Polynomials in Several Variables Over a Field and Groöbner Bases

Kevin James

Definition

A commutative ring R with 1_R is called Noetherian if every ideal of R is finitely generated.

Definition

A commutative ring R with 1_R is called Noetherian if every ideal of R is finitely generated.

Theorem (Hilbert Basis Theorem)

If R is a Noetherian ring then so is the polynomial ring $R[x]$.

Definition

A commutative ring R with 1_R is called Noetherian if every ideal of R is finitely generated.

Theorem (Hilbert Basis Theorem)

If R is a Noetherian ring then so is the polynomial ring $R[x]$.

Corollary

If F is a field, then every ideal in the polynomial ring $F[x_1, \ldots, x_n]$ is finitely generated.

Definition

A monomial ordering is a well ordering "$\geq$" on the set of monomials that satisfies $m_1 \geq m_2 \Rightarrow mm_1 \geq mm_2$ for all monomials m, m_1, m_2.

Definition

A monomial ordering is a well ordering "$\geq$" on the set of monomials that satisfies $m_1 \geq m_2 \Rightarrow mm_1 \geq mm_2$ for all monomials m, m_1, m_2.
Equivalently a monomial ordering may be specified by defining a well ordering on the n-tuples $\alpha = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ of multidegrees of monomials $Ax_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ that satisfies $\alpha \geq \beta \Rightarrow \alpha + \gamma \geq \beta + \gamma$.

Definition

Fix a monomial ordering on the polynomial ring $F[x_1, \ldots, x_n]$.

1. The leading term of $0 \neq f \in F[x_1, \ldots, x_n]$ denoted $\mathrm{LT}(f)$, is the monomial term of f of maximal order and the leading term of 0 is 0. Define the multidegree of f denoted $\partial(f)$, to be the degree of the leading term of f.
2. If I is an ideal of $F[x_1, \ldots, x_n]$, the ideal of leading terms denoted $\mathrm{LT}(I)$, is the ideal generated by the leading terms of all the elements in I.
   That is, $\mathrm{LT}(I) = (\mathrm{LT}(f) \quad | \quad f \in I)$.

Definition

Fix a monomial ordering on the polynomial ring $F[x_1, \ldots, x_n]$.

1. The leading term of $0 \neq f \in F[x_1, \ldots, x_n]$ denoted $\mathrm{LT}(f)$, is the monomial term of f of maximal order and the leading term of 0 is 0. Define the multidegree of f denoted $\partial(f)$, to be the degree of the leading term of f.
2. If I is an ideal of $F[x_1, \ldots, x_n]$, the ideal of leading terms denoted $\mathrm{LT}(I)$, is the ideal generated by the leading terms of all the elements in I.
   That is, $\mathrm{LT}(I) = (\mathrm{LT}(f) \quad | \quad f \in I)$.

Note

If f and g are nonzero, then $\partial(fg) = \partial(f) + \partial(g)$, and $\mathrm{LT}(fg) = \mathrm{LT}(f) * \mathrm{LT}(g)$

Definition

Ideals generated by monomials are called monomial ideals.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Example

Consider lexicographic with $x > y$ on $F[x, y]$.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Example

Consider lexicographic with $x > y$ on $F[x, y]$.
Let $f = x^3y - xy^2 + 1$ and $g = x^2y^2 - y^3 - 1$.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Example

Consider lexicographic with $x > y$ on $F[x, y]$.
Let $f = x^3y - xy^2 + 1$ and $g = x^2y^2 - y^3 - 1$.
$\mathrm{LT}(f) = x^3y$, $\partial(f) = (3, 1)$.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Example

Consider lexicographic with $x > y$ on $F[x, y]$.
Let $f = x^3y - xy^2 + 1$ and $g = x^2y^2 - y^3 - 1$.
$\mathrm{LT}(f) = x^3y$, $\partial(f) = (3, 1)$.
$\mathrm{LT}(g) = x^2y^2$, $\partial(g) = (2, 2)$.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. $LT(I)$ *is a monomial ideal.*
2. *Suppose that* I *is a monomial ideal. Then,* $f \in I$ *if and only if the monomials of* f *are all multiples of the monomial generators of* I *(Exercise #10).*
3. *If* $I = (f_1, \ldots, f_n)$ *then* $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.

Example

Consider lexicographic with $x > y$ on $F[x, y]$.
Let $f = x^3y - xy^2 + 1$ and $g = x^2y^2 - y^3 - 1$.
$\mathrm{LT}(f) = x^3y$, $\partial(f) = (3, 1)$.
$\mathrm{LT}(g) = x^2y^2$, $\partial(g) = (2, 2)$.
Let $I = (f, g)$. Then $(x^3y, x^2y^2) \subseteq \mathrm{LT}(I)$.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Example

Consider lexicographic with $x > y$ on $F[x, y]$.
Let $f = x^3y - xy^2 + 1$ and $g = x^2y^2 - y^3 - 1$.
$\mathrm{LT}(f) = x^3y$, $\partial(f) = (3, 1)$.
$\mathrm{LT}(g) = x^2y^2$, $\partial(g) = (2, 2)$.
Let $I = (f, g)$. Then $(x^3y, x^2y^2) \subseteq \mathrm{LT}(I)$.
Note that $yf - xg = x + y$. Thus $(x + y) \in I$ and $x \in \mathrm{LT}(I)$.

Definition

Ideals generated by monomials are called monomial ideals.

Fact

1. *$LT(I)$ is a monomial ideal.*
2. *Suppose that I is a monomial ideal. Then, $f \in I$ if and only if the monomials of f are all multiples of the monomial generators of I (Exercise #10).*
3. *If $I = (f_1, \ldots, f_n)$ then $(LT(f_1), \ldots, LT(f_n)) \subseteq LT(I)$.*

Example

Consider lexicographic with $x > y$ on $F[x, y]$.
Let $f = x^3y - xy^2 + 1$ and $g = x^2y^2 - y^3 - 1$.
$\mathrm{LT}(f) = x^3y$, $\partial(f) = (3, 1)$.
$\mathrm{LT}(g) = x^2y^2$, $\partial(g) = (2, 2)$.
Let $I = (f, g)$. Then $(x^3y, x^2y^2) \subseteq \mathrm{LT}(I)$.
Note that $yf - xg = x + y$. Thus $(x + y) \in I$ and $x \in \mathrm{LT}(I)$.
So, $(x^3y, x^2y^2) \subset \mathrm{LT}(I)$

Definition

A Gröbner Basis for an ideal I of $F[x_1, \ldots, x_n]$ is a finite set of generators $\{g_1, \ldots, g_m\}$ for I with the property that $\mathrm{LT}(I) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m))$.

Definition

A Gröbner Basis for an ideal I of $F[x_1, \ldots, x_n]$ is a finite set of generators $\{g_1, \ldots, g_m\}$ for I with the property that $\mathrm{LT}(I) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m))$.

General Polynomial Division

Fix a monomial ordering on $F[x_1, \ldots, x_n]$. Suppose that $f \in F[x_1, \ldots, x_n]$ and that $g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$ are non-zero.

Initialize: $q_1 = \cdots = q_m = r = 0$.

Step 1: If $f \neq 0$, test if $\mathrm{LT}(g_i) | \mathrm{LT}(f)$ for each i.

1. If $\mathrm{LT}(f) = a_i \mathrm{LT}(g_i)$,then $q_i \leftarrow q_i + a_i$, $f \leftarrow f - a_i g_i$. Repeat.
2. If $\mathrm{LT}(f)$ is not divisible by $\mathrm{LT}(g_i)$ for $1 \leq i \leq m$, then $r \leftarrow \mathrm{LT}(f)$, $f \leftarrow f - \mathrm{LT}(f)$. Repeat
3. If $f = 0$, terminate.

Upon termination, $f = q_1 g_1 + \cdots + q_m g_m + r$.

Theorem

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ *and suppose that* $\{g_1, \ldots, g_m\}$ *is a Gröbner basis for the nonzero ideal* $I \trianglelefteq R$. *Then,*

1. *Every polynomial* $f \in R$ *can be written uniquely as* $f = f_I + r$, *where* $f_I \in I$ *and none of the nonzero monomials in* r *is divisible by any of* $LT(g_1), \ldots, LT(g_m)$.
2. *Both* f_I *and* r *can be computed by general polynomial division by* $g_1, \ldots, g_m$ *and are independent of the order of* $g_1, \ldots, g_m$.
3. *The remainder* r *provides a unique representative in the quotient ring* $F[x_1, \ldots, x_n]/I$. *In particular,* $f \in I$ *if and only if* $r = 0$.

Proposition

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ *and let* I *be a nonzero ideal of* R.

1. *If* $g_1, \ldots, g_m$ *are any elements of* I *such that* $LT(I) = (LT(g_1), \ldots, LT(g_m))$, *then* $\{g_1, \ldots, g_m\}$ *is a Gröbner basis for* I.
2. *The ideal* I *has a Gröbner basis.*

Definition

Let $f_1, f_2 \in F[x_1, \ldots, x_n]$ and let M be the monic least common multiple of the monomial terms $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$. We define

$$S(f_1, f_2) = \frac{M}{\mathrm{LT}(f_1)} f_1 - \frac{M}{\mathrm{LT}(f_2)} f_2.$$

Definition

Let $f_1, f_2 \in F[x_1, \ldots, x_n]$ and let M be the monic least common multiple of the monomial terms $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$. We define

$$S(f_1, f_2) = \frac{M}{\mathrm{LT}(f_1)} f_1 - \frac{M}{\mathrm{LT}(f_2)} f_2.$$

Lemma

Suppose that $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ have the same multi-degree α and that the linear combination $h = a_1 f_1 + \cdots + a_m f_m$ with $a_i \in F$ has smaller multi-degree. Then,

$$h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i) \qquad \textit{for some } b_i \in F.$$

Definition

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and suppose that $G = \{g_1, \ldots, g_m\} \subset R$ is an ordered set. We write $f \equiv r \pmod{G}$ if r is the remainder of f upon generalized polynomial division by G (in order).

Definition

Fix a monomial ordering on $R = F[x_1, \ldots, x_n]$ and suppose that $G = \{g_1, \ldots, g_m\} \subset R$ is an ordered set. We write $f \equiv r \pmod{G}$ if r is the remainder of f upon generalized polynomial division by G (in order).

Proposition (Buchberger's Criterion)

Let $R = F[x_1, \ldots, x_n]$ and fix a monomial ordering on R. If $I = (g_1, \ldots, g_m)$ is a nonzero ideal of R, then $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I if and only if $S(g_i, g_j) \equiv 0 \pmod{G}$ for $1 \leq i < j \leq m$.