2. The Division Algorithm

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **24.09.2024**

If R is a field, then $\begin{array}{l} w\colon \deg(J) \to R \\ \delta \mapsto 1 \end{array}$ is a "weight function".

So the corresponding figure is of the form

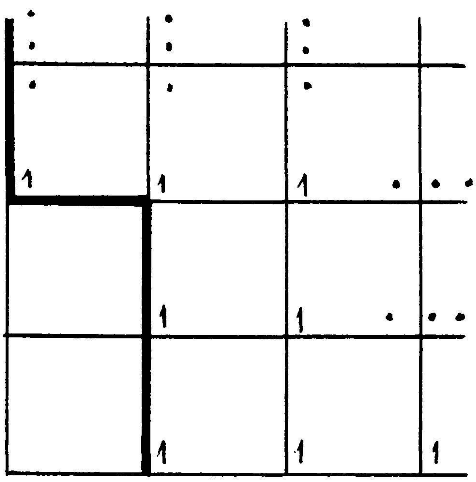

FIGURE 3.

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 $X^\alpha \cdot \mathrm{in}(P) \neq X^\beta \cdot \mathrm{in}(Q)$.

Remark. For every $Q \in <\mathrm{in}(F)>$ there is an admissible combination L of F such that $\mathrm{in}(L) = \mathrm{in}(Q)$. L can be calculated in the following way: Let $F' := \{P \in F \mid \deg(Q) - \deg(P) \in \mathbf{N}^n\}$. Then

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

For $P \in F'$ we calculate elements $c(P) \in R$ such that $\mathrm{lc}(Q) = \sum_{P \in F'} c(P)\,\mathrm{lc}(P)$. 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 $\mathrm{in}(Q) \notin \langle \mathrm{in}(F) \rangle$, *then* $L = 0$ *and* $Q = \bar{Q}$.

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

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 $\mathrm{in}(Q_k) \in \langle \mathrm{in}(F) \rangle$, 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 $\mathrm{in}(Q_k) \notin \langle \mathrm{in}(F) \rangle$, 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 $\mathrm{in}(Q_k) \notin \langle \mathrm{in}(F) \rangle$ or $Q_k = 0$.

If $\mathrm{in}(Q_j) \in \langle \mathrm{in}(F) \rangle$, 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 in $(Q_2) \notin \langle \mathrm{in}(F) \rangle$, therefore $Q = L_0 + L_1 + Q_2$.

See figure 4.

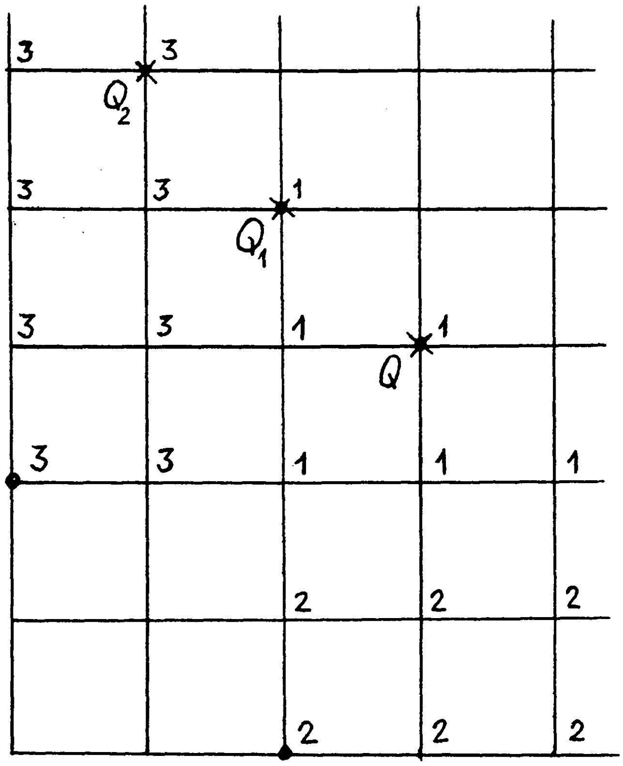

FIGURE 4.

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 $\mathrm{in}(\bar{Q}) \notin \langle \mathrm{in}(F) \rangle$. Now $L \in J$ and $Q \in J$ imply $\bar{Q} \in J$. Since $\langle \mathrm{in}(J) \rangle = \langle \mathrm{in}(F) \rangle$, $\bar{Q}$ must be zero.

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

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

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

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

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

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