

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 34 (1988)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE THEORY OF GRÖBNER BASES
Autor: Pauer, Franz / Pfeifhofer, Marlene
Kapitel: 2. The Division Algorithm
DOI: <https://doi.org/10.5169/seals-56595>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 18.04.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

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

$$\delta \mapsto 1$$

So the corresponding figure is of the form

⋮	⋮	⋮	⋮
•	•	•	•
1	1	1	• • •
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•

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 $L := \sum_{\gamma \in \mathbb{N}^n, P \in F} c(\gamma, P) X^\gamma P$, $c(\gamma, P) \in R$, such that

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

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

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

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

$$Q \in \langle \text{in}(F') \rangle \quad \text{and} \quad \text{lc}(Q) \in_R \langle \text{lc}(P) \mid P \in F' \rangle.$$

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

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 $\text{in}(Q) \notin \langle \text{in}(F) \rangle$, then $L = 0$ and $Q = \bar{Q}$.

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

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 $\text{in}(Q_k) \in \langle \text{in}(F) \rangle$, we define $Q_{k+1} := Q_k - L_k$, where L_k is an admissible combination of F with $\text{in}(L_k) = \text{in}(Q_k)$.

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

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

See figure 4.

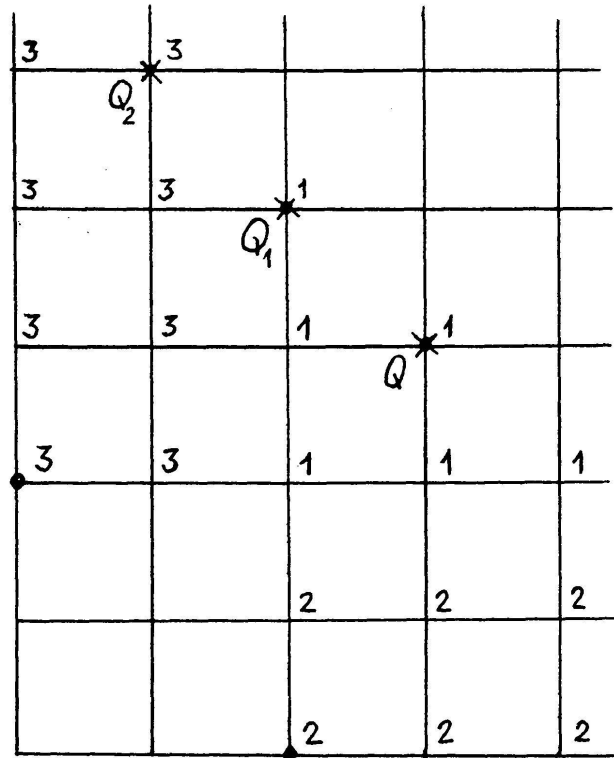


FIGURE 4.

But if we choose $L'_0 := X_1 X_2^3 P_1$, then

$$Q'_1 := Q_0 - L'_0 = -X_1^2 X_2^4 + X_1 X_2,$$

$$L'_1 := -X_1^2 X_2^2 P_2 + X_2^4 P_1$$

$$Q'_2 := Q'_1 - L'_1 = -X_1 X_2^5 + X_1^3 X_2^2 + X_1 X_2,$$

$$\text{therefore } Q = L'_0 + L'_1 + Q'_2.$$

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 $\text{in}(\bar{Q}) \notin \langle \text{in}(F) \rangle$. Now $L \in J$ and $Q \in J$ imply $\bar{Q} \in J$. Since $\langle \text{in}(J) \rangle = \langle \text{in}(F) \rangle$, \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 $J \leq R[X]$.

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 characterisation of Gröbner bases can be given as follows:

We shall say that a set $\{L_\alpha \mid \alpha \in \mathcal{D}(F)\}$ 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 $\{L_\alpha \mid \alpha \in \mathcal{D}(F)\}$ 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 $\{L_\alpha \mid \alpha \in \mathcal{D}(F)\}$ 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 $\alpha, \beta \in \mathbb{N}^n$ and let $a, b \in R$. Then the polynomial