Gröbner basis

Canonical name	GrobnerBasis
Date of creation	2013-03-22 13:03:47
Last modified on	2013-03-22 13:03:47
Owner	mathcam (2727)
Last modified by	mathcam (2727)
Numerical id	28
Author	mathcam (2727)
Entry type	Definition
Classification	msc 13P10
Defines	monomial ordering
Defines	Gröbner basis

Definition of monomial orderings and support:
Let F be a field, and let S be the set of monomials in $F[x_1, \ldots, x_n]$, the polynomial ring in n indeterminates. A *monomial ordering* is a total ordering $\leq$ on S which satisfies

1. $a \leq b$ implies that $ac \leq bc$ for all $a, b, c \in S$.
2. $1 \leq a$ for all $a \in S$.

In practice, for any $a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in F[x_1, \ldots, x_n]$, we associate to a the string $(a_1, a_2, \ldots, a_n)$ and compare monomials by looking at orderings on these n-tuples.

Example. An extremely prevalent example of a monomial ordering is given by the standard lexicographical ordering of strings. Other examples include graded lexicographic ordering and graded reverse lexicographic ordering.

Henceforth, assume that we have fixed a monomial ordering. Define the *support* of a, denoted $\mathrm{supp}(a)$, to be the set of terms x_i with $a_i \neq 0$. Then define $M(a) = \max(\mathrm{supp}(a))$.

A partial order on $F[x_1, \ldots, x_n]$:
We can extend our monomial ordering to a partial ordering on $F[x_1, \ldots, x_n]$ as follows: Let $a, b \in F[x_1, \ldots, x_n]$. If $\mathrm{supp}(a) \neq \mathrm{supp}(b)$, we say that $a < b$ if $\max(\mathrm{supp}(a) - \mathrm{supp}(b)) < \max(\mathrm{supp}(b) - \mathrm{supp}(a))$.

It can be shown that:

1. The relation defined above is indeed a partial order on $F[x_1, \ldots, x_n]$
2. Every descending chain $p_1(x_1, \ldots, x_n) > p_2(x_1, \ldots, x_n) > \ldots$ with $p_i \in [x_1, \ldots, x_n]$ is finite.

A division algorithm for $F[x_1, \ldots, x_n]$:
We can then formulate a division algorithm for $F[x_1, \ldots, x_n]$:
Let $(f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials, with $f_i \in F[x_1, \ldots, x_n]$. Then for each $f \in F[x_1, \ldots, x_n]$, there exist $a_1, \ldots, a_s, r \in F[x_1, \ldots, x_n]$ with r unique, such that

1. $f = a_1 f_1 + \cdots + a_s f_s + r$
2. For each $i = 1, \ldots, s$, $M(a_i)$ does not divide any monomial in $\mathrm{supp}(r)$.

Furthermore, if $a_i f_i \neq 0$ for some i, then $M(a_i f_i) \leq M(f)$.

Definition of Gröbner basis:
Let I be a nonzero ideal of $F[x_1, \ldots, x_n]$. A finite set $T \subset I$ of polynomials is a *Gröbner basis* for I if for all $b \in I$ with $b \neq 0$ there exists $p \in T$ such that $M(p) \mid M(b)$.

Existence of Gröbner bases:
Every ideal $I \subset k[x_1, \ldots, x_n]$ other than the zero ideal has a Gröbner basis. Additionally, any Gröbner basis for I is also a basis of I.