

5. Application to a Geometric Problem

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **08.05.2024**

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.

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

Compute the greatest common divisor P_k of the polynomials in $G_k(a_{k+1}, \dots, a_n)$. 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 $a'_n, \dots, a'_{k+1}$.

If we obtain $(a_1, \dots, a_n)$ 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. $\mathbf{N}^n - \mathcal{D}(G)$ 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

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

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 $J \subseteq R[X]$ we write $\tilde{J}$ for the ideal generated by $\{\tilde{P} \mid P \in J\}$ in $R[X_1, \dots, X_{n+1}]$.

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 $P \in R[X] - \{0\} : \text{in}(P) = \text{in}(\tilde{P})$. Hence $\langle \text{in}(\tilde{J}) \rangle = \langle \text{in}(J) \rangle = \langle \text{in}(G) \rangle = \langle \text{in}(\tilde{G}) \rangle$.

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

$$J := \langle X_1^3 - X_3, X_1^2 - X_2 \rangle \leq R[X_1, X_2, X_3]$$

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 $\tilde{J} \leq R[X_1, X_2, X_3, X_4]$.

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.