Dieses Polynom nehmen wir in die Idealbasis auf. In analoger Weise müssen wir die anderen $pp_{j,k}$ behandeln, wobei $j = 1, \ldots, s-1$ und $k = 2, \ldots, s$. s ist am Anfang 3, wird durch Hinzunahme des neuen Basispolynoms gleich 4 und ändert sich im Verlauf

des Algorithmus noch einige Male. $pp_{1,3}$ ist z.B. ein PP, für das die Überlegungen des Spezialfalles S2 zutreffen, die M-Reduktion von $S_{1,3}$ kann man also übergehen.

Als neue Idealbasis erhalten wir schliesslich:

$$\begin{aligned}\mathbf{a} = (&x_3^2 - \tfrac{1}{2}x_2^2 - \tfrac{1}{2}x_2, x_1x_3 - 2x_3 + x_1x_2, x_1^2 - x_2,\\ &x_1x_2^2 + 7x_1x_2 + 2x_2 + 6x_2^2 - 16x_3,\\ &x_2x_3 + x_2^2 + 2x_1x_2 - 4x_3, x_2^3 - 12x_2 - 29x_2^2 + 64x_3 - 24x_1x_2).\end{aligned}$$

Die GPP der sechs Basispolynome sind: x_3^2, x_1x_3, x_1^2, $x_1x_2^2$, x_2x_3, x_2^3. Anwendung von Kriterium 4.2 liefert also: **a** ist nulldimensional. Die Restklassen der PP 1, x_1, x_2, x_3, x_1x_2, x_2^2 bilden eine Basis der Restklassenalgebra. Das Produkt des vierten und sechsten Basiselements z.B. wird durch M-Reduktion von $x_2^2x_3$ gebildet. Es entsteht:

$$x_2^2x_3 \leftrightarrow -18x_1x_2 + 48x_3 - 8x_2 - 21x_2^2.$$

Entsprechend können die übrigen Elemente der Multiplikationstafel aufgesucht werden.

Die Rechenzeit steigt selbstverständlich mit zunehmender Variablenzahl und Erhöhung der Polynomgrade sehr rasch. Die Programmierung des Algorithmus ist wegen seiner einheitlichen Struktur sehr leicht möglich. Man verwendet vorteilhaft Listprocessing-Konzepte. Programme existieren im Freiburger Code und im Formelcode der ZUSE Z 23.

Es sei an dieser Stelle auch auf die Arbeit [Hermann] verwiesen, in der sich zu ähnlichen Fragen eine Fülle von Material findet.

Ich möchte die Gelegenheit benutzen, meinem verehrten Lehrer, Herrn Prof. W. Gröbner, meinen aufrichtigen Dank auszusprechen.

LITERATURHINWEISE

[Gröbner 1]: GRÖBNER, W., *Moderne algebraische Geometrie* (Springer-Verlag, Wien und Innsbruck 1949).

[Gröbner 2]: GRÖBNER, W., *Teoria degli ideali e geometria algebrica*, in *Seminari dell'Istituto Nazionale di Alta Matematica 1962–1963* (Edizione Cremonese, Roma 1964).

[Gröbner 3]: GRÖBNER, W., Mündliche Mitteilung im Math. Seminar der Universität Innsbruck, 1964.

[Hermann]: HERMANN, G., *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. *95*, 736–788 (1926).

[Waerden]: VAN DER WAERDEN, B. L., *Moderne Algebra*, 2. Band, 2. Auflage (Springer-Verlag, Berlin 1937).

Universität Innsbruck