An Introduction to Gröbner Bases and its Applications

Sarfraz Ahmad

CIMPA, Nice, France

February 2024

COMSATS University Islamabad
Lahore Campus-Pakistan

Formalities

Classes

- Feb 12-15, 2024
- 2pm-4pm (Paris Time Zone)

1. Rings Revisted

Rings Revisited

Definition (Commutative ring with 1)

A commutative ring with 1 is a non-empty set R with a

- Addition $+ : R \times R \to R$ and a
- Multiplication $* : R \times R \to R$

such that

- R with $+$ is a commutative group,
- $*$ is associative and commutative,
- there is a neutral element 1 for the multiplication,
- $a(b+c) = ab + ac$ for all $a, b, c \in R$,

Rings Revisited

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are rings with the usual addition and multiplication

Example (Polynomial ring)

For a ring R is $R[x]$ the ring of polynomials with coefficients in R in the indeterminate x.

- $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$ (assume $n \leqslant m$).

$$f = g \Leftrightarrow a_i = b_i, i = 0, \ldots, n \text{ and } b_i = 0$$

for $n < i \leqslant m$.

- $f = \sum_{i=0}^{n} a_i x^i$

$$\deg(f) = \max\{i \mid a_i \neq 0\}$$

is called degree of f.

Rings Revisited

Example (Polynomial ring)

- an $f \in R[x]$ or $f(x) \in R[x]$ has a representation as $f = a_0 + a_1 x + \cdots + a_n x^n$ for some $n \geqslant 0$.
- the representation is not unique.
- if we demand that $a_n \neq 0$ then the representation becomes unique for $f \neq 0$.

Rings Revisited

Definition (Field)

A commutative ring R with 1 is called a field if every non-zero element has a multiplicative inverse.

- a commutative ring with 1 is a field if and only if $R \setminus \{0\}$ is a commutative group.
- examples of fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,...
- $\mathbb{Z}$ ist not a field, $R[x]$ is not a field.
- we will usually $\mathbb{K}$ to denote a field

2. Polynomial Ring over a Field

Polynomial Ring over a Field

Lemma

Let $f, g \in \mathbb{K}[x]$ *then*

- $\deg(f+g) \leqslant \max\{\deg(f), \deg(g)\}$.
- $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Polynomial Ring over a Field

Theorem (Division with remainder)

Let $f, g \in \mathbb{K}[x]$ and $g \neq 0$. Then there are polynomials $q, r \in \mathbb{K}[x]$ such that $f = g \cdot q + r$ and $\deg(r) < \deg(g)$.

Proof.

- $\deg(f) < \deg(g)$: then set $q = 0$ and $r = f$.
- $n = \deg(f) \geqslant m = \deg(g)$:

$$f = \sum_{i=0}^{n} a_i x^i, \quad g := \sum_{i=0}^{m} b_i x^i.$$

We prove the assertion by induction on $n - m$.

Induction Base: $n = m$

Set $q = \frac{a_n}{b_m}$ and $r = f - g\,\frac{a_n}{b_m}$ then

$$f = g\,q + r \text{ and } \deg(r) < \deg(g).$$

Polynomial Ring over a Field

Proof.

Induction Step: $n > m$

Set $q_1 = \frac{a_n}{b_m} x^{n-m}$ and $r_1 = f - \frac{a_n}{b_m} x^{n-m} g$.

Then

$$f = g\, q_1 + r_1 \text{ and } n_1 = \deg(r_1) < \deg(f).$$

If $\deg(r_1) < \deg(g)$ then we are done othwise $0 \leqslant n_1 - m < n - m$.

By induction hypothesis we have q_2 and r_2 such that

$$r_1 = g\, q_2 + r_2 \text{ and } \deg(r_2) < \deg(g) = m.$$

$$\begin{aligned} \rightarrow f &= g\, q_1 + r_1 \\ &= g\, q_1 + g\, q_2 + r_2 \\ &= g\,(q_1 + q_2) + r_2 \end{aligned}$$

For $q = q_1 + q_2$ and $r = r_2$ we are done. □

Polynomial Ring over a Field

Example

$$f = 2x^4 + x^3 + 2x^2 + 1 \text{ and } g = x^2 + 2x + 1.$$

$$\begin{array}{rl}
2x^4 + x^3 + 2x^2 & +1 = \left(x^2 + 2x + 1\right)\left(2x^2 - 3x + 6\right) - 9x - 5 \\
\underline{-2x^4 - 4x^3 - 2x^2} & \\
-3x^3 & \\
\underline{3x^3 + 6x^2 + 3x} & \\
6x^2 + 3x + 1 & \\
\underline{-6x^2 - 12x - 6} & \\
-9x - 5 &
\end{array}$$

$$q = 2x^2 - 3x + 6 \text{ and } r = -9x - 5.$$

In the polynomial division $f = g\,q + r$ with $\deg(r) < \deg(g)$ we call r the remainder or rest .

Polynomial Ring over a Field

Definition

Let $f, g \in \mathbb{K}[x]$ and $g \neq 0$. We say that g divides f if there is a polynomial $q \in \mathbb{K}[x]$ with $g\,q = f$. We write $g \mid f$.

Definition

Let $f, g \in \mathbb{K}[x]$, $f, g \neq 0$. We say that h is the greatest common divisor of f and g if

- $h|f$, $h|g$ and
- if for some $h' \in \mathbb{K}[x]$ we have $h'|f$ and $h'|g$ then $h'|h$

We write $\gcd(f, g)$ for the greatest common divisior of f and g.

Polynomial Ring over a Field

Definition (Euclidian Algorithm)

Let $f, g \in \mathbb{K}[x]$ and $g \neq 0$.

- Set $b_0 = f, b_1 = g, i = 1$
-

(A) Division with remainder $b_{i-1} = b_i\, q_i + r_i$

- $b_{i+1} = r_i$.
- Set $i = i + 1$
- if $b_i = r_{i-1} \neq 0$ then goto (A)
-
- Return b_{i-1}

Polynomial Ring over a Field

Equivalent formulation:

$$
\begin{aligned}
f = b_0 &= b_1\, q_1 + r_1 = g\, q_1 + r_1 \\
b_1 &= b_2\, q_2 + r_2 = r_1\, q_2 + r_2 \\
b_2 &= b_3\, q_3 + r_3 = r_2\, q_3 + r_3 \\
&\vdots \\
b_{i-2} &= b_{i-1}\, q_{i-1} + r_{i-1} = r_{i-2}\, q_{i-1} + r_{i-1} \\
b_{i-1} &= b_i\, q_i + 0 = b_i\, q_i + 0
\end{aligned}
$$

$$
b_i = \gcd(f, g).
$$

Polynomial Ring over a Field

Lemma

For two polynomials $f, g \in \mathbb{K}[x]$, $f, g \neq 0$ *the Euclidian algorithm computes* $\gcd(f, g)$.

Proof.

First we show that the algorithm terminates.
We know that:

- $b_1 = g$
- $\deg(b_i) > \deg(r_i)$, $i \geqslant 1$
- $\deg(b_i) = r_{i-1}$, $i \geqslant 2$

From that it follows that

$$\deg(g) = \deg(b_1) > \deg(r_1) > \deg(r_2) > \cdots .$$

Since deg takes values in $\mathbb{N} \cup \{\infty\}$ we must have $r_i = 0$ for some i. □

Proof.

Assume the Euclidian algorithm returns b_i.
We prove by induction on j from $j = i$ to 1 that for $b_0 = f$, $b_1 = g$:

$$b_i = \gcd(b_j, b_{j-1})$$

For $i = 1$: $b_i = \gcd(b_1, b_0) = \gcd(g, f)$
Induction base : $j = i$

- $b_{i-1} = b_i q_i \Rightarrow b_i | b_{i-1}, b_i$
- $h | b_{i-1}$, $h | b_i \Rightarrow h | b_i$

$\Rightarrow b_i = \gcd(b_i, b_{i-1})$ □

Proof.

Induction step: $i > j \geqslant 2$

By induction assumption: $b_i = \gcd(b_j, b_{j-1})$.

$$b_{j-2} = b_{j-1}q_{j-1} + r_{j-1} = b_{j-1}q_{j-1} + b_j$$

- $b_i = \gcd(b_j, b_{j-1}) \Rightarrow b_i | b_{j-2}$.
- $h | b_{j-2}$, $h | b_{j-1} \Rightarrow h | b_j \Rightarrow h | \gcd(b_j, b_{j-1}) = b_i$

$\Rightarrow b_i = \gcd(b_{j-2}, b_{j-1})$. □

Polynomial Ring over a Field

Example

$$f = (x-1)(x-1)(x^2+1) \text{ and } g = (x-1)(x+1)(x+1)$$

$$x^4 - 2x^3 + 2x^2 - 2x + 1 = (x^3 + x^2 - x - 1) \cdot (x-3) + (6x^2 - 4x - 2)$$

$$x^3 + x^2 - x - 1 = (6x^2 - 4x - 2) \cdot (\tfrac{1}{6}x + \tfrac{5}{18}) + (\tfrac{4}{9}x - \tfrac{4}{9})$$

$$6x^2 - 4x - 2 = (\tfrac{4}{9}x - \tfrac{4}{9}) \cdot (\tfrac{27}{2}x + \tfrac{9}{2}) + 0$$

$$\gcd(f,g) = \frac{4}{9}(x-1).$$

Corollary

For $f, g \in \mathbb{K}[x]$, $f, g \neq 0$, we have that $\gcd(f,g)$ exists and is unique up to multiplication with $a \in \mathbb{K} \setminus \{0\}$. In addtion there are $u, v \in \mathbb{K}[x]$ such that $\gcd(f,g) = uf + vg$.

Proof.

Follows directly from the Euclidian algorithm. □

Polynomial Ring over a Field

Lemma

Let $f \in \mathbb{K}[x]$ then f has a multiplicative inverse if and only if $f = a$ for some $a \in \mathbb{K} \setminus \{0\}$.

Proof.

If $a \in \mathbb{K} \setminus \{0\}$ then $a^{-1} \in \mathbb{K}$ thus $a\,a^{-1} = 1$ and a has a multiplicative inverse in $\mathbb{K}[x]$.
Let g be a multiplicative inverse of f:

$$\Rightarrow 1 = f\,g$$

$$\Rightarrow 0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g).$$

$\deg(f), \deg(g) \in \mathbb{N} \cup \{-\infty\} \Rightarrow \deg(f), \deg(g) = 0 \Rightarrow f = a$ for some $a \in \mathbb{K} \setminus \{0\}$. □

Polynomial Ring over a Field

Definition

Let $f \in \mathbb{K}[x]$ and $\deg(f) \geqslant 1$. Then we say f is irreducible if $g \mid f$ implies that $g = af$ for some $a \in \mathbb{K} \setminus \{0\}$ or $g = a$ for some $a \in \mathbb{K} \setminus \{0\}$.

Example

- $x - b$ is irreducible for all b
- $\deg(f) = 1 \Rightarrow f$ irreducible.
- $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$
- f irreducible $\Rightarrow af$ irreducible for any $a \in \mathbb{K} \setminus \{0\}$

Polynomial Ring over a Field

Lemma

Every polynomial $f \in \mathbb{K}[x]$ of degree $\deg(f) \geqslant 1$ is a product of irreducible polynomials.

Proof.

Induction of $\deg(f)$.

Induction base: $\deg(f) = 1$

$\Rightarrow f$ is irreducible $\Rightarrow$ assertion

Induction step: $\deg(f) > 1$

Case: f is irreducible

Then the assertion is trivial.

Case: f is not irreducible

Then there is g such that $g|f$ and $g \neq a, a\,f$ for some $a \in \mathbb{K} \setminus \{0\}$

$\Rightarrow f = g\,h$ for a polynomial h with $\deg(h) \geqslant 1 \rightarrow$

$\deg(g), \deg(h) < \deg(f) \xrightarrow{\text{Induction}} g$ and h are products of irreducible polynomials $\Rightarrow$ assertion. □

Polynomial Ring over a Field

Lemma

Let g be an irreducible polynomial and $h_1, \ldots, h_s$ polynomials such that $g|h_1 \cdots h_s$ then $g|h_i$ for some $1 \leqslant i \leqslant s$.

Proof.

Induction of s:

Induction Base: $s = 1, 2$.

$s = 1$: the assertion is trivial.

$s = 2$: $g|h_1 h_2$.

If $g|h_1$ were are done.

If $g \not| h_1 \xrightarrow{g \text{ irreducible}} 1 = \gcd(g, h_1) \Rightarrow$ exist polynomials u and v such that $1 = u\,g + v\,h_1 \Rightarrow h_2 = (u\,g + v\,h_1)h_2 = u\,g\,h_2 + v\,h_1 h_2 \xrightarrow{g|h_1 h_2} g|h_2$. □

Proof.

Induction Step: $s > 2$.

$g|h_1 \cdots h_s = (h_1 \cdots h_{s-1})h_s \xrightarrow{InductionBase} g|h_1 \cdots h_{s-1}$ or $g|h_s$

$\xrightarrow{Induction} g|h_i$ for some $1 \leqslant i \leqslant s$. □

Theorem

Let $f \in \mathbb{K}[x]$ be of degree $\deg(f) \geqslant 1$. If $f = g_1 \cdots g_r = h_1 \cdots h_s$ for irreducible polynomials $g_1, \ldots, g_r$ and $h_1, \ldots, h_s$ then $r = s$ and after renumbering we have $g_i = a_i h_i$ for some $a_i \in \mathbb{K} \setminus \{0\}$, $i = 1, \ldots, r = s$.

Proof.

$f = g_1 \cdots g_r = h_1 \cdots h_s \Rightarrow g_r | h_1 \cdots h_s \xrightarrow{g_r \text{ irreducible}}$ there is i such that $g_r | h_i \xrightarrow{h_i \text{ irreducible}} h_i = a_i g_r$ for some $a_i \in \mathbb{K} \setminus \{0\}$.

Without restriction of generality : $i = s$.

It follows that $g_1 \cdots g_{r-1} = a_s h_1 \cdots h_{s-1}$

Since $a_s h_1$ is irreducible we get by induction on $\max\{r, s\}$ that $r = s$ and $g_i = a_i h_i$ for some $a_i \in \mathbb{K} \setminus \{0\}$ and $i = 1, \ldots, r$. □

Polynomial Ring over a Field

Generalization:

Definition

For variables/indeterminates $x_1, \ldots, x_n$ we call $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ a monomial .

For $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ we write $\underline{x}^\alpha$ for $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Definition

- α is the multidegree of $\underline{x}^\alpha$
- for $\alpha \in \mathbb{N}^n$ we set $|\alpha| = \alpha_1 + \cdots + \alpha_n$ which is the degree $\deg(\underline{x}^\alpha)$ of $\underline{x}^\alpha$. We also set $\deg(0) = -\infty$.

Polynomial Ring over a Field

Remark

$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$.
$\Rightarrow \underline{x}^{\alpha} \cdot \underline{x}^{\beta} = \underline{x}^{\alpha+\beta}$.

Proof.

$$\begin{aligned} \underline{x}^{\alpha} \cdot \underline{x}^{\beta} &= x_1^{\alpha_1} \cdots x_n^{\alpha_n} \cdot x_1^{\beta_1} \cdots x_n^{\beta_n} \\ &= x_1^{\alpha_1+\beta_1} \cdots x_n^{\alpha_n+\beta_n} \\ &= \underline{x}^{\alpha+\beta} \end{aligned}$$

Polynomial Ring over a Field

Definition

$\mathbb{K}[x_1, \ldots, x_n]$ is the $\mathbb{K}$-vectorspace with basis $\{\underline{x}^\alpha \mid \alpha \in \mathbb{N}^n\}$.

We call $f \in \mathbb{K}[x_1, \ldots, x_n]$ or $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ a polynomial .

As a consequence we can write every $f \in \mathbb{K}[x_1, \ldots, x_n]$ uniquely as

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \cdot \underline{x}^\alpha$$

for $c_\alpha \in \mathbb{K}$ and all but finitely many c_α are 0. The latter is equivalent to

$$\left|\{\alpha \mid c_\alpha \neq 0\}\right| < \infty.$$

Polynomial Ring over a Field

Theorem

The polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ *with the vectorspace addition and the multiplication*

$$\Big(\sum_{\alpha \in \mathbb{N}^n} c_\alpha \underline{x}^\alpha \Big) \cdot \Big(\sum_{\alpha \in \mathbb{N}^n} c'_\alpha \underline{x}^\alpha \Big) = \sum_{\alpha \in \mathbb{N}^n} \Big(\sum_{\substack{\beta, \beta' \in \mathbb{N}^n \\ \beta + \beta' = \alpha}} c_\beta \, c'_{\beta'} \Big) \underline{x}^\alpha$$

is a (commutative) ring with 1.

Proof.

Either verifying all axioms or checking that

$$\mathbb{K}[x_1, \ldots, x_n] = (\cdots(\mathbb{K}[x_1])[x_2])\cdots)[x_n].$$

Polynomial Ring over a Field

Definition

Let $f = \sum_{\alpha \in \mathbb{N}} c_\alpha \underline{x}^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. Then

$$\deg(f) = \max \left\{ \deg(\underline{x}^\alpha) \mid c_\alpha \neq 0 \right\}.$$

is called the degree of f.

We adopt the convention $\max \emptyset = -\infty$.

Remark

$$\deg(f) = -\infty \Leftrightarrow f = 0.$$

Polynomial Ring over a Field

We will provide a simple proof of the following fact later:

Lemma

For $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ we have

$$\deg(f\,g) = \deg(f) + \deg(g).$$

Lemma

For $f \in \mathbb{K}[x_1, \ldots, x_n]$ is invertible if and only if $f = a$ for some $a \in \mathbb{K} \setminus \{0\}$.

Proof.

Same proof as for $\mathbb{K}[x]$. □

Polynomial Ring over a Field

Goal

Generalize division with remainder to $\mathbb{K}[x_1, \ldots, x_n]$.

Obvious analog does not work !

Example

- $f = x_1, g = x_2 \in \mathbb{K}[x_1, x_2]$
- $\deg(f) = \deg(g) = 1$
- Assume: $f = gq + r$ for some r with $\deg(r) < \deg(g) = 1$
- Thus $x_1 = x_2\, q + r$ for $r \in \mathbb{K}$
- Evaluating at $x_2 = 0$ one gets $x_1 = r(x_1, 0)$ contradicting $\deg(r) < 1$

3. Ideals

Ideals

Definition

A subset I of a (commutative) ring R is called an ideal if

- I with the addition $+$ is an abelian group.
- for any $s \in I$ and any $r \in R$ we have that $rs \in I$.

- $\{0\}$ is an ideal
- R is an ideal.
- $\{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(0, \ldots, 0) = 0\}$ is an ideal.

Ideals

Remark

Let R be a (commutative) ring with 1.
An ideal I of R with the addition and multiplication inherited from R is a ring with 1 if and only if $I = R$.

Proof.

$I = R \Rightarrow I$ is a ring with 1.

I ring with $1 \Rightarrow 1 \in I \Rightarrow$ for $s = 1$ and $r \in R$ we have $r = r1 \in I$ $\Rightarrow I = R$. □

Note: If rings are not required to have a 1 then ideals are rings.

Ideals

Lemma

Let I be an ideal in the ring R. Then $I = R$ if and only if I contains an (multiplicatively) invertible element.

Proof.

$I = R \Rightarrow 1 \in I \Rightarrow I$ contains an invertible element.

$a \in I$ invertible $\Rightarrow$ the for any $r \in R$ we have $r = (ra^{-1})a \in I \Rightarrow I = R$. □

- The invertible elements of $\mathbb{K}[x]$ are the constant polynomials $f = a \in \mathbb{K} \setminus \{0\}$.
- The invertible elements of $\mathbb{K}[x_1, \ldots, x_n]$ are the constant polynomials $f = a \in \mathbb{K} \setminus \{0\}$.

Ideals

Lemma

For any subset A of a ring R the set

$$\{I \mid A \subseteq I, I \text{ is an ideal}\}$$

has a unique inclusionwise minimal element.

Proof.

Let J be the intersection of all I from the set

$$\mathcal{A} = \{I \mid A \subseteq I, I \text{ is an ideal}\}.$$

- As an intersection of ideals J is an ideal (see following transparency, not covered in class).
- Since all ideals in the intersection contain A, so does J.

It follows that J is in the set $\mathcal{A}$ and must be its unique minimal element.

Ideal

Lemma

Let $\mathcal{A}$ be a set of ideals in the ring R. Then $\bigcap_{I \in \mathcal{A}} I$ is an ideal in R.

Proof.

Let $J = \bigcap_{I \in \mathcal{A}} I$.

- Each $I \in \mathcal{A}$ is an abelian subgroup of the additive group $(R, +)$. $\Rightarrow$ J is an abelian subgroup of $(R, +)$.
- Let $r \in R$.
  $s \in J \Rightarrow s \in I$ for all $I \in \mathcal{A} \Rightarrow rs \in I$ for all $I \in \mathcal{A} \Rightarrow rs \in J$.

Ideals

Definition

- For a subset $A \subseteq R$ for a ring R we write (A) for the inclusionwise smallest ideal containing A. The ideal (A) is called the ideal generated by A and A a generating set for I.
- If $A = \{f_1, \ldots, f_r\}$ we write $(f_1, \ldots, f_r)$ for (A).

Note: For an ideal I even inclusionwise minimal A with $I = (A)$ can have different cardinalities.

- $R = \mathbb{Z}$, $I = (4, 6) = (2)$
- $R = \mathbb{R}[x]$, $I = ((x-1)^2, (x-1)(x-2)) = ((x-1))$
- $(\emptyset) = \{0\}$

Ideals

Lemma

Let $f_1, \ldots, f_r \in R$ then

$$(f_1, \ldots, f_r) = \left\{ g_1 f_1 + \cdots + g_r f_r \mid g_1, \ldots, g_r \in R \right\}.$$

Proof.

- "$\supseteq$"

$f_1, \ldots, f_r \in (f_1, \cdots, f_r) \Rightarrow g_1 f_1 + \cdots + g_r f_r \in (f_1, \ldots, f_r)$ for all $g_1, \ldots, g_r \in R$.

- "$\subseteq$"

One proves $J = \left\{ g_1 f_1 + \cdots + g_r f_r \mid g_1, \ldots, g_r \in R \right\}$ is an ideal.
$\Rightarrow J$ is an ideal with $f_1, \ldots, f_r \in J \Rightarrow (f_1, \ldots, f_r) \subseteq J$. □

4. Ideals in Polynomial Rings

Ideals in Polynomial Rings

Goal: Standardize generating sets of ideals in $\mathbb{K}[x_1, \ldots, x_n]$ using Gröbner bases.

From Linear Algebra and the section about polynomial rings one already knows some tools to standardize generating sets of ideals.

- Ideals in $\mathbb{K}[x]$
- linear polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ (later)

Ideals in Polynomial Rings

Theorem

Let I be an ideal in $\mathbb{K}[x]$ then $I = (f)$ for some $f \in I$.

Proof.

Case: $I = \{0\}$ then $I = (0)$.
Case: $I \neq \{0\}$
Let $f \in I \setminus \{0\}$ be a polynomial such that

$$\deg(f) = \min\{\deg(g) \mid g \in I \setminus \{0\}\}.$$

Assume: $I \neq (f)$
Since clearly $(f) \subseteq I$ the assumption implies that there is $g \in I \setminus (f)$.
Division with remainder:

$$g = fq + r, \ \deg(r) < \deg(f)$$

$g, f \in I \Rightarrow g - fq = r \in I \xrightarrow{\deg(f) \text{ minimal}} r = 0. \Rightarrow g = fq \in (f)$ a contradiction. □

Ideals in Polynomial Rings

- In ideal I in a ring R such that $I = (f)$ for some $f \in R$ is called a principal ideal .
- An integral domain R such that all ideals are principal is called a principal ideal domain or PID .
- Any integral domain with a "division with remainder" is a PID. Integral domains with "division with remainder" are called Euclidian rings.
- $\mathbb{Z}$ and $\mathbb{K}[x]$
- In PIDs every element has a "unique" factorization into irreducible elements. Ring with "unique" factorization in irreducible elements are called factorial rings .

Ideals in Polynomial Rings

- $\mathbb{K}[x_1, \ldots, x_n]$ for $n \geqslant 2$ is not a PID.

Example

(x_1, x_2) is not a principal ideal in $\mathbb{K}[x_1, x_2]$.
Assume: (x_1, x_2) is a principal ideal.

$\Rightarrow$ there is $f \in \mathbb{K}[x_1, x_2]$ with $(f) = (x_1, x_2) \Rightarrow$
$x_1, x_2 \in (f) = \left\{ fg \mid g \in \mathbb{K}[x_1, x_2] \right\} \Rightarrow$ exist $g_1, g_2 \in \mathbb{K}[x_1, x_2]$ with $x_1 = f\, g_1$ and $x_2 = f\, g_2$

Evaluating at $x_1 = 0$:

$\Rightarrow 0 = f(0, x_2) \cdot g_1(0, x_2) \Rightarrow f(0, x_2)$ or $g_1(0, x_2)$ is the 0-polynomial in $\mathbb{K}[x_2] \Rightarrow f = x_1 f_1$ or $g_1 = x_1 g_{11} \xrightarrow{x_2 = fg_2} g_1 = x_1 g_{11}$

$\Rightarrow f = a$ for some $a \in \mathbb{K} \setminus \{0\} \Rightarrow \xrightarrow{a \text{ invertible}} (f) = \mathbb{K}[x_1, x_2] \Rightarrow$ contradiction.

An Introduction to Gröbner Basis and its Applications

Sarfraz Ahmad

CIMPA, Nice, France
February 2024

February 15, 2024

Monomial Ideals

5. Monomial Ideals

Monomial Ideals

- **Problem 1**
  Given $I = \langle f_1, \ldots, f_k \rangle$ and $f \in K[x_1, \ldots, x_n]$. Then to determine whether $f \in I$ is called an "Ideal Membership Problem".
- **Problem 2**
  if $f \in I$ find $u_1, \ldots u_k$ s.t $f = u_1 f_1 + \cdots u_k f_k$ where $I = \langle f_1, \ldots, f_k \rangle$ and $u_1, \ldots, u_k \in K[x_1, \ldots, x_n]$.
- **Problem 3**
  Is I=J?

We will answer to these Questions!

Monomial Ideals

Definition

An ideal I in $\mathbb{K}[x_1, \ldots, x_n]$ is called a monomial ideal if $I = (A)$ for a set A of monomials.

Example

- $(0) = (\emptyset)$ is a monomial ideal
- $(1) = \mathbb{K}[x_1, \ldots, x_n]$ is a monomial ideal
- $(x_1, \ldots, x_n)$ is a monomial ideal in $\mathbb{K}[x_1, \ldots, x_n]$
- $(x_1^3 x_2^2, x_1^2 x_2^3)$ is a monomial ideal in $\mathbb{K}[x_1, x_2]$

Monomial Ideals

Definition

We say that $g \in \mathbb{K}[x_1, \ldots, x_n]$, $g \neq 0$ divides $f \in \mathbb{K}[x_1, \ldots, x_n]$ if there is a polynomial $q \in \mathbb{K}[x_1, \ldots, x_n]$ with $g\,q = f$. We write $g \mid f$.

Lemma

$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. *Then*

$$\underline{x}^{\alpha} | \underline{x}^{\beta} \;\Leftrightarrow\; \alpha_i \leqslant \beta_i, 1 \leqslant i \leqslant n.$$

Proof.

- "$\Leftarrow$"

$\beta_i - \alpha_i \geqslant 0$, $1 \leqslant i \leqslant n \Rightarrow \underline{x}^{\beta-\alpha}$ is a monomial $\Rightarrow \underline{x}^{\alpha}\underline{x}^{\beta-\alpha} = \underline{x}^{\beta}$
$\Rightarrow \underline{x}^{\alpha} | \underline{x}^{\beta}$ □

Monomial Ideals

Proof.

- "$\Rightarrow$"

$\underline{x}^{\alpha} | \underline{x}^{\beta} \Rightarrow \underline{x}^{\alpha} q = \underline{x}^{\beta}$ for some $q = \sum_{\gamma \in \mathbb{N}^n} c_\gamma \underline{x}^{\gamma}$

$\Rightarrow \underline{x}^{\beta} = \sum_{\gamma \in \mathbb{N}^n} c_\gamma \underline{x}^{\alpha+\gamma}$

$\Rightarrow \beta = \alpha + \gamma$ for some $\gamma \in \mathbb{N}^n$

$\Rightarrow \alpha_i \leqslant \beta_i,\ i = 1, \ldots, n.$ □

Definition

For $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$ we write $\alpha \leqslant \beta$ if $\alpha_i \leqslant \beta_i$, $i = 1, \ldots, n$.

Monomial Ideals

Remark

$$\underline{x}^{\alpha} \mid \underline{x}^{\beta} \Leftrightarrow \alpha \leqslant \beta.$$

Monomial Ideals

Theorem (Dickson's Lemma)

Let M be a non-empty set of monomials in S. Then w.r.t partial order given by divisibility, the set M has only a finite number of minimal elements..

Proof.

Let $M \subseteq S = K[x_1, \ldots, x_n]$ We will prove this lemma by induction on n, the number of variables of S.

Monomial Ideals

Proof.

Basic Step : $\Rightarrow M \subseteq S = K[x_1]$

If $n = 1$ then M consists of certain powers of x_1, and the set of minimal elements of M is the set of $\{x_1^a\}$ where a is the smallest number s.t $x_1^a \in M \Rightarrow$ M has finite number of minimal elements. $\square$

Monomial Ideals

Proof.

Let the result holds for $n-1$.
Define set :

$$N = \left\{ \underline{x}^c \in K[x_1, \ldots, x_{n-1}] : \underline{x}^c \underline{x}^d \in M,\ d \geqslant 0 \right\}$$

By induction hypothesis, the set $\mathrm{N}^{\min}$ of minimal elements of N is finite.
Say $N^{\min} = \{\underline{x}^c, \ldots, \underline{x}^{c_r}\}$
For each $x^{c_i} \exists \quad a_i \geqslant 0$ st.

$$x^{c_i} x_n^{a_i} \in M \quad , i = 1, 2, \ldots, r$$

Let $a = \max\{a_1, \ldots, a_r\}$ & for each b with $0 \leqslant b < a$ let,

$$N_b = \left\{ \underline{x^c} \in K[x_1, \ldots, x_{n-1}] : \underline{x^c} x_n^b \in M \right\}$$

Monomial Ideals

Proof.

Again by induction hypothesis, $N_b^{\min}$ is a finite set.
We denote the set of monomials $\underline{x}^c x_n^b$ with
$\underline{x}^c \in N_b^{min}$ by $N_b^{min} x_n^b$ and
we claim that $M^{\min} \subset \{\underline{x}^{c_1} x_n^{a_1}, \ldots, \underline{x}^{c_r} x_n^{a_r}\} \bigcup_{b=0}^{a-1} N_b^{min} x_n^b$
since the R.H.S of this inclusion is a finite set, the assertion of the theorem follows from this claim.
Proof of claim:- Let $u = \underline{x}^c x_n^d$ be a monomial in M. If $d \geqslant a$ then some monomial in $\left\{x^{\underline{x}^{c_1} x_n^{ar}}, \ldots, \underline{x}^{c_r} x_r\right\}$ divides u
If $0 \leqslant d \leqslant a$ then u is divisible by a monomial in $N_b^{min} x_n^b$ as desired. □

Monomial Ideals

Corollary

Let I be a monomial ideal in $\mathbb{K}[x_1, \ldots, x_n]$ then there is a finite set $A = \{m_1, \ldots, m_r\}$ of monomials such that $I = (A)$.
This set is the inclusionwise smallest set of monomials generating I.

Monomial Ideals

Lemma

Let $I = (m_1, \ldots, m_r)$ *be a monomial ideal in* $\mathbb{K}[x_1, \ldots, x_n]$ *and* $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \underline{x}^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$.

$$f \in I \Leftrightarrow \text{ for all } \alpha, c_\alpha \neq 0 \text{ there is } m_j : m_j | \underline{x}^\alpha.$$

Proof.

- $\Rightarrow$

$f \in I \Rightarrow$ there are polynomials

$$g_j = \sum_{\gamma \in \mathbb{N}^n} c_\gamma^{(j)} \underline{x}^\gamma$$

such that $f = m_1 g_1 + \cdots + m_r g_r$
every monomial in $m_j g_j$ is divisible by m_j. □

Monomial Ideals

Proof.

- $\Leftarrow$

For every α with $m_j | \underline{x}^{\alpha}$ we have $\underline{x}^{\alpha} \in (m_1, \ldots, m_r) \Rightarrow$ $f \in (m_1, \ldots, m_r)$. $\square$

Term Orders

6. Term Orders

Term orders

Definition

A linear order $\preceq$ on the set of monomials $\{\underline{x}^\alpha \mid \alpha \in \mathbb{N}^n\}$ is called term order or monomial order if

- $1 \preceq \underline{x}^\alpha$ for all $\alpha \in \mathbb{N}^n$
- $\underline{x}^\alpha \preceq \underline{x}^\beta \Rightarrow \underline{x}^\alpha \underline{x}^\gamma \preceq \underline{x}^\beta \underline{x}^\gamma$ for all $\gamma \in \mathbb{N}^n$.

Example

For $n = 1$:

Define

$$x_1^a \preceq x_1^b \Leftrightarrow a \leqslant b.$$

This is a term order for $n = 1$.

Term orders

Example (Lexicographic order)

For $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ we set

$$\underline{x}^{\alpha} \prec \underline{x}^{\beta} \text{ if and only if exists } 1 \leqslant i \leqslant n : \begin{matrix} \alpha_j = \beta_j, j = 1, \ldots, i-1 \\ \alpha_i < \beta_i \end{matrix}.$$

The order $\prec$ is called the lexicographic (lex) order.

Lemma

The lexicographic order is a term order.

Example ($n = 2$)

$$1 \prec x_2 \prec x_2^2 \prec x_2^3 \cdots \prec x_1 \prec x_1 x_2 \prec \cdots \prec x_1^2 \prec$$

Term orders

Example (Degree Lexicographic order)

For $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ we set

$$\underline{x}^{\alpha} \prec \underline{x}^{\beta} \text{ if and only if}$$

$$\begin{array}{ll} \deg(\underline{x}^{\alpha}) < \deg(\underline{x}^{\beta}) & \text{or} \\ \deg(\underline{x}^{\alpha}) = \deg(\underline{x}^{\beta}) & \text{exists } 1 \leqslant i \leqslant n : \ \begin{array}{l} \alpha_j = \beta_j, j = 1, \ldots, i-1 \\ \alpha_i < \beta_i \end{array}. \end{array}$$

The order $\prec$ is called the degree lexicographic (deg lex) order.

Lemma

The degree lexicographic order is a term order.

Example ($n = 2$)

$$1 \prec x_2 \prec x_1 \prec x_2^2 \prec x_1 x_2 \prec x_1^2 \prec x_2^3 \prec x_1 x_2^2 \prec x_1^2 x_2 \prec \cdots$$

Term orders

Example (Degree Reverse Lexicographic order)

For $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ we set

$$\underline{x}^{\alpha} \prec \underline{x}^{\beta} \text{ if and only if}$$

$$\begin{array}{ll} \deg(\underline{x}^{\alpha}) < \deg(\underline{x}^{\beta}) & \text{or} \\ \deg(\underline{x}^{\alpha}) = \deg(\underline{x}^{\beta}) & \text{exists } 1 \leqslant i \leqslant n : \begin{array}{l} \alpha_j = \beta_j, j = i+1, \ldots, n \\ \alpha_i > \beta_i \end{array}. \end{array}$$

The order $\prec$ is called the degree reverse lexicographic (deg rev lex) order.

Lemma

The degree reverse lexicographic order is a term order.

Example ($n = 3$)

- $x_1 x_2^3 \prec x_1^2 x_2 x_3$ in deg lex.
- $x_1 x_2^3 \succ x_1^2 x_2 x_3$ in deg rev lex.

Term orders

Lemma

Let $\alpha, \beta \in \mathbb{N}^n$ and $\prec$ a term order. If $\underline{x}^\alpha | \underline{x}^\beta$ then $\underline{x}^\alpha \preceq \underline{x}^\beta$.

Proof.

$\underline{x}^\alpha | \underline{x}^\beta \Rightarrow \beta - \alpha \in \mathbb{N}^n \Rightarrow 1 \preceq \underline{x}^{\beta-\alpha} \Rightarrow \underline{x}^\alpha \cdot 1 \preceq \underline{x}^\alpha \cdot \underline{x}^{\beta-\alpha} \Rightarrow \underline{x}^\alpha \preceq \underline{x}^\beta$. □

Term orders

Theorem

Let $\prec$ be a term order on the monomials $\underline{x}^{\alpha}$, $\alpha \in \mathbb{N}^n$. Then $\prec$ is a well ordering, i.e. there is not infinite descending chain

$$\underline{x}^{\alpha_1} \succ \underline{x}^{\alpha_2} \succ \underline{x}^{\alpha_3} \succ \cdots .$$

Proof.

Assumption: There is an infinite descending chain

$$\underline{x}^{\alpha_1} \succ \underline{x}^{\alpha_2} \succ \underline{x}^{\alpha_3} \succ \cdots .$$

Consider the monomial ideal $I = (\underline{x}^{\alpha_1}, \underline{x}^{\alpha_2}, \ldots)$. $\xrightarrow{\text{Dickson's Lemma}}$ exist $j_1, \ldots, j_r$: $I = (\underline{x}^{\alpha_{j_1}}, \ldots, \underline{x}^{\alpha_{j_r}}) \Rightarrow$ for all $i \geqslant 1$ there is $1 \leqslant \ell \leqslant r$: $\underline{x}^{\alpha_{j_\ell}} | \underline{x}^{\alpha_i}$ $\xrightarrow{\textit{Lemma}}$ for all $i \geqslant 1$ there is $1 \leqslant \ell \leqslant r$: $\underline{x}^{\alpha_{j_\ell}} \prec \underline{x}^{\alpha_i} \Rightarrow$ for $j = \max\{j_1, \ldots, j_r\}$ there is $1 \leqslant \ell \leqslant r$ with $\underline{x}^{\alpha_{j_\ell}} \prec \underline{x}^{\alpha_{j+1}} \Rightarrow$ contradiction and the claim follows. □

Term orders

Definition

Let $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \underline{x}^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ a term order.

If $f \neq 0$ then we set

- $\mathrm{lm}_\prec(f) = \max_\prec\{\underline{x}^\alpha \mid c_\alpha \neq 0\}$ is called the leading monomial of f (with respect to $\prec$).
- $\mathrm{lc}_\prec(f) = c_\alpha$ for $\underline{x}^\alpha = \mathrm{lm}_\prec(f)$ is called the leading coefficient of f (with respect to $\prec$).

If $f = 0$ then we set $\mathrm{lm}_\prec(f) = \mathrm{lc}_\prec(f) = 0$.
Note: This setting is for technical reasons. 0 is not a monomial.
If $\mathrm{lm}_\prec(0) = 0$ appears then it is read as $0 \prec m$ for any monomial including 1.

Term orders

Example

$f = 2x_1^2x_2x_3 + 3x_1x_2^3 - 2x_1^3 \in \mathbb{Q}[x_1, x_2, x_3]$

- $\prec$ = lex then $\mathrm{lm}_{\preceq}(f) = x_1^3$, $\mathrm{lc}_{\preceq}(f) = -2$
- $\prec$ =deg lex then $\mathrm{lm}_{\preceq}(f) = x_1^2x_2x_3$, $\mathrm{lc}_{\preceq}(f) = 2$
- $\prec$ =deg rev lex then $\mathrm{lm}_{\preceq}(f) = x_1x_2^3$, $\mathrm{lc}_{\preceq}(f) = 3$

Division Algorithm

7. Division Algorithm

Division Algorithm

Definition

$f, g, h \in \mathbb{K}[x_1, \ldots, x_n]$ and $g \neq 0$. We say f reduces to h modulo g in one step if and only if $\mathrm{lm}_{\preceq}(g)$ divides a monomial $\underline{x}^{\alpha}$ with nonzero coefficient c_α from f and

$$h = f - \frac{c_\alpha \underline{x}^{\alpha}}{\mathrm{lc}_{\preceq}(g)\mathrm{lm}_{\preceq}(g)} g.$$

We then write $f \xrightarrow{g} h$.

Example

$f, g, h \in \mathbb{K}[x_1]$, $g \neq 0$, $\deg(f) \geqslant deg(g)$, $\prec$ deg lex order

$f = a_0 + \cdots + a_n x_1^n$, $a_n \neq 0$, $\quad g = b_0 + \cdots + b_m x_1^m$, $b_m \neq 0$.

$n \geqslant m \Rightarrow \mathrm{lm}_{\preceq}(g) = x^m | x^n = \mathrm{lm}_{\preceq}(f)$

for $q = \frac{a_n x_1^n}{b_m x_1^m}$ we get that $h = f - qg$ has degree $< \deg(f)$.

Hence $f = qg + h$ is not yet division with remainder !!!

Division Algorithm

Example

$f, g \in \mathbb{K}[x_1]$, $g \neq 0$, $\deg(f) \geqslant deg(g)$, $\prec$ deg lex order
We have seen that there are $h_1, \ldots, h_s$ such that

$$f \xrightarrow{g} h_1 \xrightarrow{g} h_2 \xrightarrow{g} \cdots \xrightarrow{g} h_s.$$

such that

$$\deg(f) > \deg(h_1) > \cdots > \deg(h_s)$$

or equivalently

$$\mathrm{lm}_{\preceq}(f) \succ \mathrm{lm}_{\preceq}(h_1) \succ \cdots \succ \mathrm{lm}_{\preceq}(h_s)$$

Continue until $\deg(h_s) < \deg(g)$ then for $r = h_s$ and suitable q:

$$f = gq + r$$

is division with remainder.

Division Algorithm

Example

$$f = x_1^2 x_2 + 4x_1 x_2 - 3x_2^2, g = 2x_1 + x_2 + 1 \in \mathbb{Q}[x_1, x_2]$$

$$\prec = \text{ deg lex}$$

$$\begin{aligned} f &\xrightarrow{g} -\frac{1}{2}x_1 x_2^2 + \frac{7}{2}x_1 x_2 - 3x_2^2 \\ &\xrightarrow{g} \frac{1}{4}x_2^3 + \frac{7}{2}x_1 x_2 - \frac{11}{4}x_2^2 \\ &\xrightarrow{g} \frac{1}{4}x_2^3 - \frac{9}{2}x_2^2 - \frac{7}{4}x_2. \end{aligned}$$

Division Algorithm

Definition

Let $f, h, f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ with $f_i \neq 0$, $1 \leqslant i \leqslant s$. Set $F = \{f_1, \ldots, f_s\}$. We say f reduces to h modulo F, denoted as

$$f \xrightarrow{F}_+ h$$

if and only if there exists a sequence of indices $i_1, \ldots, i_r \in \{1, \ldots, s\}$ and a sequence of polynomials $h_1, \ldots, h_{t-1} \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} h_3 \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Division Algorithm

Example

$$f_1 = x_1x_2 - x_1, f_2 = x_1^2 - x_2 \in \mathbb{Q}[x_1, x_2]$$

$$F = \{f_1, f_2\}, f = x_1^2x_2.$$

$$\prec = \text{ deg lex}$$

$$f \xrightarrow{F}_+ x_2$$

since

$$x_1^2x_2 \xrightarrow{f_1} x_1^2 \xrightarrow{f_2} x_2.$$

Division Algorithm

Definition

We call a polynomial r reduced modulo a set $F = \{f_1, \ldots, f_s\}$ of non-zero polynomials $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ if and only if either $r = 0$ or there is no monomial with non-zero coefficient in r which is divisible by one of $\mathrm{lm}_{\preceq}(f_i)$, $i = 1, \ldots, s$.

Definition

If $f \xrightarrow{F}_{+} r$ and r is reduced modulo F then we call r the remainder of f with respect to F.

Division Algorithm

Data: $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ with $f_i \neq 0$, $i = 1, \ldots, s$

Result: $u_1, \ldots, u_s, r$ such that $f = u_1 f_1 + \cdots + u_s f_s + r$ and r reduced modulo $\{f_1, \ldots, f_s\}$

$u_1 := 0$; $u_2 := 0, \cdots$, $u_s := 0$, $r := 0$, $h := f$.

while $h \neq 0$ **do**

  if *exists* i *such that* $\mathrm{lm}_{\preceq}(f_i)$ *divides* $\mathrm{lm}_{\preceq}(h)$ **then**

    choose i minimal such that $\mathrm{lm}_{\preceq}(f_i)$ divides $\mathrm{lm}_{\preceq}(h)$

$$u_i := u_i + \frac{\mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)}{\mathrm{lc}_{\preceq}(f_i)\mathrm{lm}_{\preceq}(f_i)}$$

$$h := h - \frac{\mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)}{\mathrm{lc}_{\preceq}(f_i)\mathrm{lm}_{\preceq}(f_i)} f_i$$

  else

$$r := r + \mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)$$

$$h := h - \mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)$$

  end

end

Division Algorithm

Example

$f = x_1^2x_2 + 4x_1x_2 - 3x_2^2$, $f_1 = 2x_1 + x_2 + 1 \in \mathbb{Q}[x_1, x_2]$ $\prec =$ dex lex

- Initialization: $u_1 = 0, r := 0, h := x_1^2x_2 + 4x_1x_2 - 3x_2^2$
- First pass through while loop

$x_1 = \mathrm{lm}_{\preceq}(f_1)$ divides $\mathrm{lm}_{\preceq}(h) = x_1^2x_2$

$$u_1 := u_1 + \frac{x_1^2x_2}{2x_1}$$
$$= \frac{1}{2}x_1x_2$$

$$h := h - \frac{x_1^2x_2}{2x_1}f_1$$
$$= -\frac{1}{2}x_1x_2^2 + \frac{7}{2}x_1x_2 - 3x_2^2$$

Division Algorithm

Example

$h = -\frac{1}{2}x_1x_2^2 + \frac{7}{2}x_1x_2 - 3x_2^2$, $f_1 = 2x_1 + x_2 + 1$, $u_1 = \frac{1}{2}x_1x_2$, $r = 0$

- Second pass through while loop

$x_1 = \mathrm{lm}_{\preceq}(f_1)$ divides $\mathrm{lm}_{\preceq}(h) = x_1x_2^2$

$$u_1 := u_1 + \frac{-\frac{1}{2}x_1x_2^2}{2x_1}$$
$$= \frac{1}{2}x_1x_2 - \frac{1}{4}x_2^2$$

$$h := h - \frac{-\frac{1}{2}x_1x_2^2}{2x_1}f_1$$
$$= \frac{1}{4}x_2^3 + \frac{7}{2}x_1x_2 - \frac{11}{4}x_2^2$$

Division Algorithm

Example

$h = \frac{1}{4}x_2^3 + \frac{7}{2}x_1x_2 - \frac{11}{4}x_2^2$, $f_1 = 2x_1 + x_2 + 1$, $u_1 = \frac{1}{2}x_1x_2 - \frac{1}{4}x_2^2$, $r = 0$

- Third pass through while loop

$x_1 = \mathrm{lm}_{\preceq}(f_1)$ does not divide $\mathrm{lm}_{\preceq}(h) = x_2^3$

$$\begin{aligned} r &:= r + \frac{1}{4}x_2^3 \\ &= \frac{1}{4}x_2^3 \end{aligned}$$

$$\begin{aligned} h &:= h - \frac{1}{4}x_2^3 \\ &= \frac{7}{2}x_1x_2 - \frac{11}{4}x_2^2 \end{aligned}$$

Division Algorithm

Example

$h = \frac{7}{2}x_1x_2 - \frac{11}{4}x_2^2$, $f_1 = 2x_1 + x_2 + 1$, $u_1 = \frac{1}{2}x_1x_2 - \frac{1}{4}x_2^2$, $r = \frac{1}{4}x_2^3$

- Fourth pass through while loop

$x_1 = \mathrm{lm}_{\preceq}(f_1)$ divides $\mathrm{lm}_{\preceq}(h) = x_1x_2$

$$u_1 := u_1 + \frac{\frac{7}{2}x_1x_2}{2x_1}$$
$$= \frac{1}{2}x_1x_2 - \frac{1}{4}x_2^2 + \frac{7}{4}x_2$$

$$h := h - \frac{\frac{7}{2}x_1x_2}{2x_1}f_1$$
$$= -\frac{9}{2}x_2^2 - \frac{7}{4}x_2$$

Division Algorithm

Example

$h = -\frac{9}{2}x_2^2 - \frac{7}{4}x_2$, $f_1 = 2x_1 + x_2 + 1$, $u_1 = \frac{1}{2}x_1x_2 - \frac{1}{4}x_2^2 + \frac{7}{4}x_2$, $r = \frac{1}{4}x_2^3$

- Fifths pass through while loop

$x_1 = \mathrm{lm}_{\preceq}(f_1)$ does not divide $\mathrm{lm}_{\preceq}(h) = x_2^2$

$$r := r + \left(-\frac{9}{2}x_2^2\right)$$
$$= \frac{1}{4}x_2^3 - \frac{9}{2}x_2^2$$

$$h := h - \left(-\frac{9}{2}x_2^2\right)$$
$$= -\frac{7}{4}x_2$$

Division Algorithm

Example

$h = -\frac{7}{4}x_2$, $f_1 = 2x_1 + x_2 + 1$, $u_1 = \frac{1}{2}x_1x_2 - \frac{1}{4}x_2^2 + \frac{7}{4}x_2$,
$r = \frac{1}{4}x_2^3 - \frac{9}{2}x_2^2$

- Sixth pass through while loop

$x_1 = \mathrm{lm}_{\preceq}(f_1)$ does not divide $\mathrm{lm}_{\preceq}(h) = x_2$

$$
\begin{aligned}
r &:= r + \left(-\frac{7}{4}x_2\right) \\
&= \frac{1}{4}x_2^3 - \frac{9}{2}x_2^2 - \frac{7}{4}x_2
\end{aligned}
$$

$$
\begin{aligned}
h &:= h - \left(-\frac{7}{4}x_2\right) \\
&= 0
\end{aligned}
$$

Division Algorithm

Theorem

Given a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$ *and* f *in* $\mathbb{K}[x_1, \ldots, x_n]$ *the division algorithm produces polynomials* $u_1, \ldots, u_s \in \mathbb{K}[x_1, \ldots, x_n]$ *such that*

$$f = u_1 f_1 + \cdots + u_s f_s + r$$

and r *is reduced with respect of* F *and*

$$\mathrm{lm}_{\preceq}(f) = \max_{\preceq}\left\{\mathrm{lm}_{\preceq}(u_i)\mathrm{lm}_{\preceq}(f_i), i = 1, \ldots, s, \mathrm{lm}_{\preceq}(r)\right\}.$$

It holds that

$$f \xrightarrow{F}_{+} r.$$

Division Algorithm

Proof.

- The division algorithm terminates

In each pass through the while loop either

$$h = h - \frac{\mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)}{\mathrm{lc}_{\preceq}(f_i)\mathrm{lm}_{\preceq}(f_i)} f_i$$

or

$$h := h - \mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)$$

decrease $\mathrm{lm}_{\preceq}(h)$.

No infinite descending $\prec$-chains $\Rightarrow$ algorithm terminates. $\square$

Division Algorithm

Proof.

- $f = u_1 f_1 + \cdots + u_s f_s + r$

Show by induction that in each step the equation $f = h + u_1 f_1 + \cdots + u_s f_s + r$ is preserved.

- ▷ Induction Base: $h = f,\ u_1, \ldots, u_s, r = 0$.

Then $f = h + u_1 f_1 + \cdots + u_s f_s + r$ □

Division Algorithm

Proof.

- Induction Step: $f = h + u_1 f_1 + \cdots + u_s f_s + r$ holds before the the next iteration of while loop.

Case : "If" first part:

$$u_i f_i \to u_i f_i + \frac{\mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)}{\mathrm{lc}_{\preceq}(f_i)\mathrm{lm}_{\preceq}(f_i)} f_i$$

$$h \to h - \frac{\mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)}{\mathrm{lc}_{\preceq}(f_i)\mathrm{lm}_{\preceq}(f_i)} f_i$$

Thus $h + u_i f_i$ remains constant during the pass through while loop. Hence $f = h + u_1 f_1 + \cdots + u_s f_s + r$ after the loop. □

Division Algorithm

Proof.

Case : "If" second ("Else") part:

$$r \to r + \mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)$$
$$h \to h - \mathrm{lc}_{\preceq}(h)\mathrm{lm}_{\preceq}(h)$$

Thus $h + r$ remains constant during the pass through while loop.

Hence $f = h + u_1 f_1 + \cdots + u_s f_s + r$ after the loop. □

Division Algorithm

Proof.

- $\mathrm{lm}_{\preceq}(f) = \max_{\preceq}\left\{\mathrm{lm}_{\preceq}(u_i)\mathrm{lm}_{\preceq}(f_i), i = 1, \ldots, s, \mathrm{lm}_{\preceq}(r)\right\}$

Show that in each step the equations the following is preserved:

$$\mathrm{lm}_{\preceq}(f) = \max_{\preceq}\left\{\mathrm{lm}_{\preceq}(h), \mathrm{lm}_{\preceq}(u_i)\mathrm{lm}_{\preceq}(f_i), i = 1, \ldots, s, \mathrm{lm}_{\preceq}(r)\right\}$$

- $f \xrightarrow{F}_{+} r$.

By construction. □

8. Gröbner Bases

Gröbner Bases

Definition

Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and $\preceq$ a term order. A set of non-zero polynomials $G = \{g_1, \ldots, g_t\} \subseteq I$ is a Gröbner basis of I with respect to $\preceq$ if and only if for all $f \in I$ such that $f \neq 0$ there exists $i \in \{1, \ldots, t\}$ such that

$$\mathrm{lm}_{\preceq}(g_i) \text{ divides } \mathrm{lm}_{\preceq}(f).$$

Example

$I = (x_1^2 + x_1, x_1^2 + 2x_1 + 1) = (x_1 + 1)$ ideal in $\mathbb{K}[x_1]$, $\prec =$ deg lex.

- $G = \{x_1^2 + x_1, x_1^2 + 2x_1 + 1\}$ not a Gröbner basis for I
- $G = \{x_1 + 1\}$ not a Gröbner basis for I

Gröbner Bases

Definition

Let S be a subset of $\mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ a term order. Then

$$\mathrm{in}_{\preceq}(S) := \left(\mathrm{lm}_{\preceq}(f) \mid f \in S\right)$$

is called the initial ideal of S.

Note that $\mathrm{in}_{\preceq}(S)$ is a monomial ideal.

Example

$I = (x_1^2 + x_1, x_1^2 + 2x_1 + 1) = (x_1 + 1)$ ideal in $\mathbb{K}[x_1]$, $\prec =$ deg lex.

$$\Rightarrow \mathrm{in}_{\preceq}(I) = (x_1).$$

Gröbner Bases

Theorem

Let $I \neq (0)$ be an ideal and $G = \{g_1, \ldots, g_s\} \subseteq I$ a set of non-zero polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The for a term order $\prec$ the following are equivalent:

(i) *G is a Gröbner basis of I with respect to $\prec$*

(ii) $f \in I \Leftrightarrow f \xrightarrow{G}_+ 0$

(iii) $f \in I \Leftrightarrow f = h_1 g_1 + \cdots + h_s g_s$ *with*

$$\mathrm{lm}_\preceq(f) = \max_\preceq\{\mathrm{lm}_\preceq(h_i)\mathrm{lm}_\preceq(g_i) \mid i = 1, \ldots, s\}$$

and $h_i \in \mathbb{K}[x_1, \ldots, x_n]$, $i = 1, \ldots, s$.

(iv) $\mathrm{in}_\preceq(I) = \mathrm{in}_\preceq(G)$

Gröbner Bases

Proof.

- (i) $\Rightarrow$ (ii)

General Fact: $f \in \mathbb{K}[x_1, \ldots, x_n] \xrightarrow{\text{Division algorithm}} \exists r \in \mathbb{K}[x_1, \ldots, x_n]$

reduced with respect to G such that $f \xrightarrow{G}_+ r \Rightarrow f - r \in I \Rightarrow$

$$f \in I \Leftrightarrow r \in I$$

Using this fact we prove (i) $\Rightarrow$ (ii)

- ▷ "$\Rightarrow$"

$r = 0 \Rightarrow r \in I \Rightarrow f \in I$.

- ▷ "$\Leftarrow$"

$f \in I \Rightarrow r \in I$.

Assumption: $r \neq 0$

$\xrightarrow{G \text{ Gröbner basis}}$ exists g_i with $\mathrm{lm}_{\preceq}(g_i) | \mathrm{lm}_{\preceq}(r) \Rightarrow$ contradiction to r

reduced $\Rightarrow r = 0$

Gröbner Bases

Proof.

- (ii) $\Rightarrow$ (iii)
  - ▷ "$\Rightarrow$"

$$f \in I \overset{(ii)}{\Longrightarrow} f \xrightarrow{G}_{+} 0 \overset{\text{Theorem before}}{\Longrightarrow} f = h_1 g_1 + \cdots + h_s g_s \text{ with}$$

$$\mathrm{lm}_{\preceq}(f) = \max_{\preceq}\left\{ \mathrm{lm}_{\preceq}(h_i)\mathrm{lm}_{\preceq}(g_i) \mid i = 1, \ldots, s \right\}$$

and $h_i \in \mathbb{K}[x_1, \ldots, x_n]$, $i = 1, \ldots, s$.

  - ▷ "$\Leftarrow$"

$$f = h_1 g_1 + \cdots + h_s g_s \overset{G \subseteq I}{\Longrightarrow} f \in I.$$

□

Gröbner Bases

Proof.

- (iii) $\Rightarrow$ (iv)
  - $\mathrm{in}_\preceq(G) \subseteq \mathrm{in}_\preceq(I)$

$G \subseteq I \Rightarrow \mathrm{in}_\preceq(G) \subseteq \mathrm{in}_\preceq(I)$.

  - $\mathrm{in}_\preceq(G) \supseteq \mathrm{in}_\preceq(I)$

$f \in I \overset{(iii)}{\Longrightarrow} f = h_1 g_1 + \cdots + h_s g_s$ with

$$\mathrm{lm}_\preceq(f) = \max_\preceq \left\{ \mathrm{lm}_\preceq(h_i)\mathrm{lm}_\preceq(g_i) \mid i = 1, \ldots, s \right\}$$

$\Rightarrow \mathrm{lm}_\preceq(f) \in \mathrm{in}_\preceq(G) \Rightarrow \mathrm{in}_\preceq(I) \subseteq \mathrm{in}_\preceq(G)$. $\square$

Gröbner Bases

Proof.

- (iv) $\Rightarrow$ (i)

$f \in I \overset{(iv)}{\Longrightarrow} \mathrm{lm}_{\preceq}(f) = \mathrm{lm}_{\preceq}(g_1)h_1 + \cdots + \mathrm{lm}_{\preceq}(g_s)h_s \Rightarrow$ exists g_i with $\mathrm{lm}_{\preceq}(g_i) | \mathrm{lm}_{\preceq}(f) \Rightarrow G$ Gröbner basis $\square$

Gröbner Bases

Corollary

Let $G = \{g_1, \ldots, g_s\}$ *be a Gröbner basis of the ideal* I *in* $\mathbb{K}[x_1, \ldots, x_n]$. *Then*

$$I = (g_1, \ldots, g_s).$$

Proof.

G Gröbner basis of $I \Rightarrow G \subseteq I \Rightarrow (g_1, \ldots, g_s) \subseteq I$.

$f \in I \xrightarrow{\text{(iii) of Theorem}} f = h_1 g_1 + \cdots + h_s g_s \Rightarrow f \in (g_1, \ldots, g_s) \Rightarrow$

$I \subseteq (g_1, \ldots, g_s)$. □

Gröbner Bases

Corollary

Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $\prec$ a term order. Then there is a Gröbner basis $G = \{g_1, \ldots, g_s\}$ of I.

Proof.

$\mathrm{in}_\preceq(I)$ is a monomial ideal $\Rightarrow \mathrm{in}_\preceq(I) = (m_1, \ldots, m_s)$ for finitely many monomials $m_1, \ldots, m_s \overset{(iii)}{\Longrightarrow}$ exist $g_1, \ldots, g_s \in I$ with $\mathrm{lm}_\preceq(g_i) = m_i \overset{(iv)}{\Longrightarrow} G = \{g_1, \ldots, g_s\}$ Gröbner basis $\square$

Gröbner Bases

Corollary

If $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal. Then I is generated by a finite set of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

Proof.

We know:

- I has a Gröbner basis $\{g_1, \ldots, g_s\}$
- a Gröbner basis $\{g_1, \ldots, g_s\}$ generates the ideal.

□

Remark

The number of generators of an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ for $n \geqslant 2$ is not bounded by n !

Gröbner Bases

Definition

A ring R is called Noetherian if every ideal is generated by a finite set.

Example

- Any PID, $\mathbb{Z}$, $\mathbb{K}[x]$.
- $\mathbb{K}[x_1, \ldots, x_n]$.
- R Noetherian $\Rightarrow$ $R[x]$ Noetherian (proof in textbooks)

Gröbner Bases

For the sake of a simpler notation:

Definition

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$. We say that G is a Gröbner basis, if G is a Gröbner basis of $(g_1, \ldots, g_s)$.

Gröbner Bases

Theorem

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ *then the following are equivalent:*

(i) *G is a Gröbner basis*

(ii) *The remainder of division by G is unique*

Remark

Even for Gröbner bases: $u_1, \ldots, u_s$ such that

$$g = u_1 g_1 + \cdots + u_s g_s + r$$

for r reduced are not neccessarily unique.

Gröbner Bases

Proof.

- (i) $\Rightarrow$ (ii)

Assume $f \xrightarrow{G}_+ r$ and $f \xrightarrow{G}_+ r'$ and r and r' reduced with respect to G.

$\Rightarrow f - r, f - r' \in (G) \Rightarrow (f - r) - (f - r') = r' - r \in (G)$

r, r' reduced $\Rightarrow r - r'$ reduced with respect to $G \Rightarrow r - r' = 0 \Rightarrow r = r'$. $\square$

Gröbner Bases

Proof.

- (ii) $\Rightarrow$ (i)

We show that (ii) implies

$$f \in (G) \Leftrightarrow f \xrightarrow{G}_+ 0.$$

This is one of the equivalent conditions from the theorem and implies that G is a Gröbner basis.

- "$\Leftarrow$"

$f \xrightarrow{G}_+ 0 \Rightarrow f = u_1 g_1 + \cdots + u_s g_s \Rightarrow f \in (G)$ $\square$

Gröbner Bases

Proof.

- "$\Rightarrow$"

We must show:
$f \in (G)$ and $f \xrightarrow{G}_+ r$, r reduced $\Rightarrow$ then $r = 0$

Claim:

- $c \in \mathbb{K}$, $c \neq 0$,
- m Monomial
- $g \in \mathbb{K}[x_1, \ldots, x_n]$ with $g \xrightarrow{G}_+ r$ for r reduced.

Then $g - c\, m\, g_i \xrightarrow{G}_+ r$ for $i = 1, \ldots, s$. □

Gröbner Bases

Proof.

Proof of Claim:
Consider the monomial $m' = m\mathrm{lm} \preceq (g_i)$ Consider the following cases:

- m' does not appear in $g \Rightarrow$

$g - c\, m\, g_i \xrightarrow{g_i} g \xrightarrow{G}_+ r$.

- m' appears in $g \Rightarrow$

$d' =$ coefficient of m' in g.
$d =$ coefficient of m' in $c\, m\, g_i = c\, \mathrm{lc}_{\preceq}(g_i)$.

Gröbner Bases

Proof.

Case: $d = d'$

let r_1 reduced such that $g - c\,m\,g_i \xrightarrow{G}_+ r_1$

By $d \neq 0$ it follows that

$$g \xrightarrow{g_i} g - c\,m\,g_i \xrightarrow{G}_+ r_1$$

$$\Rightarrow g \xrightarrow{G}_+ r \text{ and } g \xrightarrow{G}_+ r_1 \xrightarrow{\text{Uniqueness of remainder}} r = r_1 \text{ and}$$

$g - c\,m\,g_i \xrightarrow{G}_+ r$ □

Gröbner Bases

Proof.

Case: $d \neq d'$

Set $h = g - \frac{d}{d'} c\, m\, g_i \Rightarrow$ the coefficient of $m\mathrm{lm}_{\preceq}(g_i)$ in h is 0.

Then:

$\xrightarrow{d,d' \neq 0} g \xrightarrow{g_i} h.$

$\xrightarrow{d \neq d'} g - c\, m\, g_i \xrightarrow{g_i} h$

$\Rightarrow$ for $h \xrightarrow{G}_+ r_1$, r_1 reduced, we have $g \xrightarrow{G}_+ r_1$ and hence $r = r_1 \Rightarrow$ $g - c\, m\, g_i \xrightarrow{G}_+ r$.

This completes the proof of the claim. □

Gröbner Bases

Proof.

Claim (already proved):

- $c \in \mathbb{K}$, $c \neq 0$,
- m Monomial
- $g \in \mathbb{K}[x_1, \ldots, x_n]$ with $g \xrightarrow{G}_+ r$ for r reduced.

Then $g - c\, m\, g_i \xrightarrow{G}_+ r$ for $i = 1, \ldots, s$.

$$f \in (g_1, \ldots, g_s) \Rightarrow f = \sum_{i=1}^{s} h_i g_i \xrightarrow{\text{expand } h_i \text{ in monomials}}$$

$$f = \sum_{j=1}^{\ell} c_j \underline{x}^{\alpha_j} g_{i_j}$$

$$\xrightarrow{\text{Claim}} f - c_1 \underline{x}^{\alpha_1} g_{i_1} \xrightarrow{G} r \xrightarrow{\text{Claim}} f - c_1 \underline{x}^{\alpha_1} g_{i_1} - c_2 \underline{x}^{\alpha_2} g_{i_2} \xrightarrow{G}_+ r$$

$$\xrightarrow{\text{Claim}} \cdots \xrightarrow{\text{Claim}} 0 = f - \sum_{i=1}^{\ell} c_j \underline{x}^{\alpha_j} g_{i_j} \xrightarrow{G}_+ r \Rightarrow r = 0. \qquad \square$$

Hilbert Basis Theorem

Every polynomial ideal is finitely generated.
OR:
Every ideal in $S = k[x_1, \ldots, x_n]$ is finitley generated i.e.,
$I = \langle f_1, \ldots, f_k \rangle$ **where** $f_1, \ldots, f_k \in S$
Proof:
Let $I \subseteq S$ be a polynomial ideal then by Dickson's lemma,

$$\text{in } \preceq (I) = (lm \preceq (f) \mid f \in I)$$

$\Rightarrow$ which is minimal ideal.
So, by Dickson's lemma it is finitely generated. so there exists $\{g_1, \ldots, g_t\} \subseteq I$ such that in $_{\preceq}(I) = \langle lm_{\preceq}(g_1), \ldots, lm_{\preceq}(g_k) \rangle$
we will show that $I = \langle g_1 \ldots, g_k \rangle$
Since $\langle g_1 \ldots, g_k \rangle \subseteq I$
We need to show that $I \subseteq \langle g_1 \ldots, g_k \rangle$

Let $f \in I \Rightarrow f \subseteq \langle g_1 \ldots, g_k \rangle$
By division Algorithm,
$f = u_1 g_1 + \ldots + u_k g_k + r$
If $r = 0$ then $f \in \langle g_1 \ldots, g_k \rangle$ we are done.
If $r \neq 0$ then $r = f - u_1 g_1 - \ldots - u_k g_k \in I$
Since
$f \in I$ and $\rangle(g_1), \ldots, g_k \rangle \in I$
$\Rightarrow r \in I$
$\Rightarrow$ lm $_{\preceq}(r) \in$ in $_{\preceq}(I) = \langle lm_{\preceq}(g_1), \ldots, lm_{\preceq}(g_k) \rangle$
which is a contradiction by division algorithm.
$\Rightarrow r = 0 \Rightarrow I \subseteq \langle g_1 \ldots, g_k \rangle$ Hence;
$I = \langle g_1 \ldots, g_k \rangle$

9. S-Polynomials and Buchberger's Algorithm

S-Polynomials and Buchberger's Algorithm

So far:

- Gröbner bases have nice properties.
- not clear how to find a Gröbner basis for a given I

Definition

$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Then

$$\operatorname{lcm}(\underline{x}^{\alpha}, \underline{x}^{\beta}) = x_1^{\max(\alpha_1, \beta_1)} \cdots x_n^{\max(\alpha_n, \beta_n)}$$

is the least common multiple of $\underline{x}^{\alpha}$,$\underline{x}^{\beta}$.

Example

$$\operatorname{lcm}(x_1 x_3^3 x_4, x_1^3 x_2 x_3^2 x_4) = x_1^3 x_2 x_3^3 x_4.$$

S-Polynomials and Buchberger's Algorithm

Definition

Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, $f, g \neq 0$ and $\prec$ a term order. Set $m = \mathrm{lcm}(\mathrm{lm}_\preceq(f), \mathrm{lm}_\preceq(g))$. The polynomial

$$S(f,g) := \frac{m}{\mathrm{lc}_\preceq(f)\mathrm{lm}_\preceq(f)}\, f - \frac{m}{\mathrm{lc}_\preceq(g)\mathrm{lm}_\preceq(g)}\, g$$

is called the S-polynomial of f and g.

Example

$f = 2x_1x_2 - x_1, g = 3x_1^2 - x_2 \in \mathbb{Q}[x_1, x_2], \prec =$ deg lex

- $\mathrm{lm}_\preceq(f) = x_1x_2$
- $\mathrm{lm}_\preceq(g) = x_1^2$
- $m = \mathrm{lcm}(x_1x_2, x_1^2) = x_1^2x_2$

$$S(f,g) = \frac{x_1^2x_2}{2\,x_1x_2} f - \frac{x_1^2x_2}{3\,x_1^2} g = \frac{1}{2}x_1 f - \frac{1}{3}x_2 g = -\frac{1}{2}x_1^2 + \frac{1}{3}x_2^2.$$

S-Polynomials and Buchberger's Algorithm

Theorem (Buchberger Criterion)

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ a term order. Then the following are equivalent:

- *G is a Gröbner basis*
- *$S(g_i, g_j) \xrightarrow{G}_+ 0$ for all $1 \leqslant i < j \leqslant s$.*

The proof of the result is technical and complicated. We first show that the theorem provides an algorithm for finding Gröbner bases.

Buchberger's Algorithm

Data: $F = \{f_1, \ldots, f_s\} \in \mathbb{K}[x_1, \ldots, x_n]$ with $f_i \neq 0$, $i = 1, \ldots, s$
Result: $G = \{g_1, \ldots, g_t\}$ Gröbner basis of (F)
$G := F$, $\mathcal{S} := \{\{f_i, f_j\} \mid 1 \leqslant i < j \leqslant s\}$.
while $\mathcal{S} \neq \emptyset$ **do**
  Choose $\{f, g\} \in \mathcal{S}$;
  $\mathcal{S} := \mathcal{S} \setminus \{\{f, g\}\}$;
  $S(f, g) \xrightarrow{G}_+ h$ for h reduced with respect to G;
  if $h \neq 0$ **then**
    $\mathcal{S} := \mathcal{S} \cup \{\{u, h\} \mid u \in G\}$;
    $G := G \cup \{h\}$;
  end
end
return G;

Buchberger's Algorithm

Example

$f_1 = x_1x_2 - x_2, f_2 = -x_1 - x_2^2 \in \mathbb{Q}[x_1, x_2], \prec = \text{lex}$

- Initializtion: $G = \{f_1, f_2\}$, $\mathcal{S} = \{\{f_1, f_2\}\}$
- First pass through while loop

$\mathcal{S} := \mathcal{S} \setminus \{\{f_1, f_2\}\} = \emptyset;$
$S(f_1, f_2) \xrightarrow{G}_+ x_2^3 - x_2 =: h =: f_3;$
$\mathcal{S} := \{\{f_1, f_3\}, \{f_2, f_3\}\};$
$G := \{f_1, f_2, f_3\};$

Buchberger's Algorithm

Example

- Second pass through while loop

$\mathcal{S} := \mathcal{S} \setminus \{\{f_1, f_3\}\} = \{\{f_2, f_3\}\};$

$S(f_1, f_3) \xrightarrow{G}_+ 0 =: h;$

Buchberger's Algorithm

Example

- Third pass through while loop

$\mathcal{S} := \mathcal{S} \setminus \{\{f_2, f_3\}\} = \emptyset$;

$S(f_2, f_3) \xrightarrow{G}_+ 0 =: h$;

Return $G = \{f_1, f_2, f_3\}$;

Buchberger's Algorithm

Theorem

Buchberger's algorithm terminates and is correct.

Proof.

Assumption: The algorithm does not terminate

$\Rightarrow$ There exist infinitly many iterations in which h is added to G

Set $G_1 := F$ and set G_i to be the set G after the ith $h =: h_i$ was added.

$$\Rightarrow G_1 \subset G_2 \subset \cdots$$

is strictly ascending $\square$

Buchberger's Algorithm

Proof.

$h_i \neq 0$ is reduced with respect to $G_{i-1} \Rightarrow \mathrm{lm}_{\preceq}(h_i) \notin \mathrm{in}_{\preceq}\Big(\{G_{i-1}\}\Big)$
$\Rightarrow$

$$\mathrm{in}_{\preceq}\Big(\{G_1\}\Big) \subset \mathrm{in}_{\preceq}\Big(\{G_2\}\Big) \subset \mathrm{in}_{\preceq}\Big(\{G_3\}\Big) \subset \cdots$$

Is a strictly ascending chain of monomial ideals. □

Buchberger's Algorithm

Proof.

$$M := \bigcup_{i=1}^{\infty} \left\{ \mathrm{lm}_{\preceq}(g) \mid g \in G_i \right\}$$

$\xrightarrow{\text{Dickson Lemma}}$ exist $m_1, \ldots, m_r \in M$ with $(m_1, \ldots, m_r) = (M)$.

Let i' be such that

$$m_1, \ldots, m_r \in \bigcup_{i=1}^{i'} \left\{ \mathrm{lm}_{\preceq}(g) \mid g \in G_i \right\}$$

$\Rightarrow \mathrm{in}_{\preceq}\Big((G_i) \Big) = (M)$, $i \geqslant i' \Rightarrow$ contradiction $\Rightarrow$ algorithm terminates. □

Buchberger's Algorithm

Proof.

Remains to show that the algorithm is correct and returns a Gröbner basis

$$(f_1, \ldots, f_s) \subseteq (g_1, \ldots, g_t) \subseteq (f_1, \ldots, f_s)$$

$$\Rightarrow (g_1, \ldots, g_t) = (f_1, \ldots, f_s)$$

$S(g_i, g_j) \xrightarrow{G}_+ 0$ for $1 \leqslant i < j \leqslant t$ by termination criterion.

$$\xRightarrow{\text{Buchberger Criterion}} G = \{g_1, \ldots, g_t\} \text{ is a Gröbner basis.}$$ □

S-Polynomials and Buchberger's Algorithm

Let us return to the proof of:

Theorem (Buchberger's Criterion)

Let $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and $\prec$ a term order. Then the following are equivalent:

- *G is a Gröbner basis*
- *$S(g_i, g_j) \xrightarrow{G}_+ 0$ for all $1 \leqslant i < j \leqslant s$.*

S-Polynomials and Buchberger's Algorithm

Lemma

Let $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, $f = \sum_{i=1}^{s} c_i f_i$, $c_i \in \mathbb{K}$ *and* $\prec$ *a term order.*
If

- $\mathrm{lm}_{\preceq}(f_1) = \cdots = \mathrm{lm}_{\preceq}(f_2) = \underline{x}^{\alpha}$
- $\mathrm{lm}_{\preceq}(f) \prec \underline{x}^{\alpha}$

Then f *is a linear combination of* $S(f_i, f_j)$, $1 \leqslant i < j \leqslant s$, *with coefficients in* $\mathbb{K}$.

S-Polynomials and Buchberger's Algorithm

Proof.

- $f_i = a_i \underline{x}^{\alpha} +$ lower terms
- $S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$

$$
\begin{aligned}
f &= c_1 f_1 + \cdots + c_s f_s \\
&= c_1 a_1 \frac{1}{a_1} f_1 + \cdots + c_s a_s \frac{1}{a_s} f_s \\
&= c_1 a_1 \left(\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) + (c_1 a_1 + c_2 a_2) \left(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3 \right) + \\
&\quad \cdots + (c_1 a_1 + \cdots + c_{s-1} a_{s-1}) \left(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s \right) + \\
&\quad (c_1 a_1 + \cdots + c_s a_s) \frac{1}{a_s} f_s \\
&= c_1 a_1 S(f_1, f_2) + \cdots + (c_1 a_1 + \cdots + c_{s-1} a_{s-1}) S(f_{s-1}, f_s)
\end{aligned}
$$

S-Polynomials and Buchberger's Algorithm

Proof of Buchberger Criterion.

- "$\Rightarrow$"

$G = \{g_1, \ldots, g_s\}$ Gröbner basis of $I = (g_1, \ldots, g_s) \Rightarrow S(g_i, g_i) \in I$ and $S(g_i, g_j) \xrightarrow{G}_+ 0$ $\square$

S-Polynomials and Buchberger's Algorithm

Proof of Buchberger Criterion.

- "$\Leftarrow$"

We use

G Gröbner basis $\Leftrightarrow$

$$f \in I = (g_1, \ldots, g_s) \Leftrightarrow f = h_1 g_1 + \cdots + h_s g_s \text{ with}$$
$$\mathrm{lm}_{\preceq}(f) = \max_{\preceq}\left\{\mathrm{lm}_{\preceq}(h_i)\mathrm{lm}_{\preceq}(g_i) \mid i = 1, \ldots, s\right\}$$
$$\text{and } h_i \in \mathbb{K}[x_1, \ldots, x_n], i = 1, \ldots, s.$$

The "$\Leftarrow$" directions of the criterion is trivial. $\square$

S-Polynomials and Buchberger's Algorithm

Proof of Buchberger Criterion.

$f \in I = (g_1, \ldots, g_s) \Rightarrow f = h_1 g_1 + \cdots + h_s g_s$ for $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$

For fixed f choose $h_1, \ldots, h_s$ such that

$$\underline{x}^{\alpha} = \max_{\prec} \left\{ \mathrm{lm}_{\preceq}(h_i)\mathrm{lm}_{\prec}(g_i) \mid i = 1, \ldots, s \right\}$$

is minimal

Case : $\underline{x}^{\alpha} = \mathrm{lm}_{\preceq}(f)$
$\Rightarrow$ we are done

Case : $\underline{x}^{\alpha} \succ \mathrm{lm}_{\preceq}(f)$
$T := \left\{ i \;\middle|\; \underline{x}^{\alpha} = \mathrm{lm}_{\preceq}(h_i)\mathrm{lm}_{\preceq}(g_i) \right\}$ □

S-Polynomials and Buchberger's Algorithm

Proof of Buchberger Criterion.

$h_i = d_i \operatorname{lm}_\prec(h_i) +$ smaller terms, $\qquad g := \sum_{i\in T} d_i \operatorname{lm}_\preceq(h_i)\, g_i$

$\Rightarrow \operatorname{lm}_\preceq\left(d_i \operatorname{lm}_\preceq(h_i)\, g_i\right) = \underline{x}^\alpha,\ i \in T$ and $\operatorname{lm}_\preceq(g) \prec \underline{x}^\alpha \xrightarrow{\text{Lemma}}$ exist $d_{ij} \in \mathbb{K}$ such that

$$g = \sum_{\substack{i,j\in T \\ i\neq j}} d_{ij} S\Big(\operatorname{lm}_\preceq(h_i)g_i, \operatorname{lm}_\preceq(h_j)g_j\Big)$$

$$\underline{x}^\alpha = \operatorname{lcm}\Big(\operatorname{lm}_\preceq(h_i g_i), \operatorname{lm}_\preceq(h_j g_j)\Big) \xrightarrow{\operatorname{lc}_\preceq(\operatorname{lm}_\preceq(h_i)g_i)=\operatorname{lc}_\preceq(g_i)}$$

$$\begin{aligned}
&S\Big(\operatorname{lm}_\preceq(h_i)g_i, \operatorname{lm}_\preceq(h_j)g_j\Big) \\
=&\frac{\underline{x}^\alpha}{\operatorname{lc}_\preceq(g_i)\operatorname{lm}_\preceq(\operatorname{lm}_\preceq(h_i)g_i)}\operatorname{lm}_\preceq(h_i)g_i - \frac{\underline{x}^\alpha}{\operatorname{lc}_\preceq(g_j)\operatorname{lm}_\preceq(\operatorname{lm}_\preceq(h_j)g_j)}\operatorname{lm}_\preceq(h_j)g_j \\
=&\frac{\underline{x}^\alpha}{\operatorname{lc}_\preceq(g_i)lm_\preceq(g_i)}g_i - \frac{\underline{x}^\alpha}{\operatorname{lc}_\preceq(g_i)\operatorname{lm}_\preceq(g_j)}g_j \\
=&\frac{\underline{x}^\alpha}{\qquad\qquad}S(g_i, g_j)
\end{aligned}$$

S-Polynomials and Buchberger's Algorithm

Proof of Buchberger Criterion.

$$\xRightarrow{\text{Assumption}} S(g_i, g_j) \xrightarrow{G}_+ 0$$

$$\xRightarrow{\text{Easy Exercise}} \frac{\underline{x}^{\alpha}}{\operatorname{lcm}(\operatorname{lm}_{\preceq}(g_i), \operatorname{lm}_{\preceq}(g_j))} S(g_i, g_j) \xrightarrow{G}_+ 0$$

$$\Rightarrow S\left(\operatorname{lm}_{\preceq}(h_i) g_i, \operatorname{lm}_{\preceq}(h_j) g_j\right) \xrightarrow{G}_+ 0$$

□

S-Polynomials and Buchberger's Algorithm

Proof of Buchberger Criterion.

$\Rightarrow$

exist $h_{i,j,\ell}, 1 \leqslant \ell \leqslant s$:

$$S\left(\mathrm{lm}_{\preceq}(h_i)g_i, \mathrm{lm}_{\preceq}(h_j)g_j\right) = \sum_{\ell=1}^{s} h_{i,j,\ell} g_\ell$$

and

$$\begin{aligned}\max_{1\leqslant\ell\leqslant s}\left(\mathrm{lm}_{\preceq}(h_{i,j,\ell})\mathrm{lm}_{\preceq}(g_\ell)\right) &= \mathrm{lm}_{\preceq}(S(\mathrm{lm}_{\preceq}(h_i)g_i, \mathrm{lm}_{\preceq}(h_j)g_j)) \\ &\prec \max_{\preceq}(\mathrm{lm}_{\preceq}(h_i)g_i, \mathrm{lm}_{\preceq}(h_j)g_j)) \\ &= \underline{x}^{\alpha}\end{aligned}$$

$\Rightarrow$

$$\mathrm{lm}_{\preceq}(\sum_{i\in T} h_i g_i) = \mathrm{lm}_{\preceq}(\sum_{i\in T} \mathrm{lm}_{\preceq}(h_i)g_i) \prec \underline{x}^{\alpha}$$

$\Rightarrow$ Contradiction

Minimal Grobner Basis

A set G is said to be minimal Grobner basis if

1. G is Grobner Basis
2. $\nexists$ any $g_i, g_j \in G$ such that $lm(g_j)/lm(g_i)$ or $lm(g_i)/lm(g_j)$

Note:
Minimal Grobner Basis is not unique but if G_1 and G_2 be two minimal Grobner Basis for some ideal I then $|G_1| = |G_2|$.

Reduced Grobner Basis

A set $G = \{g_1, \ldots, g_k\}$ is said to be Reduced Grobner basis if:

1. G is Grobner Basis
2. $\forall g \in G$ no term in g is divisible by any of the $lm(g_i); \forall i = 1, \ldots, k$

Reduced Grobner basis is always unique

Remark: R.G.B $\Rightarrow$ M.G.B $\Rightarrow$ G.B

But Converse is not true (in General)

How to find Reduced Grobner Basis

1. Use Buchburgers Algorithm to find G.B
2. Find Minimal Grobner Basis $\rightarrow \{g_1, \ldots, g_k\}$
3. $g_1 \xrightarrow{\{g_2,\ldots,g_k\}}_+ h_1$
   $g_2 \xrightarrow{\{h,g_3,\ldots,g_k\}}_+ h_2$
   $g_3 \xrightarrow{\{h_1,h_2,g_4,\ldots,g_k\}}_+ h_3$

   $\vdots$

   $g_k \xrightarrow{\{h_1,h_2,\ldots,h_{k-1}\}}_+ h_k$
   $\Rightarrow \{h_1, h_2, \ldots, h_k\}$ is reduced grobner basis.

10. Applications of Gröbner basis

Weak Hilbert Nullstellensatz

Statement:
Let I be an ideal contained in $k[x_1, \ldots, x_n]$. Then $V_{\overline{K}}(I) = \emptyset$ if and only if $I = k[x_1, \ldots, x_n]$.
Proof:
let $1 \in I \Rightarrow$ G.B $\Rightarrow \{1\} \in G \iff I = k[x_1, \ldots, x_n]$.
Result:
$V_{\overline{K}}(I) = \emptyset$ if and only if $1 \in G$ (i.e., given polynomials $f_1, \ldots, f_s$, then there are no solutions to the system $f_1 = 0, f_2 = 0, \ldots, f_s = 0$ in $\overline{K}^n$ if and only if $G = \{1\}$).
Proof:
$V_{\overline{K}}(I) = \emptyset$ if and only if $1 \in I$. But this condition is equivalent to $G = \{1\}$, since G is the reduced Gröbner basis.

Elimination

For X_1, X_2 power products in the x variables and Y_1, Y_2 power products in the y variables, we define

$$X_1 Y_1 < X_2 Y_2 \iff \begin{cases} X_1 <_x X_2 \\ \text{ or} \\ X_1 = X_2 \text{ and } Y_1 <_y Y_2. \end{cases}$$

This term order is called an elimination order with the x variables larger than the y variables.
Assignment: Elimination order is a monomial order.

Thereom

Let I be a non-zero ideal of $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$, and let $<$ be an elimination order with the x variables larger than the y variables. Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for this ideal. Then $G \cap k[y_1, \ldots, y_m]$ is a Gröbner basis for the ideal $I \cap k[y_1, \ldots, y_m]$.

Remark: The ideal $I \cap k[y_1, \ldots, y_m]$ is called an elimination ideal, since the x variables have been "eliminated".

Proposition

Let I, J be ideals in $k[x_1, \ldots, x_n]$, and let w be a new variable. Consider the ideal $\langle wI, (1-w)J \rangle$ in $k[x_1, \ldots, x_n, w]$. Then

$$I \cap J = \langle wI, (1-w)J \rangle \cap k[x_1, \ldots, x_n].$$

Proof. Let $f \in I \cap J$. Since $f = wf + (1-w)f$, we have $f \in \langle wI, (1-w)J \rangle \cap k[x_1, \ldots, x_n]$. Conversely, suppose that $f \in \langle wI, (1-w)J \rangle \cap k[x_1, \ldots, x_n]$. Then, since $f \in \langle wI, (1-w)J \rangle \subseteq k[x_1, \ldots, x_n, w]$, we have

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{s} wf_i(x_1, \ldots, x_n) h_i(x_1, \ldots, x_n, w) + \sum_{j=1}^{p} (1-w) f'_j(x_1, \ldots, x_n) h'_j(x_1, \ldots, x_n, w).$$

Since w does not appear in $f(x_1, \ldots, x_n)$, we can let $w = 1$ and get $f \in I$, and then let $w = 0$ and get $f \in J$. $\Rightarrow f \in I \cap J$.

Example:
Consider the following ideals in $\mathbb{Q}[x, y]$;
$I = \langle x^2 + y^3 - 1, x - yx + 3 \rangle$ and $J = \langle x^2 y - 1 \rangle$ We wish to compute $I \cap J$.
We compute a Grobner basis G for the ideal
$\langle w(x^2 + y^3 - 1), w(x - yx + 3), (1 - w)(x^2 y - 1) \rangle \subseteq \mathbb{Q}[x, y, w]$;
deglex $x > y$ and an elimination order $w > x > y$.
Sol:
$G = \{x^3y^2 - x^3y - 3x^2y - xy + x + 3, x^2y^4 + x^4y - x^2y - y^3 - x^2 + 1, 12853w + 118x^4y + 9x^2y^3 - 357x^3y - 972x^2y^2 + 2152x^2y - 118x^2 - 9y^2 + 357x + 972y - 2152, x^5y + 3x^2y^3 + 3x^2y^2 - x^3 + 3x^2y - 3y^2 - 3y - 3\}$.
So, a Gröbner basis for the ideal $I \cap J$ is
$\{x^3y^2 - x^3y - 3x^2y - xy + x + 3, x^2y^4 + x^4y - x^2y - y^3 - x^2 + 1, x^5y + 3x^2y^3 + 3x^2y^2 - x^3 + 3x^2y - 3y^2 - 3y - 3\}$.

lemma

Statement:

For $f, g \in k[x_1, \ldots, x_n]$, both non-zero, we have $\langle f \rangle \cap \langle g \rangle = \langle lcm(f, g) \rangle$.

Proof:

$\langle f \rangle$. Let $h \in \langle f \rangle \cap \langle g \rangle$,

$\Rightarrow h \in \langle f \rangle$ and $h \in \langle g \rangle$,

h is multiple of f

h is multiple of g

h is multiple of $\langle lcm(f, g) \rangle$

Conversaly,

h is multiple of $f \Rightarrow h \in \langle f \rangle$

h is multiple of $g \Rightarrow h \in \langle g \rangle$

$h \in \langle f \rangle \cap \langle g \rangle$,

$\Rightarrow \langle f \rangle \cap \langle g \rangle = \langle lcm(f, g) \rangle$.

Quotient Ideal

Let I and J be ideals in $k[x_1, \ldots, x_n]$. The ideal quotient $J : I$ is defined to be

$$J : I = \{g \in k[x_1, \ldots, x_n] \mid gI \subseteq J\}.$$

LEMMA

Let $I \models \langle f_1, \ldots, f_s \rangle$ and J be ideals in $k[x_1, \ldots, x_n]$. Then

$$J : I = \bigcap_{i=1}^{s} J : \langle f_i \rangle$$

Proof.
If $g \in J : I$, then $gI \subseteq J$, so in particular $gf_i \in J$ for $i = 1, \ldots, s$, and hence $g \in \bigcap_{i=1}^{s} J : \langle f_i \rangle$.
Conversely,
if $g \in \bigcap_{i=1}^{s} J : \langle f_i \rangle$, then $g\,(f_i\rangle \subseteq J$ for $i = 1, \ldots, s$, and hence $gI \subseteq J$, so that $g \in J : I$.
$\Rightarrow J : I = \bigcap_{i=1}^{s} J : \langle f_i \rangle$
Remark:
we only need to concentrate on computing $J : \langle f \rangle$ for a single polynomial f.

Example:
Let $g_1 = x(x+y)^2$, $g_2 = y$ $f_1 = x^2$, $f_2 = x+y$ in $\mathbb{Q}[x,y]$.
Consider the ideals $I = \langle f_1, f_2 \rangle$ and $J = \langle g_1, g_2 \rangle$. Compute $J : I$.
Sol:

$$J : I = (J : \langle f_1 \rangle) \bigcap (J : \langle f_2 \rangle)$$

and so by previous Lemma

$$J : I = \frac{1}{f_1} (J \cap \langle f_1 \rangle) \bigcap \frac{1}{f_2} (J \cap \langle f_2 \rangle) .$$

First we compute $J \cap \langle f_1 \rangle$ by computing a Gröbner basis G_1 for the ideal $\langle wg_1, wg_2, (1-w)f_1 \rangle \subseteq \mathbb{Q}[x,y,w]$ with respect to the lex term ordering with $w > x > y$ to obtain

$$G_1 = \left\{ x^2 w - x^2, wy, x^3, x^2 y \right\},$$

so that $\frac{1}{f_1} (J \cap \langle f_1 \rangle) = \langle x, y \rangle$.

Second;
we compute $J \cap \langle f_2 \rangle$ by computing a Gröbner basis G_2 for the ideal $\langle wg_1, wg_2, (1-w)f_2 \rangle \subseteq \mathbb{Q}[x, y, w]$ using the same order as above, and we obtain

$$G_2 = \left\{ wx - x - y, wy, x^3 + y^3, xy + y^2 \right\},$$

so that $\frac{1}{f_2}\left(J \cap \langle f_2 \rangle\right) = \left\langle x^2 - xy + y^2, y \right\rangle$.
Finally
Compute $\langle x, y \rangle \cap \left\langle x^2 - xy + \ y^2, y \right\rangle$ by computing a Gröbner basis G for the ideal $\left\langle wx, wy, (1-w)\left(x^2 - xy + \right.\right.$
$\left.\left. y^2\right), (1-w)y \right\rangle \subseteq \mathbb{Q}[x, y, w]$ with respect to the lex ordering with $w > x > y$, to obtain

$$G = \left\{ wx, x^2, y \right\}$$

Therefore $J : I = \left\langle x^2, y \right\rangle$.

Lemma

Let J be an ideal and $f \neq 0$ be a polynomial in $k[x_1, \ldots, x_n]$. Then

$$J : \langle f \rangle = \frac{1}{f}(J \cap (f\rangle)$$

Proof:
If $g \in \frac{1}{f}(J \cap \langle f \rangle)$, then $gf \in J$, and hence $g \in J : \langle f \rangle$.
Conversely,
if $g \in J : \langle f \rangle$, then $gf \in J$, and hence $gf \in J \cap \langle f \rangle$, so that $g \in \frac{1}{f}(J \cap \langle f \rangle)$.

Polynomial Maps

Consider a k-algebra homomorphism is a ring homomorphism defined as: $Q : k[y_1, \ldots, y_n] \to k[x_1, \ldots, x_n]$

$y_i \to k[x_1, \ldots, x_n]$

Example:

$Q : k[y_1, y_2, y_3] \to k[x_1, x_2, x_3]$

$y_1 \to x_1 + x_2 + x_3$

$y_2 \to x_1^2 - x_2^2 - x_3^2$

$\phi(2y_1^2 + 3y_2^3 + y_1y_2) = 2\phi(y_1)^2 + 3(\phi(y_2))^3 + \phi(y_1)\phi(y_2)$

$\phi(2y_1^2 + 3y_2^3 + y_1y_2) =$

$2(x_1 + x_2 + x_3)^2 + 3(x_1^2 - x_2^2 - x_3^2)^3 + (x_1 + x_2 + x_3)(x_1^2 - x_2^2 - x_3^2)$

LEMMA

Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be elements of a commutative ring R. Then the element $a_1 a_2 \cdots a_n - b_1 b_2 \cdots b_n$ is in the ideal $\langle a_1 - b_1, a_2 - \ b_2, \ldots, a_n - b_n \rangle$.

Proof

The proof is easily done by induction using the fact that

$$a_1 a_2 \cdots a_n - b_1 b_2 \cdots b_n = a_1 \left(a_2 \cdots a_n - b_2 \cdots b_n\right) + b_2 \cdots b_n \left(a_1 - b_1\right).$$

Theorem

Let $\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n]$ and
$y_i \longrightarrow f(x_1, \ldots, x_n)$.
Let $K = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$, Then
$ker(\phi) = K \cap k[y_1, \ldots, y_m]$.
Proof:
Let $g \in K \cap k[y_1, \ldots, y_\infty]$. Then

$$g(y_1, \ldots, y_m) = \sum_{i=1}^{m} (y_i - f_i(x_1, \ldots, x_n)) h_i(y_1, \ldots, y_m, x_1, \ldots, x_n),$$

where $h_i \in k[y_1, \ldots, y_m, x_1, \ldots, x_n]$.
Therefore g is zero when evaluated at $(y_1, \ldots, y_m) = (f_1, \ldots, f_m)$
and hence $g \in ker(\phi)$.

Conversely,
let $g \in ker\phi$. We can write $g = \sum_{\nu} c_{\nu} y_1^n \cdots y_m^{\nu}$, where
$c_{\nu} \in k, \nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}^n$, Since $g \in ker\phi$
$\Rightarrow g = g(y_1, \ldots, y_m)$
$\phi(g) = g(f_1, \ldots, f_m) = 0$
$\phi(g) = 0$
$g = g - 0 = g - \phi(g)$
$g = g - g(f_1, \ldots, f_m)$
$g = \sum_{finte} C_v (y_1{}^{v_1} \cdots y_m^{v_m} - f_1{}^{v_1} \cdots f_m{}^{v_m})$
By previous lemma, $g \in K$
but $g \in K[(y_1, \ldots, y_m)]$
$\Rightarrow g \in K \cap k[y_1, \ldots, y_m]$.
Hence,
$ker(\phi) = K \cap k[y_1, \ldots, y_m]$.

Theorem

Statement:
Let $K = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ be the ideal considered in Theorem 2.4.2, and let G be the reduced Gröbner basis for K with respect to an elimination order with the x variables larger than the y variables. Then $f \in k[x_1, \ldots, x_n]$ is in the image of ϕ if and only if there exists $h \in k[y_1, \ldots, y_m]$ such that $f \xrightarrow{G} +h$. In this case, $f = \phi(h) = h(f_1, \ldots, f_m)$.

Proof. Let $f \in k[x_1, \ldots, x_n]$ be in $\mathrm{im}(\phi)$. Then $f = g(f_1, \ldots, f_m)$ for some $g \in k[y_1, \ldots, y_m]$. Consider the polynomial

$$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m, x_1, \ldots, x_n].$$

Note that
$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) = g(f_1, \ldots, f_m) - g(y_1, \ldots, y_m)$,
and hence, using Lemma 2.4.1, we see that
$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m)$ is in K. Therefore, by Proposition 2.1.4, $g \xrightarrow{G} +h$, and $f \xrightarrow{G} +h$, where $h = N_G(g) = N_G(f)$. But, since $g \in k[y_1, \ldots, y_m]$, g can only be reduced by polynomials in G which have leading terms in the y variables alone. Since the x variables are larger than the y variables in our elimination order, the polynomials used to reduce g are in $k[y_1, \ldots, y_m]$. Therefore $h \in k[y_1, \ldots, y_m]$.

Theorem

Conversely, let $f \xrightarrow{G} h$, where $h \in k[y_1, \ldots, y_m]$. Then $f - h \in K$, so

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = \sum_{i=1}^{m} g_i(y_1, \ldots, y_m, x_1, \ldots, x_n)(y_i - f_i(x_1, \ldots, x_n)).$$

If we substitute f_i for y_i, we see that $f = h(f_1, \ldots, f_m) = \phi(h)$, and f is in the image of ϕ.

Theorem

Statement: Let $K = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ be the ideal considered in Theorem 2.4.2, and let G be the reduced Gröbner basis for K with respect to an elimination order with the x variables larger than the y variables. Then ϕ is onto if and only if for each $i = 1, \ldots, n$, there exists $g_i \in G$ such that $g_i = x_i - h_i$, where $h_i \in k[y_1, \ldots, y_m]$. Moreover, in this case, $x_i = h_i(f_1, \ldots, f_m)$.

Proof:

Let us first assume that ϕ is onto. Also, without loss of generality, let us assume that the order is such that $x_1 < \cdots < x_n$. Then by Theorem 2.4.4, since x_1 is in the image of ϕ, there exists $h_1' \in k[y_1, \ldots, y_m]$ such that $x_1 \xrightarrow{G} + h_1'$. Therefore $x_1 - h_1' \in K$, and hence there exists $g_1 \in G$ such that $\mathrm{Im}(g_1)$ divides $\mathrm{Im}(x_1 - h_1') = x_1$. Therefore, since the only terms strickly smaller than x_1 are terms in the y variables alone, $g_1 = x_1 - h_1$ for some $h_1 \in k[y_1, \ldots, y_m]$. Similarly, since x_2 is in the image of ϕ, there exists $h_2' \in k[y_1, \ldots, y_m]$ such that $x_2 \xrightarrow{G} h_2'$, and hence there exists $g_2 \in G$ such that $\mathrm{Im}(g_2)$ divides $\mathrm{Im}(x_2 - h_2') = x_2$. Since the only terms strictly smaller than x_2 are terms involving x_1 and the y variables only, and since G is the reduced Gröbner basis and any term involving x_1 could be reduced using $g_1 = x_1 - h_1$, we must have $g_2 = x_2 - h_2$ for some $h_2 \in k[y_1, \ldots, y_m]$. We proceed in a similar fashion for the remaining $x_i{}'s$.

The 3-Color Problem

We are given a graph G with n vertices with at most one edge between any two vertices. We want to color the vertices in such a way that only 3 colors are used, and no two vertices connected by an edge are colored the same way. If 9 can be colored in this fashion, then is called 3-colorable. This can be seen to be the same as the 3-color problem for a map: the vertices represent the regions to be colored, and two vertices are connected by an edge if the two corresponding regions are adjacent.
Each vertex is to be assigned one of the 3 colors 1, ω., ω^2. This can be represented by the following n equations:

$$x_i^3 - 1 = 0, \quad 1 < i < n.$$

Also, if the vertices x_i and x_j are connected by an edge, they need to have a different color. Since $x_i^3 = x_i$, we have $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. Therefore, x_i and x_j will have different colors if and only if

$$x_i + x_i x_j + x_j^2 = 0.$$

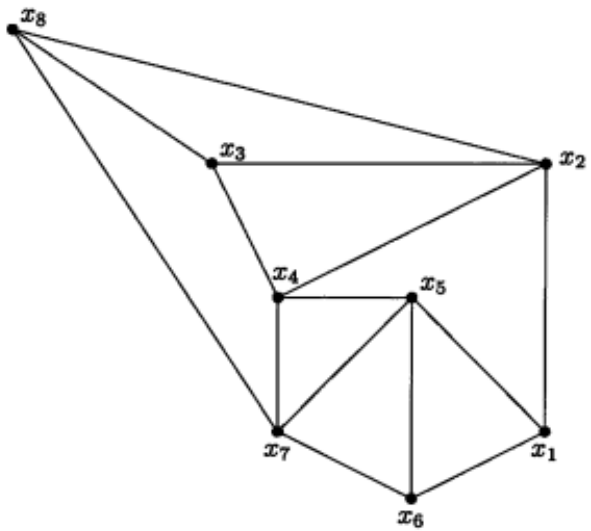
Theorem

The graph G is 3-colorable if and only if $V(I) = \emptyset$

Proof:

We can use Grobner bases to determine if $V(I) = 0$. We first compute a reduced Grobner basis for 1. If $1 \in G$, then $V(I) = 0$ and otherwise $V(I) \neq \emptyset$.

Example(3 colorable graph)



Consider the graph G. The polynomials corresponding to G are:
$x_i^3 - 1 = 0, i = \quad 1, \ldots, 8$ and $x_i^2 + x_i x^j + x_j^2$
For the pairs $(i, j) \in$
$\{(1,2),(1,5),(1,6),(2,3),(2,4),(2,8),(3,4),(3,8),(4,5),(4,7),$
$(5,6),(5,7),(6,7),(6,8)\}$.
Compute a Grobner basis G for the ideal I corresponding to the above polynomial with order lex $x_1 > x_2 > \ldots > x_8$
G=$\{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8, x_6 - x_8, x_7^2 +$
$x_7 X_8 + x_8^2, x_8^3 - 1.\}$ $1 \notin G \Rightarrow V(I) \neq \emptyset \Rightarrow G$ is 3−colorable.

Integer Programming

Integer programing is a sysytem whose solution is in form of non-negative integers.

- $No.ofequations = n \Rightarrow x_i$
- $No.ofvariables = m \Rightarrow y_i$

$$\begin{cases} a_{11}\sigma_1 + a_{12}\sigma_2 + \ldots + a_{1m}\sigma_m &= b_1, \\ a_{21}\sigma_1 + a_{22}\sigma_2 + \ldots + a_{2m}\sigma_m &= b_2, \\ a_{n1}\sigma_1 + a_{n2}\sigma_2 + \ldots + a_{nm}\sigma_m &= b_n, \end{cases}$$

Represent the equation as follow:
$x_i^{a_{i1}\sigma_1+\ldots+a_{im}\sigma_m} = x_i{}^{b_i}$, for $i = 1 \ldots n$

$$x_i^{a_{i1}\sigma_1+\cdots+a_{im}\sigma_m} = x_i^{b_i}$$

for $i = 1, \ldots, n$. Then System can be written as :

$$x_1^{a_{11}\sigma_1+\cdots+a_{1m}\sigma_m} \ldots x_n^{a_{n1}\sigma_1+\cdots+a_{nm}\sigma_m} = x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n},$$

or equivalently,
(2.8.3)
$\left(x_1^{a_{11}} x_2^{a_{21}} \ldots x_n^{a_{n1}}\right)^{\sigma_1} \ldots \left(x_1^{a_{1m}} x_2^{a_{2m}} \ldots x_n^{a_{nm}}\right)^{\sigma_m} = x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}.$
Defines polynomial map:

$$\begin{aligned} k\left[y_1, \ldots, y_m\right] &\xrightarrow{\phi} k\left[x_1, \ldots, x_n\right] \\ y_i &\longmapsto x_1^{a_{1j}} x_2^{a_{2j}} \ldots x_n^{a_{nj}}. \end{aligned}$$

Example:

$$\begin{cases} 3\sigma_1 + 2\sigma_2 + \sigma_3 + \sigma_4 = 10 \\ 4\sigma_1 + \sigma_2 + \sigma_3 = 5 \end{cases}$$

We have two x variables, x_1, x_2, one for each equation. We also have four y variables, y_1, y_2, y_3, y_4, one for each unknown.
map is

$$\begin{aligned} \mathbb{Q}[y_1, y_2, y_3, y_4] &\xrightarrow{\Phi} [x_1, x_2] \\ y_1 &\longmapsto x_1^3 x_2^4 \\ y_2 &\longmapsto x_1^2 x_2 \\ y_3 &\longmapsto x_1 x_2 \\ y_4 &\longmapsto x_1 \end{aligned}$$

Define an ideal $K = \left\langle y_1 - x_1^3 x_2^4, y_2 - x_1^2 x_2, y_3 - x_1 x_2, y_4 - x_1 \right) \subseteq \mathbb{Q}[y_1, y_2, y_3, y_4, x_1, x_2]$.
The Gröbner basis for K with order lex $x_1 > x_2 > y_1 > y_2 > y_3 > y_4$ is $G = \{f_1, f_2, f_3, f_4, f_5\}$,
where
$f_1 = x_1 - y_4, f_2 = x_2 y_4 - y_3,$
$f_3 = x_2 y_3^3 - y_1, f_4 = y_2 - y_3 y_4, f_5 = y_1 y_4 - y_3^4.$
Then
$x_1^1 0 x_2^5 \xrightarrow{f_1, f_2} y_3^5 y_4^5$
h is reduced with respect to G.
$\Rightarrow (0, 0, 5, 5)$ is a solution of System.

Modules and Grobner Bases

Definition:
For monomials $\boldsymbol{X} = X\boldsymbol{e}_i$ and $\boldsymbol{Y} = Y\boldsymbol{e}_j$ of A^m, we say that

$$\boldsymbol{X} < \boldsymbol{Y} \iff \begin{cases} X \notin Y \\ \text{ or} \\ X = Y \text{ and } i < j. \end{cases}$$

We call this order TOP for **"term over position"**, since it places more importance on the term order on A than on the position in the vector.
So, for example, in the case of two variables and $m = 2$, using deglex on the power products of A with $x < y$, we see that

$$(x, 0) < (0, x) < (y, 0) < (xy, 0).$$

Definition:
For monomials $\boldsymbol{X} = X\boldsymbol{e}_i$ and $\boldsymbol{Y} = Y\boldsymbol{e}_j$ of A^m, we say that

$$\boldsymbol{X} < \boldsymbol{Y} \iff \begin{cases} i < j \\ \text{ or} \\ i = j \text{ and } X < Y. \end{cases}$$

We call this order POT for **"position over term"**, since it places more importance on the position in the vector than on the term order on A.
So in this case we have, again for the case of two variables and $m = 2$, using deglex on the power products of A with $x < y$,

$$(x, 0) < (y, 0) < (xy, 0) < (0, x).$$

DEFINITION:

Given $f, g, hinA^m, g \neq 0$, we say that f reduces to h modulo g in one step, written $f \xrightarrow{g} h$, if and only if $It(g)$ divides a term X that appears in f and $h = f - \frac{X}{Lt(g)}g$ **Example:**

Let $f = (-y^3 + 2x^3y, 3xy^2 + y^2 + 4x)$ and $g = (x + 1, y^2 + x)$. We use the lex ordering with $x < y$, and TOP with $e_1 < e_2$. Then, $It(g) = (0, y^2) = y^2e_2$, and

$f - \frac{X}{Lt(g)}g$

$f \to f - \frac{3xy^2}{y^2}g$

$\Rightarrow ({}^{3}_{y}+2x^3y - 3x^2 - 3x, y^2 - 3x^2 + 4x)$.

Again by division, we get:

$\Rightarrow (-y^3 + 2x^3y - 3x^2 - 4x - 1, -3x^2 + 3x)$.

S-polynomial

Definition:
Let $0 \neq f, g \in S^m$. Let $L = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$.
The vector
$S(f, g) = \frac{L}{lt(f)}(f) - \frac{L}{lt(g)}(g)$
is called the S-polynomial of f and g.