Introduction

L'Enseignement Mathématique, t. 34 (1988), p. 215-232

THE THEORY OF GRÖBNER BASES

by Franz PAUER and Marlene PFEIFHOFER

INTRODUCTION

Let R be a principal ideal domain (for example the ring of integers or a field) and $R[X] = R[X_1, ..., X_n]$ the polynomial ring in n variables over R.

Let us mention some questions related to a subset F of $R[X]$:

1) Let $P \in R[X]$. How can we decide (in a finite number of steps) if P is an element of the ideal generated by F?

2) How can we find exact solutions to the system of algebraic equations corresponding to F?

3) If F' is another subset of $R[X]$, how can we decide if F and F' generate the same ideal?

An answer to these questions can be given by the method of so-called "Gröbner-bases". [1])

A "basis" of an ideal in $R[X]$ is a subset which generates this ideal. If we choose a strict ordering on $\mathbf{N}^n$, we can (analogous to the one-variable case) define the degree and the initial term of polynomials in $R[X]$. A "Gröbner basis" is a finite ideal basis, such that the initial terms of its elements generate the ideal generated by all initial terms of polynomials in the given ideal (see 1.5.).

In the first section we arrange some notations and give the definition of a Gröbner basis.

Then we present a division algorithm, which generalizes the usual division of univariate polynomials, and we give a characterization of Gröbner bases in terms of this division.

In the third section we explain how to construct a Gröbner basis from a given finite ideal basis.

---

[1]) Wolfgang Gröbner, 1899-1980, tyrolean mathematician.

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.