1. Notations and Definitions

Finally, we apply the method of Gröbner bases to systems of algebraic equations and to a geometric problem:

Using the "lexicographic ordering" on $\mathbf{N}^n$, a Gröbner basis of an ideal immediately yields ideal bases of the corresponding elimination ideals (see 4.3.).

If X is an algebraic subset of the affine n-space, a Gröbner basis with respect to the "inverse lexicographic ordering" permits to obtain an ideal basis of the homogeneous ideal, which defines the Zariski-closure of X in the projective n-space (see 5.).

The method of Gröbner bases was introduced by B. Buchberger in 1965. For the history of the theory and for further applications see [B].

Our aim is to give a short and self-contained introduction to the theory of Gröbner bases. In this form it could be part of a second or third year algebra course. The results written down in this article can be found elsewhere, but we present short proofs.

We do not enter into questions of implementation or complexity of the algorithms (see for instance [B], [E], [K1], [T]).

Acknowledgements:

We thank Bruno Buchberger for sending us a long list of references.

We thank Ingrid Mittelberger for her interest and many discussions on this subject.

We thank Thierry Vust and the referee for proposing several improvements on the first version of this article.

1. Notations and Definitions

The notations introduced here will be valid throughout this article.

1.1. We denote by R a principal ideal domain (for example: $\mathbf{Z}$, a field, the polynomial ring or power series ring in one variable over a field) and by $R[X]$ the polynomial ring over R in n variables $X_1, ..., X_n$. Sometimes we make tacitly the additional assumption that we can compute a greatest common divisor of two elements in R.

If S is a subset of $R[X]$, we write $<S>$ for the ideal generated by S in $R[X]$.

Recall that $R[X]$ is a noetherian ring, this means that every strictly ascending sequence of ideals in $R[X]$ is finite.

For $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbf{N}^n$ we abbreviate $X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n}$ by X^α.

1.2. Let $<$ be a strict ordering on $\mathbf{N}^n$ which has the following two properties:

$$\forall \alpha \in \mathbf{N}^n - \{0\}, \quad 0 < \alpha;$$
$$\forall \alpha, \beta, \gamma \in \mathbf{N}^n, \quad (\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma).$$

Well-known examples for such orderings are:

the lexicographic ordering ($\alpha \underset{L}{<} \beta :\Leftrightarrow$ there is a $j \in \{1, ..., n\}$ such that $\alpha_k = \beta_k$ if $k < j$ and $\alpha_j < \beta_j$),

the graded lexicographic ordering

$$(\alpha \underset{GL}{<} \beta :\Leftrightarrow (\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i) \text{ or } ((\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i) \text{ and } \alpha \underset{L}{<} \beta)),$$

the graded inverse lexicographic ordering ($\alpha \underset{GIL}{<} \beta :\Leftrightarrow (\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i)$ or $((\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i)$ and there is a $j \in \{1, ..., n\}$ such that $\alpha_k = \beta_k$ if $k > j$ and $\alpha_j > \beta_j)$).

Examples:
$$(0, 2, 0) \underset{L}{<} (1, 0, 0) \underset{L}{<} (1, 0, 1)$$
$$(1, 0, 0) \underset{GL}{<} (0, 2, 0) \underset{GL}{<} (1, 0, 1)$$
$$(1, 0, 0) \underset{GIL}{<} (1, 0, 1) \underset{GIL}{<} (0, 2, 0)$$

As usual, we write $\alpha \leqslant \beta$ instead of ($\alpha < \beta$ or $\alpha = \beta$).

All expressions like maximum, minimum, smaller, ... refer to this ordering.

1.3. LEMMA. a) *Each* $\alpha \in \mathbf{N}^n$ *is the smallest element in*

$$\alpha + \mathbf{N}^n := \{\alpha + \gamma \mid \gamma \in \mathbf{N}^n\}.$$

In particular: if X^α *divides* X^β, *then* $\alpha \leqslant \beta$.

b) *Every strictly descending sequence in* $\mathbf{N}^n$ *is finite. In particular, any subset in* $\mathbf{N}^n$ *contains a smallest element.*

Proof.

a) $0 < \gamma$ implies $\alpha = 0 + \alpha < \gamma + \alpha$.

b) Let $\alpha(1) > \alpha(2) > ...$ be a strictly descending sequence in $\mathbf{N}^n$. Consider the corresponding sequence $X^{\alpha(1)}, X^{\alpha(2)}, ...$ of monomials. By a) the sequence of ideals $<X^{\alpha(1)}> \subset <X^{\alpha(1)}, X^{\alpha(2)}> \subset ...$ is strictly ascending, hence finite.

1.4. With $\sum_{\alpha} c_\alpha X^\alpha$ or $\sum_{\alpha \in \mathbf{N}^n} c_\alpha X^\alpha$ we always tacitly mean that only finitely many of the coefficients c_α are different from zero.

Let $0 \neq P = \sum_{\alpha} c_\alpha X^\alpha \in R[X]$. Then we define

$\deg(P) := \max\{\alpha \in \mathbf{N}^n \mid c_\alpha \neq 0\}$ ("the degree of P"),

$\mathrm{lc}(P) := c_{\deg(P)}$ ("the leading coefficient of P") and

$\mathrm{in}(P) := \mathrm{lc}(P) X^{\deg(P)}$ ("the initial term of P").

If $A, B \subseteq \mathbf{N}^n$, then $A + B := \{\alpha + \beta \mid \alpha \in A, \beta \in B\}$.

For a subset $F \subseteq R[X]$ we define

$\deg(F) := \{\deg(P) \mid P \in F - \{0\}\}$, $\mathscr{D}(F) := \deg(F) + \mathbf{N}^n$ and

$\mathrm{in}(F) := \{\mathrm{in}(P) \mid P \in F - \{0\}\}$.

1.5. Let J be an ideal in $R[X]$, $J \neq \{0\}$.

Definition. A finite subset G of $J - \{0\}$ is a "Gröbner basis of J" iff $\mathrm{in}(G)$ generates the ideal $<\mathrm{in}(J)>$.

Remarks and examples.

1) Let R be a field. Then a finite subset G of $J - \{0\}$ is a Gröbner basis of J iff $\deg(J) = \mathscr{D}(G)\,(= \deg(G) + \mathbf{N}^n)$.

2) Gröbner bases always exist: Choose a finite generating subset $M \subseteq \mathrm{in}(J)$ of $<\mathrm{in}(J)>$. Then any finite subset G of J with $\mathrm{in}(G) \supseteq M$ is a Gröbner basis of J.

3) Not every generating subset of an ideal is a Gröbner basis: Consider the graded lexicographic ordering on $\mathbf{N}^2$. Let $P_1 := X_1^2 X_2 + X_1$ and $P_2 := X_1 X_2^2$ be elements of $\mathbf{Q}[X_1, X_2]$. Then $\{P_1, P_2\}$ is not a Gröbner basis of $J := <P_1, P_2>$, since $X_1 X_2 = X_2 P_1 - X_1 P_2 \in J$, but $X_1 X_2 \notin <X_1^2 X_2, X_1 X_2^2> = <\mathrm{in}(P_1), \mathrm{in}(P_2)>$.

4) Any finite subset of $J - \{0\}$ containing a Gröbner basis is a Gröbner basis.

5) Let J be a principal ideal. Then any finite subset of J which contains a generating element of J is a Gröbner basis of J.

6) Any set of monomials $\{c_1 X^{\alpha(1)}, \ldots, c_k X^{\alpha(k)}\} \subseteq R[X]$ is a Gröbner basis of the ideal generated by them.

1.6. Let J be an ideal in $R[X]$, $J \neq \{0\}$.

The set $\mathrm{in}(J)$ is determined by a "weight-function"

$$w: \deg(J) \to R$$
$$\delta \mapsto w(\delta),$$

where $w(\delta)$ is a generating element of the (principal) ideal

$$<\mathrm{lc}(P) \mid P \in J, \deg(P) = \delta> .$$

So for $n = 2$ we can visualize $\mathrm{in}(J)$ by a figure of the following form:

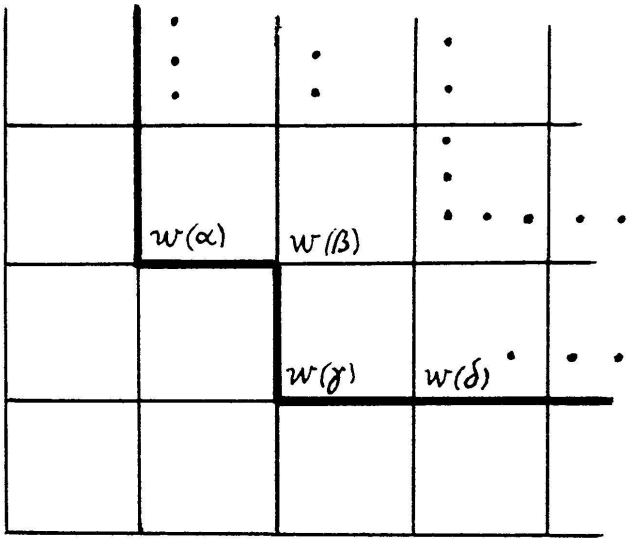

FIGURE 1.

For example, to $<2X_1, 3X_2> \subseteq \mathbf{Z}[X_1, X_2]$ corresponds figure 2.

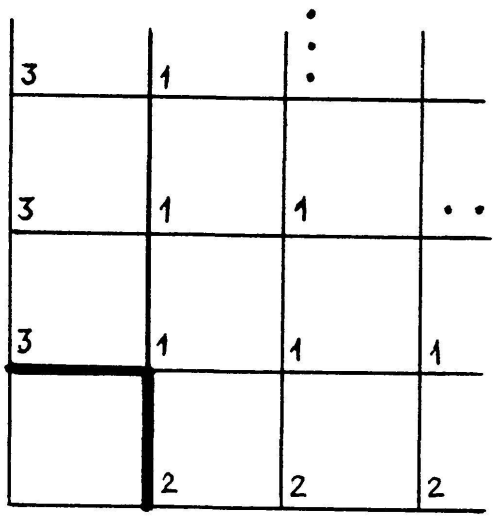

FIGURE 2.

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

$$\delta \mapsto 1$$

So the corresponding figure is of the form

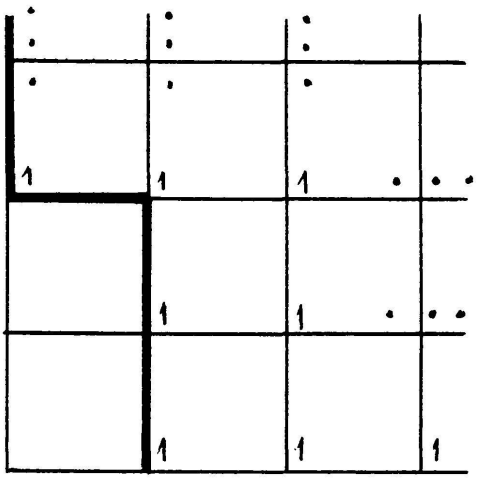

FIGURE 3.

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

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

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

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

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

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 $L = -X_1 X_2^3 (5X_1 + 1) + 2X_1^2 X_2^2 (3X_2 + 2)$.