4. Application to Systems of Algebraic Equations

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **26.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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:

$$\operatorname{lc}(P) \text{ generates the ideal } {}_R\!<\operatorname{lc}(Q) \mid Q \in J, \deg(Q) = \deg(P)>$$

and

$$\operatorname{in}(P) \notin <\operatorname{in}(G - \{P\})> .$$

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 $\operatorname{lc}(P')$ generates the ideal

$${}_R\!<\operatorname{lc}(Q) \mid Q \in J, \deg(Q) = \deg(P)> .$$

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

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

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 $\operatorname{in}(P_2) = -X_2 \operatorname{in}(P_3)$ and $\operatorname{in}(P_4) = 2X_2 \operatorname{in}(P_5)$. $\{P_1, P_3, P_5\}$ 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 $\tilde{J}$.*