3. Construction of Gröbner Bases

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.05.2024**

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

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

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 $\operatorname{lc}(L_\alpha)$ generates the ideal

$$_R\langle \operatorname{lc}(P) \mid P \in \langle \operatorname{in}(F) \rangle, \deg(P) = \alpha \rangle .$$

Any F-admissible set is R-linearly independent.
If R is a field the condition on $\operatorname{lc}(L_\alpha)$ 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 $\operatorname{in}(Q)$, hence $\operatorname{in}(Q) \in \langle \operatorname{in}(F) \rangle$.

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

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.

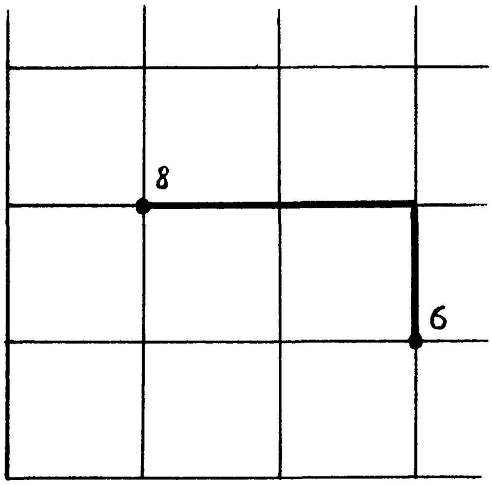

FIGURE 5.

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 $l_i := \mathrm{lc}(P_i)$, $1 \leqslant i \leqslant k$. 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

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

$$\text{and} \quad (c_1 + d_1) l_1 = d_2 l_2, \quad (c_2 + d_2) l_2 = d_3 m, \quad (1 + d_3) m = d_1 l_1.$$

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 $P'_i := (P_i / l_i)$, $1 \leqslant i \leqslant k$, then

$$\sum_{i=1}^{k} c_i P_i = c_1 l_1 (P'_1 - P'_2) + (c_1 l_1 + c_2 l_2)(P'_2 - P'_3) + \dots + \Big(\sum_{i=1}^{k-1} c_i l_i\Big)(P'_{k-1} - P'_k).$$

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 $\operatorname{in}(A) \in \langle \operatorname{in}(F) \rangle$. 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 $\operatorname{in}(A) = \operatorname{in}(L) \in \langle \operatorname{in}(F) \rangle$.

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 $<\mathrm{in}(F_i)> \subset <\mathrm{in}(F_{i+1})>$. Since the strictly ascending sequence $<\mathrm{in}(F_0)> \subset <\mathrm{in}(F_1)> \subset \ldots$ 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.

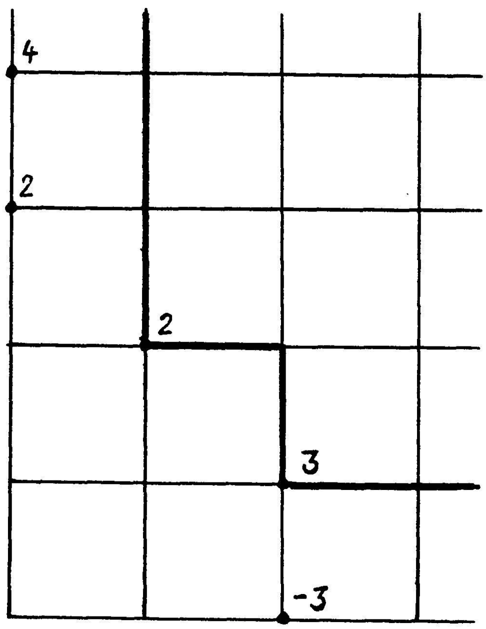

FIGURE 6.

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 $Z_K(F) = Z_K(J)$.