PERIODICA POLYTECHNICA SER. MECH. ENG. VOL. 46, NO. 1, PP. 45–57 (2002)

GRÖBNERSCHE BASEN IN SPEZIELLEN RINGEN (AUS DER GESCHICHTE DER GRÖBNERSCHEN BASEN)

Ján ČIŽMÁR

Lehrstuhl für Geometrie MFF UK
Mlynská dolina
SK-842 48 Bratislava, Slovakia
e-mail: cizmar@fmph.uniba.sk

Eingegangen: März 8, 2000

Zum Andenken an Herrn Professor Julius Strommer gewidmet

Abstract

The basic concepts of Gröbner basis of an ideal in the polynomial ring is described. Particularly the computation of the standard basis in a local ring is explained. A short history of the development of the theory of Gröbner bases is sketched.

Keywords: Gröbner basis, Buchberger's algorithm, Mora's algorithm, standard basis.

Gröbnersche Basen sind in den letzten dreißig Jahren zu einem Hauptstrom der Computeralgebra und Computergeometrie geworden. Ihr algorithmischer und konstruktiver Charakter hat sich erst mit der raschen Entwicklung der Computertechnik und Computermethoden als höchst anwendbar erwiesen. Ihre Verbreitung nicht nur in mathematischen Kreisen, sondern auch und sogar mehr im Milieu der Informatiker und Techniker weist auf ihre hohe Anwendungsfähigkeit und numerische Bedeutung hin. Die theoretischen Grundlagen der Gröbnerschen Basen stellen eine Bereicherung einiger schon in der Antik angegangenen Fragestellungen dar und sind gleichzeitig mit der Theorie von modernen Strukturen der kommutativen Algebra eng verknüpft.

1. Motivierung

Eine von Grundaufgaben der algebraischen Geometrie ist die Bestimmung einer algebraischen Varietät in einem n-dimensionalen affinen Raum.

Sei $k = \bar{k}$ ein algebraisch abgeschlossener Körper, $A^n(k)$, $(n \geq 1)$ ein n-dimensionaler affine Raum über k, $R = k[X] = k[X_1, \ldots, X_n]$ ein Polynomring von n Unbestimmten über k und $I = (f_1, \ldots, f_r)$ ein durch Polynome $f_1, \ldots, f_r \in R$ erzugtes Ideal in R. Die Nullstellenmenge $V(I) = \{(x) \in A^n(k) | f(x) = 0$ für jedes Polynom $f \in I\}$ des Ideals im affinen Raum $A^n(k)$ ist eine durch das Ideal I bestimmte algebraische Varietät im Raum $A^n(k)$. Es gibt für das Ideal I eine Primzerlegung

$$I = Q_1 \cap \ldots \cap Q_s \cap \ldots \cap Q_t,$$

in welcher die isolierten Komponenten $Q_1, \ldots, Q_s$ eindeutig bestimmt sind und ihre Radikale $P_1, \ldots, P_s$ durch seinen Durschnitt $\bigcap_{i=1}^{s} P_i$ das $Rad(I)$ des Ideals I bilden. Es gilt

$$V(I) = V(Rad(I)) = \bigcup_{i=1}^{s} V(P_i),$$

wo $V(P_i)$ eindeutig bestimmte irreduzible Komponenten der Zerlegung $V(I)$ sind.

Anderseits ist

$$V(I) = \bigcap_{f \in I} V((f)).$$

Dann entsteht als Hauptproblem die Frage, wann $f \in I$ ist. Die Antwort ist einfach: $f = \sum_{i=1}^{r} h_i f_i$ mit gewissen $h_i \in R$.

Die Quelle neuer Probleme besteht darin, daß die Basis $\{f_1, \ldots, f_r\}$ des Ideals I allgemein nicht eindeutig bestimmt wird.

a) Für $n = 1$ ist $R = k[X]$ ein euklidischer Ring, folglich ist er auch Hauptidealring. (Daneben ist er auch ein Ring mit eindeutiger Primzerlegung.) Daraus folgt, daß $I = (f_1, \ldots, f_r) = (g)$ ist, wo g der größte gemeinsame Teiler von Polynomen $f_1, \ldots, f_r$ ist. Dann ist $f \in I$ genau dann, wenn f durch g teilbar ist. Der größte gemeinsame Teiler g von Polynomen $f_1, \ldots, f_r$ ist durch die sukzessive Anwendung des euklidischen Algorithmus auf die Polynome $f_1, \ldots, f_r$ berechenbar.

b) Im Fall $n \geq 2$ ist $R = k[X_1, \ldots, X_n]$ kein Hauptidealring, deswegen ist er nicht euklidisch. Der euklidische Algorithmus ist zur Berechnung des größten gemeinsamen Teilers von Polynomen $f_1, \ldots, f_r$ nicht verwendbar. Wolfgang GRÖBNER [1] hat im Jahre 1939 eine Idee ausgesprochen, das Verfahren nach dem euklidischen Algorithmus auf die Polynomringe in n ($n \geq 2$) Unbestimmten zu verallgemeinern. Er hat wörtlich geschrieben: „Man kann dieses Verfahren dazu benützen, den Restklassenring eines nulldimensionalen Polynomideals wirklich zu berechnen. . .” Das war keine blinde Vermutung, sondern ein mit langjährigen Forschungen begründetes hoffnungsvolles Programm der Idealtheorie. Wie er sich im Jahre 1950 geäußert hatte, befaßte er sich mit diesen Fragestellungen seit 1932 und hat dabei die Feststellungen von älteren fast vergessenen Arbeiten von MACAULAY wiederentdeckt.

Die Idee von W. GRÖBNER wurde durch Bruno BUCHBERGER in seiner Doktordissertation ‘Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Ideal’ an der Universität Innsbruck im Jahre 1965 verwirklicht.

[1] Wolfgang GRÖBNER, 11. 2. 1899 Gossensaß (Colle Isarco) – 20. 8. 1980 Innsbruck – österreichischer Mathematiker. Hauptbereiche seiner wissenschaftlichen Tätigkeit waren algebraische Geometrie und angewandte Mathematik. Bedeutende Monographien: Moderne algebraische Geometrie (Wien-Innsbruck 1949); Algebraische Geometrie I, II (Mannheim 1968, 1970).

Im Vergleich mit dem Fall $n = 1$ bestehen wesentliche Unterschiede in Polynomringen mit mehreren Unbestimmten in folgenden Tatsachen:

1. Die Division des untersuchten Polynoms muß wiederholt durch alle Erzeugenden des Ideals durchgeführt werden.
2. Das Endergebnis ist von der Reihenfolge der Division abhängig.

Die zweite Tatsache stellt ziemlich strenge Forderungen an die Anordnung im Polynomring vor. (Im Ring $k[X_1]$ ist die 'natürliche' Gradanordnung üblich.) Auf die bedeutsame Rolle der Anordnung hat besonders W. Gröbner im Zusammenhang mit den Arbeiten von Macaulay hingewiesen.

2. Gröbnersche Basis

a) Anordnungen

Sei M die Menge aller Monome $X^{(d)} = X_1^{d_1} \dots X_n^{d_n}$, $(d_i \geq 0, i = 1, \dots, n)$ im Ring $R = k[X] = k[X_1, ..., X_n]$.

Definition 1 Eine binäre Relation $>$ an M heißt Monomanordnung an R, wenn sie folgende Bedingungen erfüllt:

1. $>$ ist lineare (totale) Anordnung.
2. $>$ ist kompatibel mit der Multiplikation der Monome in R, d. h. aus $X^{(d)} > X^{(e)}$ folgt $X^{(d)}X^{(c)} = X^{(d)+(c)} > X^{(e)+(c)} = X^{(e)}X^{(c)}$ für ein beliebiges Monom $X^{(c)}$.
   Manchmal wird auch die Erfüllung einer zusätzlichen Bedingung gefordert:
3. $>$ ist Wohlanordnung, d. h. jede nichtleere Untermenge von Monomen hat das kleinste Element bezüglich $>$.

Übliche Monomanordnungen

1. **Lexikographische (lexikale) Anordnung**
   Sie ist folgendermaßen definiert:
   $X_1^{d_1} ... X_n^{d_n} > X_1^{e_1} ... X_n^{e_n}$ genau dann, wenn ein $i \in \{1, \dots, n\}$ existiert, so daß $d_k = e_k$ für $1 \leq k \leq i - 1$ und $d_i > e_i$.
2. **Inverse lexikographische (lexikale) Anordnung**
   $X_1^{d_1} ... X_n^{d_n} > X_1^{e_1} ... X_n^{e_n}$ genau dann, wenn es ein $i \in \{1, \dots, n\}$ gibt, so daß $d_k = e_k$ für $i + 1 \leq k \leq n$ und $d_i > e_i$.
3. **Lexikographische Totalanordnung (Homogene lexikographische Anordnung)**
   $X_1^{d_1} ... X_n^{d_n} > X_1^{e_1} ... X_n^{e_n}$ genau dann, wenn entweder $\sum_{i=1}^n d_i > \sum_{i=1}^n e_i$ oder $\sum_{i=1}^n d_i = \sum_{i=1}^n e_i$ und $X_1^{d_1} ... X_n^{d_n} > X_1^{e_1} ... X_n^{e_n}$ in der lexikographischen Anordnung ist.

4. **Inverse lexikographische Totalanordnung**
   $X_1^{d_1}...X_n^{d_n} > X_1^{e_1}...X_n^{e_n}$ genau dann, wenn entweder $\sum_{i=1}^n d_i > \sum_{i=1}^n e_i$ oder $\sum_{i=1}^n d_i = \sum_{i=1}^n e_i$ und $X_1^{d_1}...X_n^{d_n} > X_1^{e_1}...X_n^{e_n}$ in der inversen lexikographischen Anordnung ist.
5. **Blockanordnung**
   Sei M_1 die Menge aller Monome der Gestalt $X_1^{d_1}...X_i^{d_i}$, $i \in \{1, \ldots, n-1\}$, M_2 die Menge aller Monome der Gestalt $X_{i+1}^{d_{i+1}}...X_n^{d_n}$, $>_1$ die gewählte Anordnung an der Menge M_1, $>_2$ die gewählte Anordnung an der Menge M_2. Jedes Monom $m \in M \subset R$ hat eine eindeutige Darstellung $m = m_1 m_2$ mit $m_1 \in M_1$ und $m_2 \in M_2$.
   Seien $m = m_1 m_2$ und $t = t_1 t_2$ zwei beliebige Monome. Eine *Blockanordnung* an der Menge M ist folgendermaßen definiert: $m > t$ genau dann, wenn entweder $m_1 >_1 t_1$, oder $m_1 = t_1$ und $m_2 >_2 t_2$ ist.

b) Divisionsalgorithmus in $R = k[X_1, \ldots, X_n]$

Sei $>$ eine feste Monomanordnung an R, $f = \sum_{(d_1,\ldots,d_n)} c_{(d_1,\ldots,d_n)} X_1^{d_1} \ldots X_n^{d_n}$ ein beliebiges Polynom in R, $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ das größte Monom des Polynoms f in der Anordnung $>$, $c_{(\alpha_1,\ldots,\alpha_n)} X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ das Anfangsglied des Polynoms f in der Anordnung $>$ (Bezeichnung: $LT_>(f)$), $c_{(\alpha_1,\ldots,\alpha_n)}$ der Anfangskoeffizient des Polynoms f in der Anordnung $>$ (Bezeichnung $LC_>(f)$).

Sei $F = (f_1, \ldots, f_s)$ ein durch die Anordnung $>$ geordnetes s-Tupel der Polynome in R und $f \in R$ ein beliebiges Polynom. Dann gibt es eine Darstellung

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

mit $a_1, \ldots, a_s, r \in R$ und entweder $r = 0$ oder r ist eine lineare Kombination der Monome, die durch $LT_>(f_i)$ nicht teilbar sind. Das Polynom r heißt *Rest* des Polynoms f in der Division durch F. Die Bezeichnung: $r = \bar{f}^F$. Dieses Symbol drückt auch die Reihenfolge der sukzessiven Division des Polynoms f durch die Polynome $f_1, \ldots, f_s$ aus.

c) Gröbnersche Basis

Von verschiedenen äquivalenten Definitionsweisen der Gröbnerschen Basis besitzt die folgende Definition hoffentlich die größte Anschaulichkeit.

Definition 2 Sei $>$ eine feste Monomanordnung am Ring $R = k[X_1, \ldots, X_n]$ und sei $I \subset R (I \neq 0)$ ein Ideal. Unter Gröbnerschen Basis des Ideals I (in Bezug auf die Anordnung $>$) versteht man eine endliche Polynommenge $G = \{g_1, \ldots, g_t\} \subset I$, die folgende Eigenschaften besitzt:

1. $0 \neq G$
2. Für jedes Polynom $f \neq 0$ des Ideals I gibt es ein $i \in \{1, \ldots, t\}$ so daß $LT_>(f)$ durch $LT_>(g_i)$ teilbar ist.

Man sieht leicht ein, daß das durch die Anfangsglieder von Polynomen $g_1, \ldots, g_t$ erzeugte Ideal dem durch die Anfangsglieder aller Polynome des Ideals I erzeugten Ideal gleich ist. Dieses Ideal spielt eine wichtige Rolle beim Beweis der Existenz einer Gröbnerschen Basis eines beliebigen Ideals.

d) Algorithmus von Buchberger

Die Berechnung einer Gröbnerschen Basis für ein beliebiges Ideal bietet der Algorithmus von Buchberger an.

Definition 3 (S-Polynom) Sei $>$ eine feste Monomanordnung am Ring $R = k[X_1, \ldots, X_n]$ und seien $f \neq 0, g \neq 0$ zwei verschiedene Polynome von R mit den Anfangsgliedern

$$LT_>(f) = aX^{(c)}, LT_>(g) = bX^{(d)}, a, b \in k, (a \neq 0, b \neq 0).$$

Sei $X^{(e)}$ das kleinste gemeinsame Vielfache der Monome $X^{(c)}$, $X^{(d)}$. Das Polynom

$$S(f, g) = \frac{X^{(e)}}{LT(f)} f - \frac{X^{(e)}}{LT(g)} g$$

heißt das S-Polynom von Polynomen f und g.

Beispiel. Seien $f = X_1^3 X_2 - 2X_1^2 X_2^2 + X_1$, $g = 3X_1^4 - X_2$ Polynome des Rings $R = \mathbb{Q}[X_1, X_2]$ und sei $>$ lexikographische Anordnung an R.

$$X^{(c)} = X_1^3 X_2, X^{(d)} = X_1^4, X^{(e)} = X_1^4 X_2,$$
$$S(f, g) = X_1 f - \frac{1}{3} X_2 g = -2X_1^3 X_2^2 + X_1^2 + \frac{1}{3} X_2^2.$$

Kriterium von Buchberger Endliche Polynommenge $G = \{g_1, \ldots, g_t\} \subset I (\subset R)$ ist Gröbnersche Basis des Ideals $I \subset R$ genau dann, wenn $\overline{S(g_i, g_j)}^G = 0$ für alle Paare $(i, j), i \neq j$ ist.

Auf dem Kriterium von Buchberger beruht eine effektive Berechnung der Gröbnerschen Basis eines Ideals. Das Verfahren ergibt den *Algorithmus von Buchberger*:

Sei $F = \{f_1, \ldots, f_s\}$ eine beliebige Basis des Ideals $I \subset R$. Man berechne S-Polynome $S(f_i, f_j)$ für alle Paare (i, j), $i \neq j, i, j = 1, \ldots, s$. Ist $\overline{S(f_i, f_j)}^F \neq 0$ für irgendein Paar $(i, j), i \neq j$, ergänze man die Basis F durch $\overline{S(f_i, f_j)}^F$ und setze man das Verfahren fort. Da in diesem Fall $I = (f_1, \ldots, f_s) \subsetneq (f_1, \ldots, f_s, \overline{S(f_i, f_j)}^F)$ ist, muß dieses Verfahren nach endlich vielen Schritten abbrechen, weil der Ring R noetherisch ist.

Auf diese Weise kann jede Idealbasis zu einer Gröbnerschen Basis ergänzt werden.

Beispiel Sei $I = (f, g) \subset k[X, Y]$ ein durch die Polynome $f = X^2 - Y$ und $g = X - Y^2$ erzeugtes Ideal des Polynomrings $k[X, Y]$ (k ist ein algebraisch abgeschlossener Körper).

$$F = (f, g);\ LT_{lex}(f) = X^2,\ LT_{lex}(g) = X;\ X^{(e)} = X^2,$$
$$S(f, g) = f - Xg = X^2 - Y - (X^2 - XY^2) = XY^2 - Y,$$
$$\overline{S(f, g)}^F = Y^4 - Y \neq 0,$$
$$F' = (f, g, h);\ h = Y^4 - Y,$$
$$\overline{S(f, g)}^F = 0,$$
$$S(f, h) : X^{(e)} = X^2Y^4,$$
$$S(f, h) = Y^4(X^2 - Y) - X^2(Y^4 - Y) = X^2Y - Y^5,$$
$$(X^2Y - Y^5) : (X^2 - Y) = Y,\ \text{Rest: } -Y^5 + Y^2,$$
$$(-Y^5 + Y^2) : (Y^4 - Y) = -Y,\ \text{Rest: } 0.$$

Das bedeutet: $\overline{S(f, h)}^{F'} = 0$.

$$S(g, h) : X^{(e)} = XY^4,$$
$$S(g, h) = Y^4(X - Y^2) - X(Y^4 - Y) = XY - Y^6,$$
$$(XY - Y^6) : (X - Y^2) = Y,\ \text{Rest: } -Y^6 + Y^3,$$
$$(-Y^6 + Y^3) : (Y^4 - Y) = -Y^2,\ \text{Rest: } 0.$$

Das bedeutet: $\overline{S(g, h)}^{F'} = 0$.

$F' = G$ ist Gröbnersche Basis des Ideals I.

e) Reduzierte Gröbnersche Basis

Gröbnersche Basis G eines Ideals I heißt *reduziert,* wenn sie folgende Eigenschaft besitzt:

Für zwei beliebige Polynome $p, q \in G$, $p \neq q$, ist kein Monom des Polynoms p ein Vielfaches des Anfangsgliedes $LT(q)$ des Polynoms q.

Reduzierte Gröbnersche Basis G des Ideals I heißt *monisch,* wenn sie entweder $\emptyset$ ist (im Fall $I = (0)$) oder jedes darin enthaltene Polynom den Anfangskoeffizienten 1 hat.

In einer festen Monomanordnung des Rings R besitzt jedes Ideal $I \subset R$ eine einzige monische Gröbnersche Basis.

3. Gröbnersche Basis und lokale Ringe

a) Endlichkeitssatz

Sei I ein eigentliches Ideal des Rings $R = k[X_1, \ldots, X_n]$. Die folgenden Eigenschaften sind äquivalent:

1. $\dim_k(I) = 0$.
2. Die Algebra $A = R/I$ ist (als ein Vektorraum) endlichdimensional über k.
3. Es gibt eine Monomanordnung $>$ am Ring R und eine Gröbnersche Basis G des Ideals I in Bezug auf die Anordnung $>$, so daß für jedes i, $1 \leq i \leq n$, ein Polynom $g_i \in G$ mit dem Anfangsglied $LT_>(g_i) = X_i^{m_i}$ für ein $0 < m_i \in N$ existiert.
4. Für eine beliebige Monomanordnung $>$ an R und eine beliebige Gröbnersche Basis G (in Bezug auf $>$) gibt es für jedes i, $1 \leq i \leq n$, ein Polynom $g_i \in G$ mit dem Anfangsglied $LT_>(g_i) = X_i^{m_i}$ für $0 < m_i \in \mathbb{N}$.

Folgerung: $\dim_k R/I = m_1 \ldots . m_n$.

b) Geometrische Bedeutung

Sei $I \subset R = k[X_1, \ldots, X_n]$ ein Ideal und $\dim_k(I) = 0$; sei $(LT_>(I))$ das durch die Anfangsglieder (in Bezug auf eine feste Monomanordnung $>$ in R) aller Polynome von I erzeugte Ideal.

$$\dim_k R/I = \dim_k R/(LT_>(I)) =$$
$$= \text{ die Anzahl aller Monome } X^{(d)} \in R | X^{(d)} \notin (LT_>(I)).$$

Sei $I = Q_1 \cap \ldots \cap Q_s$ die Primärzerlegung des Ideals I und $M_1, \ldots, M_s$ die Radikale von $Q_1, \ldots, Q_s$. Diese Radikale sind maximale Ideale von der Gestalt $M_i = (X_1 - a_1^{(i)}, \ldots, X_n - a_n^{(i)})$. Das Radikal $Rad(I)$ des Ideals I besitzt eine Primzerlegung $Rad(I) = M_1 \cap \ldots \cap M_s$ und $V(I) = V(Rad(I)) = V(\bigcap_{i=1}^s M_i) = \bigcup_{i=1}^s V(M_i) = \bigcup_{i=1}^s (a^{(i)})$ ist eine endliche Punktmenge.

Durch eine geeignete Wahl des affinen Koordinatensystems kann man erreichen, daß $(a^{(1)}) = (0, \ldots, 0) = 0$ der Ursprung des Koordinatensystems wird. Dann ist es $M_1 = (X_1, \ldots, X_n)$.

Die Lokalisierung des Rings R nach dem Ideal M_1 ist ein lokaler Ring $R_{M_1} = k[X_1, \ldots, X_n]_{(X_1, \ldots, X_n)} = \{\frac{a}{b} | a, b \in R, b \notin M_1, d.\,h.\, b(0, \ldots, 0) \neq 0\}$.

Unter dem *Erweiterungsideal* eines Ideals $I \subset R$ im lokalen Ring R_{M_1} versteht man das Ideal $I R_{M_1} = \{\frac{a}{b} | a \in I, b \in R - M_1\}$.

Das Erweiterungsideal $M_1 R_1$ des Ideals M_1 im lokalen Ring R_{M_1} ist das einzige maximale Ideal des Rings R_{M_1}. (Für $M_i \neq M_1$ ist es $M_i R_{M_1} = (1)$.)

Auf Grund der vorangegangenen Begriffe ist der folgende algebraisch-geometrische Begriff definiert:
Unter der *Multiplizität* des Punktes $0 = (0, \ldots, 0)$ an der algebraischen Varietät $V(i)$ versteht man die Zahl $m(0) = \dim_k R_{M_1}/I R_{M_1}$.

Diese Definition stimmt mit der Krullschen Definition der (statischen) Multiplizität überein.

Beispiel. Die Berechnung der Multiplizität

Sei $I = (X^2, Y^2 + Y^3)$ das Ideal des Rings $R = k[X, Y]$ (k – algebraisch abgeschlossener Körper) mit der lexikographischen Monomanordnung, in welcher

$X > Y$ ist.

$$\dim_k R/I = \dim_k R/(LT(I)) = \dim_k R/(X^2, Y^3) = 6$$

da die Restklassen durch die Elemente $1, X, Y, XY, Y^2, XY^2$ dargestellt werden.

Algebraische Varietät $V(I)$ besteht aus zwei Punkten: $V(i) = \{(0,0), (0,-1)\}$. Die Gesamtmultiplizität beider von diesen Punkten muß gleich 6 sein.

a) Das assoziierte Ideal des Punktes $(0,0)$ ist $I((0,0)) = (X, Y)$. $U = R_{(X,Y)}$ ist lokaler Ring des Punktes $(0,0)$. Das Erweiterungsideal des Ideals I in U ist $(X^2, Y^2 + Y^3)U = (X^2, Y^3)U$. Die Restklassen des Rings $U/(X^2, Y^2)U$ werden durch die Elemente $1, X, Y, XY$ dargestellt. Das bedeutet: $\dim_k U/(X^2, Y^2)U = 4$. Die Multiplizität des Punktes $(0,0)$ ist gleich 4 (*Abb. 1*).

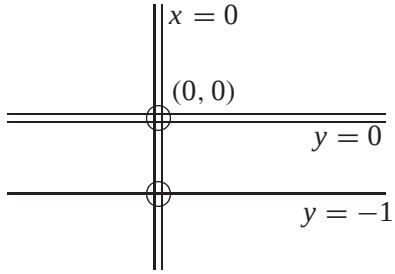

Abb. 1

b) Durch die Transformation $X' = X, Y' = Y + 1$ geht der Punkt $(0,-1)$ in den Punkt $(0,0)$ und das Polynom $Y^2 + Y^3$ ins Polynom $Y'(1 - 2Y' + Y'^2)$ über.

Sei $S = k[X', Y']_{(X',Y')}$; dann ist es $(X'^2, Y'(1 - 2Y' + Y'^2))S = (X'^2, Y')S$.

$\dim_k S/(X'^2, Y')S = 2$, da die Restklassen durch die Elemente $1, X'$ dargestellt werden. Die Multiplizität des Punktes $(0,-1)$ ist gleich 2 (*Abb. 1*).

c) Standardbasen in lokalen Ringen

1. **Lokale Anordnung**
   Die Monomanordnung $>$ am Ring $R = k[X_1, \ldots, X_n]$ heißt *lokal,* wenn sie die folgende zusätzliche Bedingung erfüllt:
   3'. $1 > X_i$ für alle $i = 1, \ldots, n$
2. **Lokalisierung bezüglich der Anordnung** $>$
   Sei $R = k[X_1, \ldots, X_n] >$ eine Monomanordnung, f – ein Polynom, $\{X^{(d)}\}$ die Menge aller Monome, die im Polynom f mit Nichtnullkoeffizienten vorkommen.
   Unter dem *Multigrad* des Polynoms f versteht man das n-Tupel

$$\text{multideg}(f) := \max_> \{(d) | c_{(d)} X^{(d)} \text{ kommt in } f \text{ vor }, c_{(d)} \neq 0\}.$$

Weiter ist es

$$\begin{aligned} LC_>(f) &:= c_{\text{multideg}(f)} \text{ – Anfangskoeffizient von } f, \\ LM_>(f) &:= X^{\text{multideg}(f)} \text{ – Anfangsmonom von } f, \\ LT_>(f) &:= LC_>(f).LM_>(f) \text{ – Anfangsglied von } f. \end{aligned}$$

Die Menge von Polynomen

$$S = \{(1+g) \in R | \text{ entweder } g = 0 \text{ oder } LT_>(g) < 1\}$$

ist multiplikativ abgeschlossen.
Der Quotientenring

$$R_S = S^{-1}R := \left\{ \frac{f}{1+g} | f \in R, (1+g) \in S \right\} =: Loc_> R$$

heißt *Lokalisierung* des Rings R bezüglich der Anordnung $>$.

3. **Homogenisierung**
Sei $R = k[X_1, \ldots, X_n]$, $g = \sum_{(\alpha)} c_{(\alpha)} X^{(\alpha)}$ ein Polynom von R, $|\alpha| = \sum_{i=1}^{n} \alpha_i$, $d = \max |\alpha|$ – Totalgrad des Polynoms f. Sei T eine von $X_1, \ldots, X_n$ algebraisch unabhängige Unbestimmte. Das Polynom

$$g^h = \sum_{(\alpha)} c_{(\alpha)} T^{d-|\alpha|} X^{(\alpha)}$$

heißt *Homogenisierung* des Polynoms g bezüglich T.

4. **Erweiterungsanordnung**
Sei $>$ eine Monomanordnung am Ring R. Die Erweiterungsanordnung $>'$ an der Menge aller Monome im Ring $k[T, X_1, \ldots, X_n]$ ist folgendermaßen definiert: $T^a X^{(\alpha)} >' T^b X^{(\beta)}$ genau dann, wenn entweder $a + |\alpha| > b + |\beta|$ oder $a + |\alpha| = b + |\beta|$ und $X^{(\alpha)} = X^{(\beta)}$.

5. **Normalformalgorithmus von Mora**
Seien $F, F_1, \ldots, F_s$ homogene Polynome von $k[T, X_1, \ldots, X_n]$ und $>'$ die Erweiterung einer Monomanordnung $>$ am Ring $k[X_1, \ldots, X_n]$. Es gibt einen Algorithmus, der homogene Polynome $H, U, A_1, \ldots, A_s$ bietet, so daß

$$UF = A_1 F_1 + \cdots + A_s F_s + H$$

ist, wobei $LT(U) = T^a$ für irgendeine Zahl $a \in \mathbb{N}$ ist,

$$a + \deg(F) = \deg(A_i) + \deg(F_i) = \deg(H),$$

solange A_i und H vom Null abweichend sind und kein $LT(F_i)$ das Produkt $T^b LT(H)$ für beliebege Zahl b teilt.

Dieser Algorithmus geht an MORA zurück und heißt *Normalformalgorithmus*.

Folgerung: Sei $>$ eine Monomanordnung an $R = k[X_1, \ldots, X_n]$ und $S = Loc_> R$. Sei $f \in S$ und $f_1, \ldots, f_s \in R$. Es gibt einen Algorithmus für die Berechnung der Elemente $h, a_1, \ldots, a_s \in S$, so daß $f = a_1 f_1 + \cdots + a_s f_s + h$ ist, wobei $LT(a_i).LT(f_i) \leq LT(f)$ für alle $i = 1, \ldots, s$ ist, entweder $h = 0$ oder $LT(h) \leq LT(f)$ und $LT(h)$ durch kein $LT(f_1), \ldots, LT(f_s)$ teilbar ist.

Man sieht unmittelbar, daß der Algorithmus von Mora eine Verallgemeinerung des Buchbergerschen Algorithmus auf den homogenen Fall ist.

6. **Standardbasis**
Sei $R = k[X_1, \ldots, X_n]$, $>$ – eine Monomanordnung an R, $S = Loc_> R$ – die Lokalisierung des Rings R bezüglich $>$ und $I \subset S$ ein Ideal. Eine endliche Menge $\{g_1, \ldots, g_t\} \subset I$ heißt *Standardbasis* des Ideals I, wenn $(LT(I)) = (LT(g_1), \ldots, LT(g_t))$ ist. Es ist offenbar, daß dieser Begriff eine Verallgemeinerung der Gröbnerschen Basis auf den Erweiterungsring S des Rings R ist.

7. **Verallgemeinerung der Ergebnisse von Buchberger**
Man bezeichne mit S eine endliche Polynommenge in $k[X_1, \ldots, X_n]$, $>$ – eine Monomanordnung und $I \subset S = Loc_>(k[X_1, \ldots, X_n])$ ein durch eine endliche Menge $G \subset S$ erzeugtes Ideal.

   (a) (Analog des Kriteriums von Buchberger) Eine Menge $W = \{g_1, \ldots, g_t\}$ ist Standardbasis des Ideals I genau dann, wenn die Anwendung des Normalformalgorithmus von Mora an jedes von der Menge der Homogenisierungen $W^h = \{g_1^h, \ldots, g_t^h\}$ erzeugte S-Polynom den Nullrest bietet.

   (b) (Analog des Algorithmus von Buchberger) Man wende an eine endliche Polynommenge W folgende Schritte an:
      i. Die Homogenisierung
      ii. Die Modifikation des Algorithmus von Buchberger in der Gestalt des Normalformalgorithmus von Mora
      iii. Die Enthomogenisierung

   Das Verfahren bricht nach endlich vielen Schritten ab und berechnet eine Standardbasis des durch die Menge W erzeugten Ideals.

4. Anwendung der Gröbnerschen Basen

a) Konstruktive Theorie von Moduln

Die Verallgemeinerung der Theorie von Gröbnerschen Basen von Idealen auf Moduln ermöglicht die Durchführung analogischer Operationen in der Kategorie von Moduln über einem festen Ring. Die Menge dieser Operationen schließt u. a. folgende Operationen ein:

- Eine Modifizierung des Dividierens mit dem Rest und das Feststellen der Angehörigkeit zu gegebenem Ideal:
  - Für ein gegebenes Ideal I des Ringes R eine Basis des Vektorraums R/I zu finden
  - Für ein gegebenes Polynom $f \in R$ eine Darstellung seines Bildes im Homomorphismus $R \to R/I$ mittels Basis des Vektorraums R/I zu finden
- Für ein Polynom $f \in I$ seine Darstellung mittels Erzeugender des Ideals I zu finden
- Die Berechnung von Syzygien
  - Für ein gegebenes s-Tupel $(f_1, \ldots, f_s)$ von Elementen eines R-Moduls M die Menge aller s-Tupel $(a_1, \ldots, a_s) \in R^s$ mit der Eigenschaft $\sum_{i=1}^{s} a_i f_i = 0$ zu finden; die Menge $\{(a_1, \ldots, a_s)\}$ aller solchen s-Tupel heißt Menge von Syzygien des n-Tupels $(f_1, \ldots, f_s)$ und wird mit $\mathrm{Syz}(f_1, \ldots, f_s)$ bezeichnet.
- Die Berechnung des Annulators eines Moduls
- Die Berechnung des Durchschnitts von zwei Idealen
- Die Berechnung des Moduls von Homomorphismen $\mathrm{Hom}_R(M, N)$ von Moduln M, N; verallgemeinert die Berechnung der Moduln Ext und Tor
- Die Berechnung der Hilbertschen Funktion und des Hilbertschen Polynoms eines gegebenen gradierten Moduls.

b) Eliminationstheorie

Zur Menge der Operationen in diesem Themenbereich zählen folgende Operationen:

- Elimination: Die Berechnung (der Erzeugenden) eines Ideals $J = I \cap R'$, wo I ein Ideal des Rings $R = k[X_1, \ldots, X_n]$ und $R' = k[X_1, \ldots, X_s]$ mit $s < n$ ist
- Die Berechnung von Hülle des Bildes einer affinen oder projektiven Varietät im gegebenen Morphismus
- Die Darstellung einer Aufblasungsalgebra und eines assoziierten gradierten Ringes zum Ring $\bar{R} = R/I$ bezüglich des Ideals M aufzufinden
- Die Gleichungen der Hülle einer affinen Varietät $V \subset \mathbb{A}^n$ im projektiven Raum $\mathbb{P}^n$ zu berechnen

5. Aus der Geschichte der Gröbnerschen Basen

Vorgeschichte

Zu den ersten die Probleme der späteren Gröbnerschen Basen untersuchenden Arbeiten gehört die Arbeit von P. GORDAN „Les invariants des formes binaires", Journal de Mathématiques Pures et Appliqués 6 (1900), 141 – 156. Die Gröbnersche Basis kommt in dieser Arbeit als „le système irreducible" vor und eine

endliche Erzeugung eines Monomideals wird zum Beweis des Hilbertschen Basissatzes benutzt. F. S. MACAULAY hat in der Monographie „Algebraic theory of modular systems", Cambridge Tracts 16, Cambridge University Press, Cambridge 1916, den Begriff der H-Basis eines Ideals eingeführt und zur Standarddarstellung der Basis (in der neueren Terminologie) gelangt. In seiner Arbeit „Some properties of enumeration in the theory of modular systems", Proc. London Math. Soc. 26 (1927), 531 – 555, wird die Totalgradanordnung in der Monomenmenge beschrieben. W. GRÖBNER verwendete die Ideen und Methoden von Macaulay in der Monomanordnung seit 1932, aber die Ergebnisse waren erst im Jahre 1939 im Werk „Über die algebraischen Eigenschaften der Intergrale von linearen Differentialgleichungen mit konstanten Koeffizienten", Monatsh. der Math. 47, 247 – 284, veröffentlicht. In demselben Jahre hat er das Grundproblem formuliert, das seinen Doktoranden B. BUCHBERGER zur Ausarbeitung der Fundamentalergebnisse in der Dissertation in Jahren 1964 – 65 veranlaßt hat. Daneben hat Gröbner in der Arbeit „Über die Eliminationstheorie", Monatsh. der Math. 54 (1950), 71 – 78, eine Übersicht der vorangegangenen Untersuchungen und Ergebnisse übermittelt und eine Überzeugung über die Effektivität und Wirksamkeit der Methoden auch bei der Lösung weiterer idealtheoretischen Probleme ausgesprochen. Unabhängig von den Forschungen von Buchberger wurden einzelne mit seiner Theorie zusammenhängende Begriffe und Verfahren (z. B. der Divisionsalgorithmus und Standardbasen) auch in anderen Strukturen (z. B. im Ring der formalen Potenzreihen) durch H. HIRONAKA (1964) und H. GRAUERT (1972) entwickelt.

Geschichte

Die eigentliche Geschichte der Gröbnerschen Basen ist durch die oben erwähnte Arbeit von Buchberger im Jahre 1965 begonnen. Die erste Fassung wurde von Buchberger in seinen späteren Arbeiten in Jahren 1970, 1976 und 1979 komplettiert, wo er auch nachträglich die Benennung zu Ehren von Gröbner und das zweite Kriterium angeführt hat. Die Ergebnisse von Buchberger wurden schrittweise und vielseitig durch viele weiteren Autoren entwickelt. G. BERGMAN hat die Fragestellungen im Jahre 1978 auf assoziative nichtkommutative Algebren und verallgemeinerte algebraische Systeme erweitert. Mit den analogischen Problemen in nichtkommutativen Strukturen befaßten sich D. E. KNUTH und P. B. BENDIX seit dem Jahre 1967. Im Jahre 1970 sind sie zum Analogon des S-Polynoms und zur Ergänzung des Systems von Polynomen zu einem die Buchbergerschen Kriterien erfüllenden System gelangt. Im Jahre 1983 erzielte D. LAZARD die Erweiterung des Kriteriums von Buchberger auf t-Darstellungen.

Zur Berechnung von Syzygien benutzten Gröbnersche Basen D. A. SPEAR (1977), G. ZACHARIAS (1978), F.-O. SCHREYER (1980), A. FURUKAWA (1986), B. WALL (1989) und andere. J. APEL und W. LASSNER untersuchten den nichtkommutativen Fall im Jahre 1988, eine Erweiterung unter Anwendung von S-Polynomen geht auf H. M. MOLLER im Jahre 1992 zurück.

Eine Reihe von Forschern untersuchten die Existenz und Eigenschaften der Gröbnerschen Basen in speziellen Ringen, wie z. B. in Ringen mit der eindeutigen

Zerlegung in Primfaktoren, in euklidischen Ringen usw. Zu der Liste gehören G. ZACHARIAS (1978), A. KANDI-RODY und D. KAPUR (1984, 1988), L. PAN (1989), F. PAUER (1992) und andere.

Gröbnersche Basen im homogenen Fall wurden u. a. von D. LAZARD (1983) und H. M. MOLLER und F. MORA (1984) untersucht. Besonders wichtiges Ergebnis war durch die Projektivisierung mit Hilfe der Darstellung einer affinen Varietät mittels einer Kegelfläche durch F. Mora im Jahre 1982 erreicht (Algorithmus von Mora).

Mit der Verallgemeinerung des Themenkreises der Gröbnerschen Basen auf Moduln beschäftigten sich D. BAYER (1982), D. LAZARD (1983), H. M. MÖLLER und F. MORA (1986), A. FURUKAWA (1986), C. J. BILLERA und L. L. ROSE (1989) und andere.

Die Literatur über Gröbnersche Basen stellt einen mächtigen und reichlichen Strom der gegenwärtigen reinen und angewandten Algebra dar. Das Literaturverzeichnis zu diesem Thema in [3] zählt insgesamt 515 Titel, davon 34 Tagungsbände, 89 Monographien und 392 Zeitschriftsarbeiten.

Literatur

[1] EISENBUD, D., *Commutative Algebra with a View toward Algebraic Geometry*, Springer, New York – Berlin etc. 1995.

[2] COX, D. – LITTLE, J. – O'SHEA, D., *Using Algebraic Geometry*, Springer, New York – Berlin etc. 1998.

[3] BECKER, T. – WEISPFENNIG, V., *Gröbner Bases*, Springer, New York – Berlin etc. 1993.