THE THEORY OF GRÖBNER BASES

L'Enseignement Mathématique, t. 34 (1988), p. 215-232

THE THEORY OF GRÖBNER BASES

by Franz PAUER and Marlene PFEIFHOFER

INTRODUCTION

Let R be a principal ideal domain (for example the ring of integers or a field) and $R[X] = R[X_1, ..., X_n]$ the polynomial ring in n variables over R.

Let us mention some questions related to a subset F of $R[X]$:

1) Let $P \in R[X]$. How can we decide (in a finite number of steps) if P is an element of the ideal generated by F?

2) How can we find exact solutions to the system of algebraic equations corresponding to F?

3) If F' is another subset of $R[X]$, how can we decide if F and F' generate the same ideal?

An answer to these questions can be given by the method of so-called "Gröbner-bases". [1])

A "basis" of an ideal in $R[X]$ is a subset which generates this ideal. If we choose a strict ordering on $\mathbf{N}^n$, we can (analogous to the one-variable case) define the degree and the initial term of polynomials in $R[X]$. A "Gröbner basis" is a finite ideal basis, such that the initial terms of its elements generate the ideal generated by all initial terms of polynomials in the given ideal (see 1.5.).

In the first section we arrange some notations and give the definition of a Gröbner basis.

Then we present a division algorithm, which generalizes the usual division of univariate polynomials, and we give a characterization of Gröbner bases in terms of this division.

In the third section we explain how to construct a Gröbner basis from a given finite ideal basis.

---

[1]) Wolfgang Gröbner, 1899-1980, tyrolean mathematician.

Finally, we apply the method of Gröbner bases to systems of algebraic equations and to a geometric problem:

Using the "lexicographic ordering" on $\mathbf{N}^n$, a Gröbner basis of an ideal immediately yields ideal bases of the corresponding elimination ideals (see 4.3.).

If X is an algebraic subset of the affine n-space, a Gröbner basis with respect to the "inverse lexicographic ordering" permits to obtain an ideal basis of the homogeneous ideal, which defines the Zariski-closure of X in the projective n-space (see 5.).

The method of Gröbner bases was introduced by B. Buchberger in 1965. For the history of the theory and for further applications see [B].

Our aim is to give a short and self-contained introduction to the theory of Gröbner bases. In this form it could be part of a second or third year algebra course. The results written down in this article can be found elsewhere, but we present short proofs.

We do not enter into questions of implementation or complexity of the algorithms (see for instance [B], [E], [K1], [T]).

Acknowledgements:

We thank Bruno Buchberger for sending us a long list of references.

We thank Ingrid Mittelberger for her interest and many discussions on this subject.

We thank Thierry Vust and the referee for proposing several improvements on the first version of this article.

1. Notations and Definitions

The notations introduced here will be valid throughout this article.

1.1. We denote by R a principal ideal domain (for example: $\mathbf{Z}$, a field, the polynomial ring or power series ring in one variable over a field) and by $R[X]$ the polynomial ring over R in n variables $X_1, ..., X_n$. Sometimes we make tacitly the additional assumption that we can compute a greatest common divisor of two elements in R.

If S is a subset of $R[X]$, we write $<S>$ for the ideal generated by S in $R[X]$.

Recall that $R[X]$ is a noetherian ring, this means that every strictly ascending sequence of ideals in $R[X]$ is finite.

For $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbf{N}^n$ we abbreviate $X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n}$ by X^α.

1.2. Let $<$ be a strict ordering on $\mathbf{N}^n$ which has the following two properties:

$$\forall \alpha \in \mathbf{N}^n - \{0\}, \quad 0 < \alpha;$$
$$\forall \alpha, \beta, \gamma \in \mathbf{N}^n, \quad (\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma).$$

Well-known examples for such orderings are:

the lexicographic ordering ($\alpha \underset{L}{<} \beta :\Leftrightarrow$ there is a $j \in \{1, ..., n\}$ such that $\alpha_k = \beta_k$ if $k < j$ and $\alpha_j < \beta_j$),

the graded lexicographic ordering

$$(\alpha \underset{GL}{<} \beta :\Leftrightarrow (\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i) \text{ or } ((\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i) \text{ and } \alpha \underset{L}{<} \beta)),$$

the graded inverse lexicographic ordering ($\alpha \underset{GIL}{<} \beta :\Leftrightarrow (\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i)$ or $((\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i)$ and there is a $j \in \{1, ..., n\}$ such that $\alpha_k = \beta_k$ if $k > j$ and $\alpha_j > \beta_j)$).

Examples:
$$(0, 2, 0) \underset{L}{<} (1, 0, 0) \underset{L}{<} (1, 0, 1)$$
$$(1, 0, 0) \underset{GL}{<} (0, 2, 0) \underset{GL}{<} (1, 0, 1)$$
$$(1, 0, 0) \underset{GIL}{<} (1, 0, 1) \underset{GIL}{<} (0, 2, 0)$$

As usual, we write $\alpha \leqslant \beta$ instead of ($\alpha < \beta$ or $\alpha = \beta$).

All expressions like maximum, minimum, smaller, ... refer to this ordering.

1.3. LEMMA. a) *Each* $\alpha \in \mathbf{N}^n$ *is the smallest element in*

$$\alpha + \mathbf{N}^n := \{\alpha + \gamma \mid \gamma \in \mathbf{N}^n\}.$$

In particular: if X^α *divides* X^β, *then* $\alpha \leqslant \beta$.

b) *Every strictly descending sequence in* $\mathbf{N}^n$ *is finite. In particular, any subset in* $\mathbf{N}^n$ *contains a smallest element.*

Proof.

a) $0 < \gamma$ implies $\alpha = 0 + \alpha < \gamma + \alpha$.

b) Let $\alpha(1) > \alpha(2) > ...$ be a strictly descending sequence in $\mathbf{N}^n$. Consider the corresponding sequence $X^{\alpha(1)}, X^{\alpha(2)}, ...$ of monomials. By a) the sequence of ideals $<X^{\alpha(1)}> \subset <X^{\alpha(1)}, X^{\alpha(2)}> \subset ...$ is strictly ascending, hence finite.

1.4. With $\sum_{\alpha} c_\alpha X^\alpha$ or $\sum_{\alpha \in \mathbf{N}^n} c_\alpha X^\alpha$ we always tacitly mean that only finitely many of the coefficients c_α are different from zero.

Let $0 \neq P = \sum_{\alpha} c_\alpha X^\alpha \in R[X]$. Then we define

$\deg(P) := \max\{\alpha \in \mathbf{N}^n \mid c_\alpha \neq 0\}$ ("the degree of P"),

$\mathrm{lc}(P) := c_{\deg(P)}$ ("the leading coefficient of P") and

$\mathrm{in}(P) := \mathrm{lc}(P) X^{\deg(P)}$ ("the initial term of P").

If $A, B \subseteq \mathbf{N}^n$, then $A + B := \{\alpha + \beta \mid \alpha \in A, \beta \in B\}$.

For a subset $F \subseteq R[X]$ we define

$\deg(F) := \{\deg(P) \mid P \in F - \{0\}\}$, $\mathscr{D}(F) := \deg(F) + \mathbf{N}^n$ and

$\mathrm{in}(F) := \{\mathrm{in}(P) \mid P \in F - \{0\}\}$.

1.5. Let J be an ideal in $R[X]$, $J \neq \{0\}$.

Definition. A finite subset G of $J - \{0\}$ is a "Gröbner basis of J" iff $\mathrm{in}(G)$ generates the ideal $<\mathrm{in}(J)>$.

Remarks and examples.

1) Let R be a field. Then a finite subset G of $J - \{0\}$ is a Gröbner basis of J iff $\deg(J) = \mathscr{D}(G)\,(= \deg(G) + \mathbf{N}^n)$.

2) Gröbner bases always exist: Choose a finite generating subset $M \subseteq \mathrm{in}(J)$ of $<\mathrm{in}(J)>$. Then any finite subset G of J with $\mathrm{in}(G) \supseteq M$ is a Gröbner basis of J.

3) Not every generating subset of an ideal is a Gröbner basis: Consider the graded lexicographic ordering on $\mathbf{N}^2$. Let $P_1 := X_1^2 X_2 + X_1$ and $P_2 := X_1 X_2^2$ be elements of $\mathbf{Q}[X_1, X_2]$. Then $\{P_1, P_2\}$ is not a Gröbner basis of $J := <P_1, P_2>$, since $X_1 X_2 = X_2 P_1 - X_1 P_2 \in J$, but $X_1 X_2 \notin <X_1^2 X_2, X_1 X_2^2> = <\mathrm{in}(P_1), \mathrm{in}(P_2)>$.

4) Any finite subset of $J - \{0\}$ containing a Gröbner basis is a Gröbner basis.

5) Let J be a principal ideal. Then any finite subset of J which contains a generating element of J is a Gröbner basis of J.

6) Any set of monomials $\{c_1 X^{\alpha(1)}, \ldots, c_k X^{\alpha(k)}\} \subseteq R[X]$ is a Gröbner basis of the ideal generated by them.

1.6. Let J be an ideal in $R[X]$, $J \neq \{0\}$.

The set $\mathrm{in}(J)$ is determined by a "weight-function"

$$w: \deg(J) \to R$$
$$\delta \mapsto w(\delta),$$

where $w(\delta)$ is a generating element of the (principal) ideal

$$<\mathrm{lc}(P) \mid P \in J, \deg(P) = \delta> .$$

So for $n = 2$ we can visualize $\mathrm{in}(J)$ by a figure of the following form:

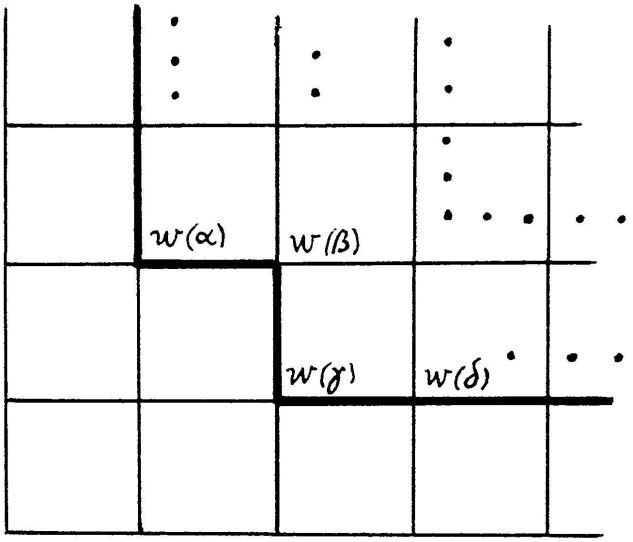

FIGURE 1.

For example, to $<2X_1, 3X_2> \subseteq \mathbf{Z}[X_1, X_2]$ corresponds figure 2.

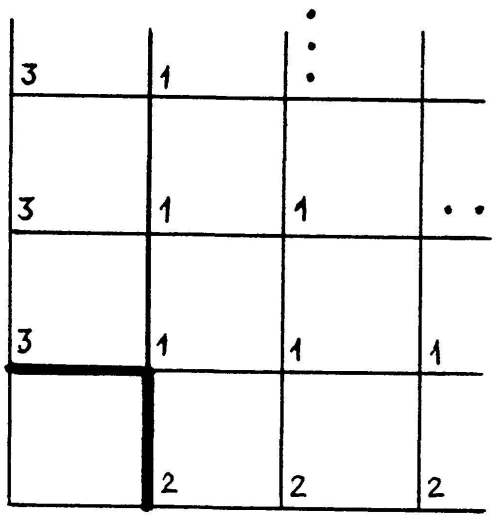

FIGURE 2.

If R is a field, then $w: \deg(J) \to R$ is a "weight function".

$$\delta \mapsto 1$$

So the corresponding figure is of the form

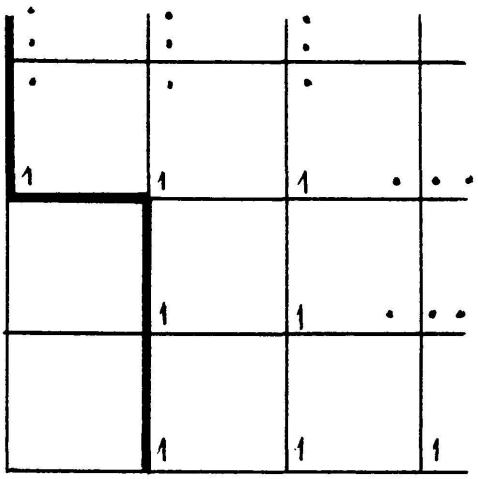

FIGURE 3.

2. THE DIVISION ALGORITHM

Let F be a finite subset of $R[X] - \{0\}$.

2.1. *Definition.* An "admissible combination of F" is an expression of the form $L := \sum_{\gamma \in \mathbf{N}^n,\, P \in F} c(\gamma, P) X^\gamma P$, $c(\gamma, P) \in R$, such that

$$\deg(L) = \max\{\deg(X^\gamma P) \mid c(\gamma, P) \neq 0\}.$$

Example. Let $P, Q \in R[X]$ and let $\alpha, \beta \in \mathbf{N}^n$. Then $X^\alpha P - X^\beta Q$ is an admissible combination of $\{P, Q\}$ iff $X^\alpha \cdot \operatorname{in}(P) \neq X^\beta \cdot \operatorname{in}(Q)$.

Remark. For every $Q \in <\operatorname{in}(F)>$ there is an admissible combination L of F such that $\operatorname{in}(L) = \operatorname{in}(Q)$. L can be calculated in the following way:

Let $F' := \{P \in F \mid \deg(Q) - \deg(P) \in \mathbf{N}^n\}$. Then

$$Q \in <\operatorname{in}(F')> \quad \text{and} \quad \operatorname{lc}(Q) \in {}_R<\operatorname{lc}(P) \mid P \in F'>.$$

For $P \in F'$ we calculate elements $c(P) \in R$ such that $\operatorname{lc}(Q) = \sum_{P \in F'} c(P) \operatorname{lc}(P)$.

Set $L := \sum_{P \in F'} c(P) X^{\deg(Q) - \deg(P)} P$.

Example: $F := \{5X_1 + 1, 3X_2 + 2\}$, $Q := X_1^2 X_2^3$.

Then $L = -X_1 X_2^3 (5X_1 + 1) + 2X_1^2 X_2^2 (3X_2 + 2)$.

2.2. PROPOSITION. *Every* $Q \in R[X] - \{0\}$ *may be written as* $Q = L + \bar{Q}$ *with the following properties:*

If $\mathrm{in}(Q) \notin <\mathrm{in}(F)>$, *then* $L = 0$ *and* $Q = \bar{Q}$.

If $\mathrm{in}(Q) \in <\mathrm{in}(F)>$, *then* L *is an admissible combination of* F *with* $\mathrm{in}(L) = \mathrm{in}(Q)$, *and either* $\bar{Q} = 0$ *or* $\mathrm{in}(\bar{Q}) \notin <\mathrm{in}(F)>$.

L and $\bar{Q}$ can be found in a finite number of steps by the following algorithm:

$$Q_0 := Q;$$

For $k \in \mathbf{N}$ assume that Q_k has already been defined. If $\mathrm{in}(Q_k) \in <\mathrm{in}(F)>$, we define $Q_{k+1} := Q_k - L_k$, where L_k is an admissible combination of F with $\mathrm{in}(L_k) = \mathrm{in}(Q_k)$.

If $Q_k = 0$ or $\mathrm{in}(Q_k) \notin <\mathrm{in}(F)>$, then $L := \sum_{j=0}^{k-1} L_j$ and $\bar{Q} := Q_k$.

Proof. We only have to show that there is a number $k \in \mathbf{N}$ such that $\mathrm{in}(Q_k) \notin <\mathrm{in}(F)>$ or $Q_k = 0$.

If $\mathrm{in}(Q_j) \in <\mathrm{in}(F)>$, then $\deg(Q_j) > \deg(Q_{j+1})$, so the assertion follows from the lemma 1.3.

2.3. *Definition.* The algorithm above is called "division by F", the polynomial $\bar{Q}$ (or, more precisely, $\bar{Q}^F$) is "a rest of Q after division by F".

Remarks.

1) Even if the strict ordering $<$ is fixed, $\bar{Q}$ depends on the choice of the L_k's in the algorithm. Hence $\bar{Q}$ is in general not uniquely determined by Q and F.

2) If a rest of Q after division by F is zero, then Q belongs to the ideal generated by F. In general the inverse is not true.

2.4. *Example.* Consider the graded lexicographic ordering and

$$P_1 := 2X_1^2 + X_1X_2, \quad P_2 := 3X_2^2 + X_1 \in \mathbf{Z}[X_1, X_2].$$

Let F be $\{P_1, P_2\}$ and let $Q := 2X_1^3X_2^3 + X_1X_2$. Then $Q_0 = Q$.

$$L_0 := 2X_1^3X_2P_2 - 2X_1X_2^3P_1,$$
$$Q_1 := Q_0 - L_0 = -2X_1^2X_2^4 + 2X_1^4X_2 + X_1X_2.$$
$$L_1 := -2X_1^2X_2^2P_2 + 2X_2^4P_1,$$
$$Q_2 := Q_1 - L_1 = -2X_1X_2^5 + 2X_1^4X_2 + 2X_1^3X_2^2 + X_1X_2.$$

Now $\text{in}(Q_2) \notin <\text{in}(F)>$, therefore $Q = L_0 + L_1 + Q_2$.

See figure 4.

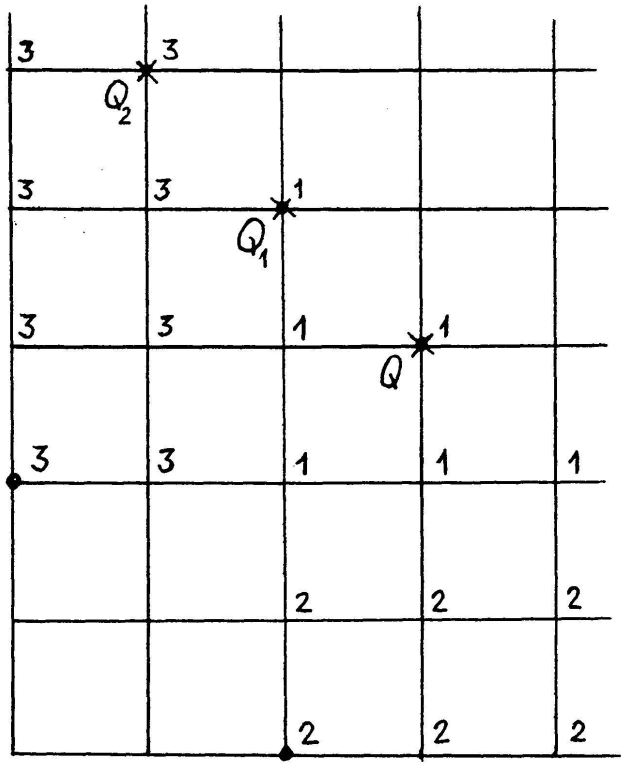

FIGURE 4.

But if we choose $L_0' := X_1 X_2^3 P_1$, then

$$Q_1' := Q_0 - L_0' = -X_1^2 X_2^4 + X_1 X_2,$$
$$L_1' := -X_1^2 X_2^2 P_2 + X_2^4 P_1$$
$$Q_2' := Q_1' - L_1' = -X_1 X_2^5 + X_1^3 X_2^2 + X_1 X_2,$$
$$\text{therefore} \quad Q = L_0' + L_1' + Q_2'.$$

So Q_2 and Q_2' are rests of Q after division by F and $Q_2 \neq Q_2'$.

2.5. PROPOSITION. *Let J be an ideal in $R[X]$ containing F. Then the following conditions are equivalent:*

(1) *F is a Gröbner basis of J.*

(2) *For every $Q \in J$, each rest of Q after division by F is zero.*

(3) *For every $Q \in J$, a rest of Q after division by F is zero.*

Proof.

(1) $\Rightarrow$ (2): Division of $Q \in J$ by F yields $Q = L + \bar{Q}$ with $\bar{Q} = 0$ or $\text{in}(\bar{Q}) \notin <\text{in}(F)>$. Now $L \in J$ and $Q \in J$ imply $\bar{Q} \in J$. Since $<\text{in}(J)> = <\text{in}(F)>$, $\bar{Q}$ must be zero.

(2) $\Rightarrow$ (3): trivial.

(3) $\Rightarrow$ (1): By (3) we have $\mathrm{in}(Q) \in <\mathrm{in}(F)>$ for every $Q \in J - \{0\}$. Hence $<\mathrm{in}(J)> = <\mathrm{in}(F)>$.

2.6. COROLLARY. *Let F be a Gröbner basis of an ideal $J \leqslant R[X]$.*

1) *F generates J.*

2) *Let $Q \in R[X]$. Then $Q \in J$ iff a rest of Q after dividing by F is zero.*

Proof. Obvious.

2.7. Another caracterisation of Gröbner bases can be given as follows:

We shall say that a set $\{L_\alpha \mid \alpha \in \mathscr{D}(F)\}$ of admissible combinations of F (with pairwise different degrees) is an "F-admissible set", if for all α we have $\deg(L_\alpha) = \alpha$ and $\mathrm{lc}(L_\alpha)$ generates the ideal

$$_R<\mathrm{lc}(P) \mid P \in <\mathrm{in}(F)>, \deg(P) = \alpha> .$$

Any F-admissible set is R-linearly independent.

If R is a field the condition on $\mathrm{lc}(L_\alpha)$ is superfluous.

PROPOSITION. *Let J be an ideal in $R[X]$ containing F. Then the following conditions are equivalent:*

(1) *F is a Gröbner basis of J.*

(2) *There is an F-admissible set which is a R-basis of J.*

(3) *Every F-admissible set is a R-basis of J.*

Proof. Let $\{L_\alpha \mid \alpha \in \mathscr{D}(F)\}$ be a F-admissible set.

(1) $\Rightarrow$ (3): Let Q be an element of $J - \{0\}$. Division of Q by $\{L_{\deg(Q)}\}$, of its rest $\bar{Q}$ by $\{L_{\deg(\bar{Q})}\}$, ... yields in a finite number of steps an expression of Q as R-linear combination of L_α's.

(3) $\Rightarrow$ (2): trivial.

(2) $\Rightarrow$ (1): Suppose that $\{L_\alpha \mid \alpha \in \mathscr{D}(F)\}$ is a R-basis of J. For every $Q \in J - \{0\}$ the initial term of $L_{\deg(Q)}$ divides $\mathrm{in}(Q)$, hence $\mathrm{in}(Q) \in <\mathrm{in}(F)>$.

3. CONSTRUCTION OF GRÖBNER BASES

3.1. *Definition.* Let P, Q be elements of $R[X]$, let $\alpha, \beta \in \mathbf{N}^n$ and let $a, b \in R$. Then the polynomial

$$S(P, Q) := aX^{\alpha}P - bX^{\beta}Q$$

is called a "*S*(ubtraction)-polynomial of P, Q" iff

$$\alpha + \deg(P) = \beta + \deg(Q) = \min(\mathscr{D}(\{P\}) \cap \mathscr{D}(\{Q\}))$$

and $\operatorname{lc}(P) \cdot a = \operatorname{lc}(Q) \cdot b =$ a least common multiple of $\operatorname{lc}(P)$ and $\operatorname{lc}(Q)$.

3.2. *Example.* Consider the graded lexicographic ordering on $\mathbf{N}^2$ and

$$P := 6X_1^3X_2 + 1, \quad Q := 8X_1X_2^2 + 3X_1X_2 + X_2 \in \mathbf{Z}[X_1, X_2].$$

Then

$$4X_2P - 3X_1^2Q = -9X_1^3X_2 - 3X_1^2X_2 + 4X_2 \quad \text{and} \quad -4X_2P + 3X_1^2Q$$

are *S*-polynomials of P, Q.

See figure 5.

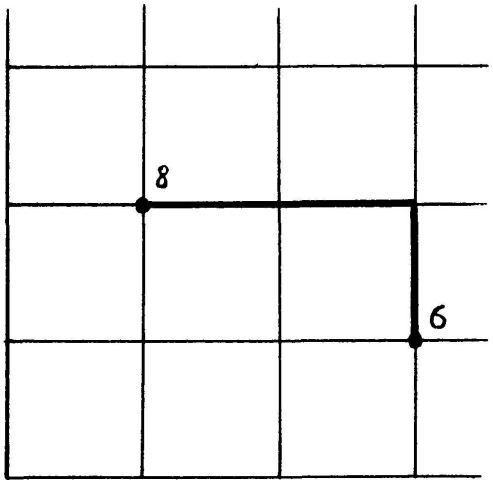

FIGURE 5.

3.3 *Remark.* For $P, Q \in R[X]$, $S(P, Q)$ as defined above is unique up to multiplication by an invertible element of R. Therefore we shall call it "the" *S*-polynomial of P, Q.

3.4. LEMMA. *Let* $P_1, \ldots, P_k \in R[X]$, $c_1, \ldots, c_k \in R$ *such that* $\deg(P_1) = \ldots = \deg(P_k) =: \delta$ *but* $\deg(\sum_{i=1}^{k} c_iP_i) \neq \delta$.

Then $\sum_{i=1}^{k} c_iP_i$ *is a R-linear combination of the S-polynomials* $S(P_i, P_j)$, $1 \leqslant i, j \leqslant k$.

Proof. By induction on k.

Let $l_i := \operatorname{lc}(P_i)$, $1 \leqslant i \leqslant k$. Then $\sum_{i=1}^{k} c_il_i = 0$.

It is sufficient to prove the existence of $a_{ij}, b_{ij} \in R$ such that

$$\sum_{i=1}^{k} c_i P_i = \sum_{1 \leqslant i,j \leqslant k} (a_{ij} P_i - b_{ij} P_j) \quad \text{and} \quad a_{ij} l_i = b_{ij} l_j, \quad 1 \leqslant i,j \leqslant n .$$

For $k = 2$ we have $c_1 P_1 + c_2 P_2 = c_1 P_1 - (-c_2) P_2$ and $c_1 l_1 = (-c_2) l_2$. $k = 3$: Let l be a greatest common divisor of l_1, l_2, l_3. Since $c_2 l_2 = -c_1 l_1 - c_3 l_3$, a greatest common divisor of l_1 and l_3 divides $c_2 l$. Hence there are elements $x_2, x_3 \in R$ such that $c_2 l = x_1 l_1 + x_3 l_3$.

Then $d_1 := (-x_1 l_2 - c_1 l)/l$, $d_2 := (-x_1 l_1)/l$, $d_3 := (x_3 l_2)/l$ are elements of R. Furthermore, we have

$$\begin{aligned} (c_1 + d_1) l_1 &= d_2 l_2 \\ (c_2 + d_2) l_2 &= d_3 l_3 \\ (c_3 + d_3) l_3 &= d_1 l_1 \quad \text{and} \end{aligned}$$

$$\sum_{i=1}^{3} c_i P_i = [(c_1 + d_1) P_1 - d_2 P_2] + [(c_2 + d_2) P_2 - d_3 P_3] + [(c_3 + d_3) P_3 - d_1 P_1] .$$

$k > 3$: Let $Q := \sum_{i=3}^{k} c_i P_i$ and $m := \sum_{i=3}^{k} c_i l_i$.

If $m = 0$, we can apply the induction hypothesis to Q.

If $m \neq 0$, by the $k = 3$ case there are $d_1, d_2, d_3 \in R$ such that

$$c_1 P_1 + c_2 P_2 + Q = [(c_1 + d_1) P_1 - d_2 P_2] + [(c_2 + d_2) P_2 - d_3 Q] + [(1 + d_3) Q - d_1 P_1]$$

and $(c_1 + d_1) l_1 = d_2 l_2$, $(c_2 + d_2) l_2 = d_3 m$, $(1 + d_3) m = d_1 l_1$.

Therefore, we can apply the induction hypothesis to $(c_2 + d_2) P_2 - \sum_{i=3}^{k} d_3 c_i P_i$ and to $-d_1 P_1 + \sum_{i=3}^{k} (1 + d_3) c_i P_i$ and thus terminate the proof.

Remark. If R is a field, the proof is trivial: Let $l_i := \mathrm{lc}(P_i)$ and

$$P_i' := (P_i/l_i),\ 1 \leqslant i \leqslant k, \quad \text{then} \quad \sum_{i=1}^{k} c_i P_i = c_1 l_1 (P_1' - P_2') + (c_1 l_1 + c_2 l_2)(P_2' - P_3') + \ldots + (\sum_{i=1}^{k-1} c_i l_i)(P_{k-1}' - P_k') .$$

3.5. THEOREM. *Let* J *be an ideal of* $R[X]$ *generated by a finite subset* $F \subseteq R[X] - \{0\}$.

Then the following assertions are equivalent:

(1) F *is a Gröbner basis of* J.

(2) *For all* $P, Q \in F$ *a rest of* $S(P, Q)$ *after division by* F *is zero.*

Proof.

(1) $\Rightarrow$ (2): Let $P, Q \in F$. Then $S(P, Q)$ and its rest after division by F are elements of J. Therefore, this implication is a special case of proposition 2.5., (1) $\Rightarrow$ (2).

(2) $\Rightarrow$ (1): Let $A \in J - \{0\}$. We have to show that $\text{in}(A) \in <\text{in}(F)>$. Since J is generated by F, there are elements $c(\gamma, P) \in R$ such that $A = \sum_{P \in F, \gamma \in \mathbf{N}^n} c(\gamma, P) X^\gamma P$.

Let $\delta := \max\{\gamma + \deg(P) \mid c(\gamma, P) \neq 0\}$ and $L := \sum_{\substack{\gamma, P \\ \gamma, \deg(P) = \delta}} c(\gamma, P) X^\gamma P$.

By lemma 1.3. we may assume that δ is minimal, i.e.:

if $A = \sum_{P \in F, \gamma \in \mathbf{N}^n} d(\gamma, P) X^\gamma P$ then $\delta \leqslant \max\{\gamma + \deg(P) \mid d(\gamma, P) \neq 0\}$.

Suppose that $\deg(L) < \delta$. Then the lemma above yields

$$L = \sum_{P, Q \in F, \alpha \in \mathbf{N}^n} a(\alpha, P, Q) X^\alpha S(P, Q), \quad a(\alpha, P, Q) \in R$$

(note that for $\beta, \gamma \in \mathbf{N}^n$ there is an $\alpha \in \mathbf{N}^n$ such that $S(X^\beta P, X^\gamma Q) = X^\alpha S(P, Q)$).

But according to (2) the S-polynomials are admissible combinations of F and clearly the same holds for the $X^\alpha S(P, Q)$'s. Since their degree is smaller than δ, this is a contradiction to the minimality of δ. Hence $\deg(L) = \delta$. But then $\text{in}(A) = \text{in}(L) \in <\text{in}(F)>$.

3.6. THEOREM. *Let* J *be the ideal generated by* F. *Then a Gröbner basis of* J *can be constructed (in a finite number of steps) by the following algorithm:*

$$F_0 := F$$

$$F_{i+1} := F_i \cup (\{\overline{S(P, Q)} \mid P, Q \in F_i\} - \{0\})$$

($\overline{S(P, Q)}$ *is a rest of* $S(P, Q)$ *after division by* F_i). *If* $F_i = F_{i+1}$, *then* F_i *is a Gröbner basis of* J.

Proof. By the preceding theorem we only have to show that there is a $k \in \mathbf{N}$ such that $F_k = F_{k+1}$.

If $F_i \subset F_{i+1}$ then $<\text{in}(F_i)> \subset <\text{in}(F_{i+1})>$. Since the strictly ascending sequence $<\text{in}(F_0)> \subset <\text{in}(F_1)> \subset \ldots$ must be finite, there is a $k \in \mathbf{N}$ with $F_k = F_{k+1}$.

3.7. *Example.* Consider the graded lexicographic ordering on $\mathbf{N}^2$ and

$$F := \{P_1 := 2X_1X_2^2 - X_1, P_2 := 3X_1^2X_2 - X_2\} \subseteq \mathbf{Z}[X_1, X_2].$$

Then

$$F_0 = F \quad \text{and} \quad S(P_1, P_2) = 3X_1P_1 - 2X_2P_2 = -3X_1^2 + 2X_2^2$$
$$= \overline{S(P_1, P_2)} =: P_3.$$

So

$$F_1 = \{P_1, P_2, P_3\} \quad \text{and} \quad \overline{S(P_1, P_2)}^{F_1} = 0,$$

$$\overline{S(P_1, P_3)}^{F_1} = 4X_2^4 - 3X_1^2 =: P_4, \quad \overline{S(P_2, P_3)}^{F_1} = 2X_2^3 - X_2 =: P_5.$$

Therefore $F_2 = \{P_1, P_2, P_3, P_4, P_5\}$ and all rests after division by F_2 of S-polynomials are 0. Hence F_2 is a Gröbner basis of the ideal generated by F.

See figure 6.

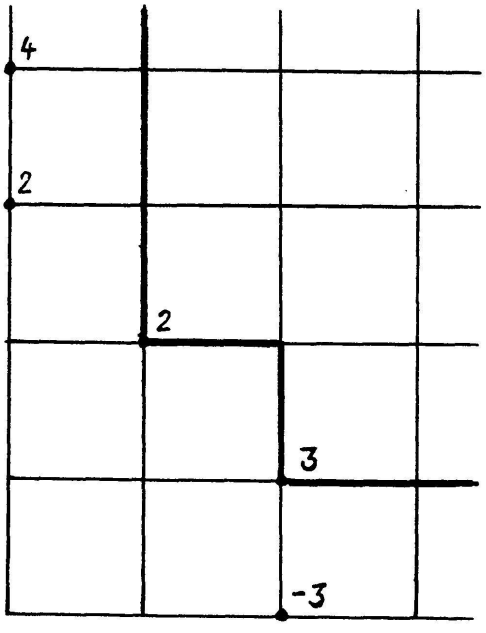

FIGURE 6.

3.8. *Remark.* Let G be a Gröbner basis of an ideal J. We shall say that G is "simplified" if all $P \in G$ fulfill the following two conditions:

$$\mathrm{lc}(P) \text{ generates the ideal } {}_R\langle \mathrm{lc}(Q) \mid Q \in J, \deg(Q) = \deg(P)\rangle$$

and

$$\mathrm{in}(P) \notin \langle \mathrm{in}(G - \{P\})\rangle .$$

It is easy to see that the elements of a simplified Gröbner basis have pairwise different degrees.

If R is a field then G is simplified iff the elements of G have pairwise different degrees and $\deg(G)$ is the set of minimal elements (with respect to the natural partial ordering on $\mathbf{N}^n$) in $\deg(J)$.

If G is not simplified, then in the following way we can construct (in a finite number of steps) a simplified Gröbner basis of J:

For every $P \in G$ choose an admissible combination P' of G such that $\deg(P) = \deg(P')$ and $\mathrm{lc}(P')$ generates the ideal

$${}_R\langle \mathrm{lc}(Q) \mid Q \in J, \deg(Q) = \deg(P)\rangle .$$

Then $G' := \{P' \mid P \in G\}$ is a Gröbner basis of J, since $\langle \mathrm{in}(J)\rangle = \langle \mathrm{in}(G)\rangle \subseteq \langle \mathrm{in}(G')\rangle \subseteq \langle \mathrm{in}(J)\rangle$.

If there is a $P' \in G'$ with $\mathrm{in}(P') \in \langle \mathrm{in}(G' - \{P'\})\rangle$, then $G' - \{P'\}$ is a Gröbner basis, since then $\langle \mathrm{in}(G' - \{P'\})\rangle = \langle \mathrm{in}(G')\rangle = \langle \mathrm{in}(J)\rangle$.

Replace G' by $G' - \{P'\}$. After finitely many eliminations of this kind we obtain a simplified Gröbner basis.

In example 3.7. the Gröbner basis F_2 is not simplified, since $\mathrm{in}(P_2) = -X_2 \mathrm{in}(P_3)$ and $\mathrm{in}(P_4) = 2X_2 \mathrm{in}(P_5)$. $\{P_1, P_3, P_5\}$ is a simplified Gröbner basis of the ideal generated by F_2.

4. Application to Systems of Algebraic Equations

Let J be an ideal in $R[X]$, generated by a subset $F \neq \{0\}$.

4.1. We may consider F as a system of algebraic equations in n variables. We denote by K an algebraic closure of the quotient field of R.

Let $Z(F)$ (resp. $Z_K(F)$) be the set $\{z \in R^n \text{ (resp. } K^n) \mid P(z) = 0 \text{ for all } P \in F\}$ of common zeros in R^n (resp. K^n) of the elements of F. Clearly $Z(F) = Z(J)$ and $Z_K(F) = Z_K(J)$.

4.2. PROPOSITION. *Let G be a Gröbner basis of J.*

1) *$Z_K(J) = \emptyset$ iff $G \cap R \neq \emptyset$.*

2) *The set $Z_K(J)$ is finite iff $\mathbf{N}^n - \mathscr{D}(G)$ is finite. In this case the cardinality of $Z_K(J)$ is smaller than or equal to the cardinality of $\mathbf{N}^n - \mathscr{D}(G)$.*

Proof.

1) By Hilbert's Nullstellensatz we know:

$Z_K(J) = \emptyset$ iff $J \cap R \neq \emptyset$. Therefore $Z_K(J) = \emptyset$ implies $0 \in \deg(J)$, hence $G \cap R \neq \emptyset$.

2) Let I be the ideal generated by J in $K[X]$. Then F is a Gröbner basis of I, too. Again by Hilbert's Nullstellensatz the dimension (as K-vector space) of $K[X]/I$ is an upper bound for the cardinality of $Z_K(J) = Z_K(I)$, and this dimension is finite iff $Z_K(J)$ is so. Since G is a Gröbner basis of I, one easily verifies that the residue classes $X^\alpha + I$, $\alpha \in \mathbf{N}^n - \mathscr{D}(G)$, form a K-basis of $K[X]/I$. This proves the proposition.

4.3. PROPOSITION. *Let G be a Gröbner basis of J with respect to the lexicographic ordering (see 1.2.).*

If $J \cap R[X_k, ..., X_n] \neq \{0\}$, then

$$G_k := G \cap R[X_k, ..., X_n]$$

is a Gröbner basis of

$$J_k := J \cap R[X_k, ..., X_n];$$

in particular, G_k generates the ideal $J_k \leqslant R[X_k, ..., X_n]$ $(1 \leqslant k \leqslant n)$.

Proof. Let $Q \in J_k$. For any $P \in R[X]$ with $\deg(P) \leqslant \deg(Q)$ we have $P \in R[X_k, ..., X_n]$, since $<$ is the lexicographic ordering. By 2.2. and 2.5. there are $c(\alpha, P) \in R$ such that $Q = \sum_{P \in G,\, \alpha \in \mathbf{N}^n} c(\alpha, P) X^\alpha P$ and $c(\alpha, P) \neq 0$ implies $\deg(X^\alpha P) \leqslant \deg(Q)$.

Hence we have $X^\alpha P \in R[X_k, ..., X_n]$ for $c(\alpha, P) \neq 0$, and, by 2.5. again, G_k is a Gröbner basis of J_k.

4.4. Now we can apply the theory of Gröbner bases to find the solutions to the system F of algebraic equations. Consider the following algorithm:

First we construct a Gröbner basis G of J with respect to the lexicographic ordering (see 3.6.). As in 4.3. we write G_k for $G \cap R[X_k, ..., X_n]$, $1 \leqslant k \leqslant n$.

Compute the greatest common divisor P_n of the (univariate) polynomials in G_n. Find a zero $a_n \in R$ of P_n. If P_n has no zero in R, then $Z(J) = \emptyset$.

Let $k \in \{1, ..., n-1\}$. Suppose that $a_{k+1}, ..., a_n \in R$ have already been found. Let $G_k(a_{k+1}, ..., a_n) \subseteq R[X_k]$ be the set of polynomials in one variable X_k obtained from G_k by substituting everywhere a_j for X_j, $k+1 \leqslant j \leqslant n$.

Compute the greatest common divisor P_k of the polynomials in $G_k(a_{k+1}, ..., a_n)$. Find a zero $a_k \in R$ of P_k. If P_k has no zero in R, we have to go back to G_n and to find another sequence $a'_n, ..., a'_{k+1}$.

If we obtain $(a_1, ..., a_n)$ by this algorithm, it is an element of $Z(J)$. By 4.3. all elements of $Z(J)$ can be computed in this way.

Suppose that $Z_K(J)$ is finite (i.e. $\mathbf{N}^n - \mathscr{D}(G)$ is finite) and that we are able to solve univariate polynomial equations in R (which is the case for $R = \mathbf{Z}$). Then the algorithm above yields $Z(J)$ in a finite number of steps.

4.5. *Example.* Let F be the subset

$$\{2X_1^4+3X_1^3X_2X_3-X_1X_2^2+5X_1-3X_2^2-5X_2X_3-2X_3+41,$$
$$4X_1^4+6X_1^3X_2X_3-2X_1X_2^2+10X_1+3X_2^2+5X_2X_3+2X_3^3-11X_3^2+19X_3+25,$$
$$6X_2^2+10X_2X_3+2X_3^3-11X_3^2+21X_3-40\} \quad \text{of} \quad \mathbf{Z}[X_1, X_2, X_3].$$

By the algorithm 3.6. we get a Gröbner basis G of the ideal generated by F:

$$\begin{aligned} G = \{&2X_3^3-11X_3^2+17X_3-6, \\ &3X_2^2+5X_2X_3+2X_3-17, \\ &2X_1^4+3X_1^3X_2X_3-X_1X_2^2+5X_1+24\}. \end{aligned}$$

Now $Z(G_3) = \{2, 3\}$, $Z(G_2(2)) = \{1\}$, $Z(G_2(3)) = \emptyset$ and $Z(G_1(1, 2)) = \{-2\}$. So $Z(F) = \{(-2, 1, 2)\}$.

5. Application to a Geometric Problem

5.1. For $P \in R[X]$ let $\tilde{P}$ be the homogeneization of P by a further variable X_{n+1}. For an ideal $J \leqslant R[X]$ we write $\tilde{J}$ for the ideal generated by $\{\tilde{P} \mid P \in J\}$ in $R[X_1, ..., X_{n+1}]$.

Proposition. *Let G be a Gröbner basis of J with respect to the graded inverse lexicographic ordering (see 2.1.). Then $\tilde{G} := \{\tilde{P} \mid P \in G\}$ is a Gröbner basis of $\tilde{J}$.*

Proof. Since we consider the graded inverse lexicographic ordering, we have for all $P \in R[X] - \{0\}$: $\mathrm{in}(P) = \mathrm{in}(\tilde{P})$. Hence $<\mathrm{in}(\tilde{J})> = <\mathrm{in}(J)> = <\mathrm{in}(G)> = <\mathrm{in}(\tilde{G})>$.

5.2. *Example.* Let R be a field. Consider the "twisted cubic"

$$Z := \{(t, t^2, t^3) \mid t \in R\} \subseteq R^3 .$$

Then

$$J := <X_1^3 - X_3, X_1^2 - X_2> \leqslant R[X_1, X_2, X_3]$$

is the ideal of polynomials vanishing on Z.

Recall that the set of zeroes of $\tilde{J}$ in the projective space $\mathbf{P}_3(R)$ is the closure (with respect to the Zariski topology) of Z.

The polynomials $X_1^3 - X_3X_4^2$ and $X_1^2 - X_2X_4$ do *not* generate the ideal $\tilde{J} \leqslant R[X_1, X_2, X_3, X_4]$.

By 3.6. $G := \{X_1^2 - X_2, X_1X_2 - X_3, X_2^2 - X_1X_3\}$ is a Gröbner basis of J with respect to the graded inverse lexicographic ordering. Hence $\tilde{J}$ is generated by $\{X_1^2 - X_2X_4, X_1X_2 - X_3X_4, X_2^2 - X_1X_3X_4\}$.

REFERENCES

[Ba] BAYER, D. An Introduction to the Division Algorithm. Preprint 1985.

[B] BUCHBERGER, B. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. In: Bose, N. (ed.), *Multidimensional Systems Theory*, pp. 184-232. Reidel Publ. Comp., Dordrecht 1985.

[E] ELIAHOU, S. Minimal Syzygies of Monomial Ideals and Gröbner Bases. Preprint 1987.

[K1] KANDRI-RODY, A. and D. KAPUR. Computing the Gröbner Basis of an Ideal in Polynomial Rings over the Integers. In: *Proceedings of Third MACSYMA Users Conference.* Schenectady, New York, 1984, pp. 436-451.

[K2] KANDRI-RODY, A. and D. KAPUR. *An Algorithm for Computing the Gröbner Basis of a Polynomial Ideal over a Euclidian Ring.* Report No. 84CRD045, General Electric Research and Development Center, Schenectady, New York, 1984.

[L] LAZARD, D. Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations. In: H. van Hulzen (ed.), *Proceedings of the EUROCAL 83*. Lecture Notes in Computer Science 162, Springer, Berlin 1983, pp. 146-156.

[LJ] LEJEUNE-JALABERT, M. *Effectivité de calculs polynomiaux*. Cours de D.E.A., Université de Grenoble. 140 pages, Grenoble 1986.

[MM] MÖLLER, M. and F. MORA. New Constructive Methods in Classical Ideal Theory. *Journal of Algebra 100 (1986), 138-178.*

[T] TRINKS, W. Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *Journal of Number Theory 10* (1978), 475-488.

See also the literature cited in these articles.

(Reçu le 20 juillet 1987)

Franz Pauer
Marlene Pfeifhofer

Institut für Mathematik
Universität Innsbruck
Technikerstrasse 25
A-6020 Innsbruck (Austria)