# An Introduction To Gröbner Basis

Speakers: Sarasij Maitra and Stephanie Shand

University of Virginia

# Motivation

- Gröbner bases (GB) are a tool for doing explicit algorithmic calculations in a polynomial ring over a field or a homomorphic image of a polynomial ring over a field.

# Motivation

- Gröbner bases (GB) are a tool for doing explicit algorithmic calculations in a polynomial ring over a field or a homomorphic image of a polynomial ring over a field.
- While they mainly help in computations, they can also be used to prove substantial theorems, such as Hilbert Basis Theorem, Hilbert's Syzygy Theorem, etc.

## Motivation

- Gröbner bases (GB) are a tool for doing explicit algorithmic calculations in a polynomial ring over a field or a homomorphic image of a polynomial ring over a field.
- While they mainly help in computations, they can also be used to prove substantial theorems, such as Hilbert Basis Theorem, Hilbert's Syzygy Theorem, etc. (Of course, any systematic study generates it own problems as well.)

**Key Idea**

Monomials are easy to work with.

**Key Idea**

Monomials are easy to work with.

For instance,

• looking at partial derivatives $\frac{\partial}{\partial x_i}$ of monomials is essentially division by $x_i$

**Key Idea**

Monomials are easy to work with.

For instance,

• looking at partial derivatives $\frac{\partial}{\partial x_i}$ of monomials is essentially division by $x_i$

• etc.

# Two Important Computational Problems

**Membership Problem**

Given a finitely generated ideal $I$ and an element $f$, check whether $f \in I$?

# Two Important Computational Problems

## Membership Problem

Given a finitely generated ideal $I$ and an element $f$, check whether $f \in I$? More generally, given two ideals $I, J$, check whether $I \subset J$?

**A GB $G$ helps here by a method called reduction of $f$ by $G$.

# Two Important Computational Problems

## Membership Problem

Given a finitely generated ideal $I$ and an element $f$, check whether $f \in I$? More generally, given two ideals $I, J$, check whether $I \subset J$?

**A GB $G$ helps here by a method called reduction of $f$ by $G$.

## Elimination

Given a finite set of generators for an ideal $I \subset k[X_1, \ldots, X_n]$, can we find a finite set of generators for $I \cap k[X_{r+1}, \ldots, X_n]$, $1 \leq r \leq n-1$.

# Two Important Computational Problems

## Membership Problem

Given a finitely generated ideal $I$ and an element $f$, check whether $f \in I$? More generally, given two ideals $I, J$, check whether $I \subset J$?

**A GB $G$ helps here by a method called reduction of $f$ by $G$.

## Elimination

Given a finite set of generators for an ideal $I \subset k[X_1, \ldots, X_n]$, can we find a finite set of generators for $I \cap k[X_{r+1}, \ldots, X_n]$, $1 \leq r \leq n-1$.

Assuming $k$ is algebraically closed, this problem is deeply connected to finding the vanishing set ($V(I)$ or $\mathcal{Z}(I)$).

# Two Important Computational Problems

## Membership Problem

Given a finitely generated ideal $I$ and an element $f$, check whether $f \in I$? More generally, given two ideals $I, J$, check whether $I \subset J$?

**A GB $G$ helps here by a method called reduction of $f$ by $G$.

## Elimination

Given a finite set of generators for an ideal $I \subset k[X_1, \ldots, X_n]$, can we find a finite set of generators for $I \cap k[X_{r+1}, \ldots, X_n]$, $1 \leq r \leq n-1$.

Assuming $k$ is algebraically closed, this problem is deeply connected to finding the vanishing set ($V(I)$ or $\mathcal{Z}(I)$).

Check the Wikipedia page on Gröbner basis for many such computational problems where GB acts as a positive catalyst. Currently, it is being applied to applied fields like coding theory in error-correcting codes as well.

# Notations and Basic Setup

Throughout we will be concerned with (and often denote by $R$) the polynomial ring $k[x_1, \ldots, x_n]$ where $k$ is any field.

# Notations and Basic Setup

Throughout we will be concerned with (and often denote by $R$) the polynomial ring $k[x_1, \ldots, x_n]$ where $k$ is any field.

($R$ is Noetherian, so all ideals $I$ are finitely generated. This is called Hilbert Basis Theorem – this fact can be proved using Gröbner Basis as well without using the Noetherian assumption.)

## Notations and Basic Setup

Throughout we will be concerned with (and often denote by $R$) the polynomial ring $k[x_1, \dots, x_n]$ where $k$ is any field.

($R$ is Noetherian, so all ideals $I$ are finitely generated. This is called Hilbert Basis Theorem – this fact can be proved using Gröbner Basis as well without using the Noetherian assumption.)

A **monomial** is of the form $m = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ $(:= \boldsymbol{x}^A; A = (\alpha_1, \dots, \alpha_n)$; Write $|A| = \sum_i \alpha_i))$, where $\alpha_i \in \mathbb{Z}_+ \cup \{0\}$.

# Notations and Basic Setup

Throughout we will be concerned with (and often denote by $R$) the polynomial ring $k[x_1, \ldots, x_n]$ where $k$ is any field.

($R$ is Noetherian, so all ideals $I$ are finitely generated. This is called Hilbert Basis Theorem – this fact can be proved using Gröbner Basis as well without using the Noetherian assumption.)

A **monomial** is of the form $m = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ $(:= \boldsymbol{x}^A; A = (\alpha_1, \ldots, \alpha_n)$; Write $|A| = \sum_i \alpha_i))$, where $\alpha_i \in \mathbb{Z}_+ \cup \{0\}$. Let $\mathcal{M}$ denote the collection of all such monomials.

# Notations and Basic Setup

Throughout we will be concerned with (and often denote by $R$) the polynomial ring $k[x_1, \ldots, x_n]$ where $k$ is any field.

($R$ is Noetherian, so all ideals $I$ are finitely generated. This is called Hilbert Basis Theorem – this fact can be proved using Gröbner Basis as well without using the Noetherian assumption.)

A **monomial** is of the form $m = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ $(:= \boldsymbol{x}^A; A = (\alpha_1, \ldots, \alpha_n)$; Write $|A| = \sum_i \alpha_i))$, where $\alpha_i \in \mathbb{Z}_+ \cup \{0\}$. Let $\mathcal{M}$ denote the collection of all such monomials.

A ***monomial ideal*** is an ideal generated by monomials.

# Notations and Basic Setup

Throughout we will be concerned with (and often denote by $R$) the polynomial ring $k[x_1, \ldots, x_n]$ where $k$ is any field.

($R$ is Noetherian, so all ideals $I$ are finitely generated. This is called Hilbert Basis Theorem – this fact can be proved using Gröbner Basis as well without using the Noetherian assumption.)

A **monomial** is of the form $m = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ $(:= \boldsymbol{x}^A; A = (\alpha_1, \ldots, \alpha_n)$; Write $|A| = \sum_i \alpha_i)$), where $\alpha_i \in \mathbb{Z}_+ \cup \{0\}$. Let $\mathcal{M}$ denote the collection of all such monomials.

A ***monomial ideal*** is an ideal generated by monomials.

A **term** is an element of the form $\lambda m$ where $\lambda \in k, m \in \mathcal{M}$.

## Orderings

- A ***term ordering*** $\tau$ (denoted $>_\tau$ ) is a partial ordering on $\mathcal{M}$ where:
  (a) for any monomial $a \in \mathcal{M}$ such that $a \neq 1$, then $a >_\tau 1$.

# Orderings

- A ***term ordering*** $\tau$ (denoted $>_\tau$ ) is a partial ordering on $\mathcal{M}$ where:

  (a) for any monomial $a \in \mathcal{M}$ such that $a \neq 1$, then $a >_\tau 1$.

  (b) if $a, b, c \in \mathcal{M}$ with $a >_\tau b$, then $ac >_\tau bc$.

# Orderings

- A ***term ordering*** $\tau$ (denoted $>_\tau$ ) is a partial ordering on $\mathcal{M}$ where:
  (a) for any monomial $a \in \mathcal{M}$ such that $a \neq 1$, then $a >_\tau 1$.
  (b) if $a, b, c \in \mathcal{M}$ with $a >_\tau b$, then $ac >_\tau bc$.
- A ***monomial ordering*** $\tau$ (notated $>_\tau$ ) is a term ordering on $\mathcal{M}$ such that $>_\tau$ is a total ordering.
- A ***degree-wise monomial ordering*** is a monomial ordering which respects the degrees of a monomial.

### Example

Let $R = k[X, Y, Z]$ and $\tau$ be a monomial ordering such that $X >_\tau Y >_\tau Z$. Consider the degree 2 monomials.

### Example

Let $R = k[X, Y, Z]$ and $\tau$ be a monomial ordering such that $X >_\tau Y >_\tau Z$. Consider the degree 2 monomials. Multiplying by $X$, $Y$ and $Z$ we get the respective inequalities:

$$X^2 >_\tau XY >_\tau XZ, XY >_\tau Y^2 >_\tau YZ, XZ >_\tau YZ >_\tau Z^2$$

.

## Example

Let $R = k[X, Y, Z]$ and $\tau$ be a monomial ordering such that $X >_\tau Y >_\tau Z$. Consider the degree 2 monomials. Multiplying by $X, Y$ and $Z$ we get the respective inequalities:

$$X^2 >_\tau XY >_\tau XZ, XY >_\tau Y^2 >_\tau YZ, XZ >_\tau YZ >_\tau Z^2$$

. Hence

$$X^2 >_\tau XY >_\tau \begin{matrix} XZ \\ \\ Y^2 \end{matrix} >_\tau YZ >_\tau Z^2$$

## Example

Let $R = k[X, Y, Z]$ and $\tau$ be a monomial ordering such that $X >_\tau Y >_\tau Z$. Consider the degree 2 monomials. Multiplying by $X, Y$ and $Z$ we get the respective inequalities:

$$X^2 >_\tau XY >_\tau XZ, XY >_\tau Y^2 >_\tau YZ, XZ >_\tau YZ >_\tau Z^2$$

. Hence

$$X^2 >_\tau XY >_\tau \begin{matrix} XZ \\ \\ Y^2 \end{matrix} >_\tau YZ >_\tau Z^2$$

Thus, here we need to make a choice in degree 2, namely $XZ >_\tau Y^2$ or $Y^2 >_\tau XZ$.

# Types of Monomial Orderings

There are three different types of basic monomial orderings:

1. **Lex**: $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$ if and only if the first nonzero entry of $A - B$ is positive.

# Types of Monomial Orderings

There are three different types of basic monomial orderings:

1. **Lex**: $\mathbf{x}^A >_{lex} \mathbf{x}^B$ if and only if the first nonzero entry of $A - B$ is positive.
2. **Deglex**: $\mathbf{x}^A >_{deglex} \mathbf{x}^B$ if and only if either:
    1. $|A| > |B|$ or
    2. $|A| = |B|$ and $\mathbf{x}^A >_{lex} \mathbf{x}^B$.

# Types of Monomial Orderings

There are three different types of basic monomial orderings:

1. **Lex**: $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$ if and only if the first nonzero entry of $A - B$ is positive.
2. **Deglex**: $\boldsymbol{x}^A >_{deglex} \boldsymbol{x}^B$ if and only if either:
    1. $|A| > |B|$ or
    2. $|A| = |B|$ and $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$.
3. **Revlex**: $\boldsymbol{x}^A >_{revlex} \boldsymbol{x}^B$ if and only if either:
    1. $|A| > |B|$ or
    2. $|A| = |B|$ and the *last* nonzero entry of $A - B$ is negative.

### Example

Let $R = k[x_1, x_2, x_3]$, $A = (4, 2, 6)$, and $B = (2, 3, 4)$.
Then:

- $A - B = (2, -1, 2)$

Therefore $\boldsymbol{x}^A >_{lex} \boldsymbol{x}^B$ since the first entry is positive.

### Example

Let $R = k[x_1, x_2, x_3, x_4, x_5, x_6]$, $A = (4, 2, 6, 3, 1, 5)$, and $B = (4, 4, 0, 4, 4, 5)$.
Then:

- $|A| = 4 + 2 + 6 + 3 + 1 + 5 = 21$
- $|B| = 4 + 4 + 4 + 0 + 4 + 5 = 21$
- $A - B = (0, -2, 2, 3, -3, 0)$

So $|A| = |B|$.
Therefore $\mathbf{x}^B >_{deglex} \mathbf{x}^A$ since $\mathbf{x}^B >_{lex} \mathbf{x}^A$.
We also have that $\mathbf{x}^A >_{revlex} \mathbf{x}^B$ since the *last nonzero* entry is negative.

# Initial Ideal

Let $\tau$ be a monomial ordering and let $f \in R = k[x_1, x_2, \ldots, x_n]$.

1. The ***initial term*** of $f$ with respect to $\tau$ (denoted $\text{in}_\tau(f)$) is the largest monomial in a term of $f$.

# Initial Ideal

Let $\tau$ be a monomial ordering and let $f \in R = k[x_1, x_2, \dots, x_n]$.

1. The ***initial term*** of $f$ with respect to $\tau$ (denoted $\text{in}_\tau(f)$) is the largest monomial in a term of $f$.
2. The ***leading term*** of $f$ with respect to $\tau$ (notated $\text{lt}_\tau(f)$) is the term in $f$ which has $\text{in}_\tau(f)$.
3. The ***initial ideal*** of $I$ with respect to $\tau$ (denoted $\text{in}_\tau(I)$) is the ideal generated by the initial terms of all elements (not necessarily just generators) in $I$. Notationally, $\text{in}_\tau(I) := (\text{in}_\tau(f) \ : \ f \in I)$.

**Example**

Let $R = k[x, y]$ with $x >_\tau y$. Let $f, g, h$ be polynomials in $R$ where

$$f = x^3 + 3x^2y + 3xy^2 + y^3, g = 4x^2 - y^2, h = 3xy + 6y^2$$

**Example**

Let $R = k[x, y]$ with $x >_\tau y$. Let $f, g, h$ be polynomials in $R$ where

$$f = x^3 + 3x^2y + 3xy^2 + y^3, g = 4x^2 - y^2, h = 3xy + 6y^2$$

Then

- $\text{in}_\tau(f) = x^3, \text{in}_\tau(g) = x^2$, $\text{in}_\tau(h) = xy$.

### Example

Let $R = k[x, y]$ with $x >_\tau y$. Let $f, g, h$ be polynomials in $R$ where

$$f = x^3 + 3x^2y + 3xy^2 + y^3, g = 4x^2 - y^2, h = 3xy + 6y^2$$

Then

- $\text{in}_\tau(f) = x^3, \text{in}_\tau(g) = x^2$, $\text{in}_\tau(h) = xy$.
- $\text{lt}_\tau(f) = x^3, \text{lt}_\tau(g) = 4x^2$, and $\text{lt}_\tau(h) = 3xy$.

### Example

Let $R = k[x, y]$ with $x >_\tau y$. Let $f, g, h$ be polynomials in $R$ where

$$f = x^3 + 3x^2y + 3xy^2 + y^3, g = 4x^2 - y^2, h = 3xy + 6y^2$$

Then

- $\text{in}_\tau(f) = x^3, \text{in}_\tau(g) = x^2$, $\text{in}_\tau(h) = xy$.
- $\text{lt}_\tau(f) = x^3, \text{lt}_\tau(g) = 4x^2$, and $\text{lt}_\tau(h) = 3xy$.

$\star$ If $I = (f_1, f_2, \ldots, f_m)$, then $\text{in}_\tau(I) \neq (\text{in}_\tau(f_1), \ldots, \text{in}_\tau(f_m))$.

### Example

Let $R = k[x, y]$ with $x >_\tau y$. Let $f, g, h$ be polynomials in $R$ where

$$f = x^3 + 3x^2y + 3xy^2 + y^3, g = 4x^2 - y^2, h = 3xy + 6y^2$$

Then

- $\text{in}_\tau(f) = x^3, \text{in}_\tau(g) = x^2$, $\text{in}_\tau(h) = xy$.
- $\text{lt}_\tau(f) = x^3, \text{lt}_\tau(g) = 4x^2$, and $\text{lt}_\tau(h) = 3xy$.

$\star$ If $I = (f_1, f_2, \ldots, f_m)$, then $\text{in}_\tau(I) \neq (\text{in}_\tau(f_1), \ldots, \text{in}_\tau(f_m))$. Thus, finding $\text{in}_\tau(I)$ will itself require some work.

## Example

Let $R = k[x, y]$ with $x >_\tau y$. Let $f, g, h$ be polynomials in $R$ where

$$f = x^3 + 3x^2y + 3xy^2 + y^3, g = 4x^2 - y^2, h = 3xy + 6y^2$$

Then

- $\text{in}_\tau(f) = x^3, \text{in}_\tau(g) = x^2$, $\text{in}_\tau(h) = xy$.
- $\text{lt}_\tau(f) = x^3, \text{lt}_\tau(g) = 4x^2$, and $\text{lt}_\tau(h) = 3xy$.

$\star$ If $I = (f_1, f_2, \ldots, f_m)$, then $\text{in}_\tau(I) \neq (\text{in}_\tau(f_1), \ldots, \text{in}_\tau(f_m))$. Thus, finding $\text{in}_\tau(I)$ will itself require some work. Notice that $\text{in}_\tau(I)$ is a monomial ideal.

### Example

$R = k[x, y, z], \mathrm{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

## Example

$R = k[x, y, z], \mathrm{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\mathrm{in}_\tau(f_1) = x = \mathrm{in}_\tau(f_2)$.

## Example

$R = k[x, y, z], \mathrm{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\mathrm{in}_\tau(f_1) = x = \mathrm{in}_\tau(f_2)$. $f_1 - f_2 = 2y - 2z$, so $\mathrm{in}_\tau(f_1 - f_2) = y$.

## Example

$R = k[x, y, z], \text{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\text{in}_\tau(f_1) = x = \text{in}_\tau(f_2)$. $f_1 - f_2 = 2y - 2z$, so $\text{in}_\tau(f_1 - f_2) = y$.

**Claim:** $\text{in}_\tau(I) = (x, y)$:

## Example

$R = k[x, y, z], \text{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\text{in}_\tau(f_1) = x = \text{in}_\tau(f_2)$. $f_1 - f_2 = 2y - 2z$, so $\text{in}_\tau(f_1 - f_2) = y$.

**Claim:** $\text{in}_\tau(I) = (x, y)$: Note that $f_1 - f_2 = x \in I$. So, $I = (x, y - z)$.

## Example

$R = k[x, y, z], \text{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\text{in}_\tau(f_1) = x = \text{in}_\tau(f_2)$. $f_1 - f_2 = 2y - 2z$, so $\text{in}_\tau(f_1 - f_2) = y$.

**Claim:** $\text{in}_\tau(I) = (x, y)$: Note that $f_1 - f_2 = x \in I$. So, $I = (x, y - z)$. Suppose $z^i \in \text{in}_\tau(I)$, then

$$\exists\ f = \lambda z^i + (\text{lower terms only in } y \text{ and } z) \in I, \lambda \in k$$

## Example

$R = k[x, y, z], \mathrm{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\mathrm{in}_\tau(f_1) = x = \mathrm{in}_\tau(f_2)$. $f_1 - f_2 = 2y - 2z$, so $\mathrm{in}_\tau(f_1 - f_2) = y$.

**Claim:** $\mathrm{in}_\tau(I) = (x, y)$: Note that $f_1 - f_2 = x \in I$. So, $I = (x, y - z)$. Suppose $z^i \in \mathrm{in}_\tau(I)$, then

$$\exists\ f = \lambda z^i + (\text{lower terms only in } y \text{ and } z) \in I, \lambda \in k$$

But, no such lower term can exist!

## Example

$R = k[x, y, z], \mathrm{char}(k) \neq 2$, $I = (x + y - z, x - y + z)$, $\tau$ is a monomial ordering on $R$ such that $x >_\tau y >_\tau z$. Let

$$f_1 = x + y - z, \qquad f_2 = x - y + z.$$

$\mathrm{in}_\tau(f_1) = x = \mathrm{in}_\tau(f_2)$. $f_1 - f_2 = 2y - 2z$, so $\mathrm{in}_\tau(f_1 - f_2) = y$.

**Claim:** $\mathrm{in}_\tau(I) = (x, y)$: Note that $f_1 - f_2 = x \in I$. So, $I = (x, y - z)$. Suppose $z^i \in \mathrm{in}_\tau(I)$, then

$$\exists\ f = \lambda z^i + (\text{lower terms only in } y \text{ and } z) \in I, \lambda \in k$$

But, no such lower term can exist! So, $z^i \in I$ and hence $z \in \sqrt{I}$.

**Example (Cntd.)**

$y - z, x \in I \Rightarrow y - z, x \in \sqrt{I}$

## Example (Cntd.)

$y - z, x \in I \Rightarrow y - z, x \in \sqrt{I} \Rightarrow (y - z) + z = y \in \sqrt{I}.$

### Example (Cntd.)

$y - z, x \in I \Rightarrow y - z, x \in \sqrt{I} \Rightarrow (y - z) + z = y \in \sqrt{I}$. Therefore $\sqrt{I} = (x, y, z)$.

## Example (Cntd.)

$y - z, x \in I \Rightarrow y - z, x \in \sqrt{I} \Rightarrow (y - z) + z = y \in \sqrt{I}$. Therefore $\sqrt{I} = (x, y, z)$.
This implies that $\mathrm{ht}(I) = 3$

## Example (Cntd.)

$y - z, x \in I \Rightarrow y - z, x \in \sqrt{I} \Rightarrow (y - z) + z = y \in \sqrt{I}$. Therefore $\sqrt{I} = (x, y, z)$.

This implies that $\mathrm{ht}(I) = 3$ But

$$I = (x + y - z, x - y + z) \xrightarrow[\text{Height Theorem}]{\text{Krull's}} \mathrm{ht}(I) \leq 2$$

## Example (Cntd.)

$y - z, x \in I \Rightarrow y - z, x \in \sqrt{I} \Rightarrow (y - z) + z = y \in \sqrt{I}$. Therefore $\sqrt{I} = (x, y, z)$.

This implies that $\mathrm{ht}(I) = 3$ But

$$I = (x + y - z, x - y + z) \xrightarrow[\text{Height Theorem}]{\text{Krull's}} \mathrm{ht}(I) \leq 2 \Rightarrow\Leftarrow$$

$\square$

# Reduction

## Definition

Let $f, g, h$ be polynomials in $R$ with $g \neq 0$. Let $G$ be a collection of nonzero polynomials in $R$. Fix a monomial ordering $\tau$ on $R$.

# Reduction

## Definition

Let $f, g, h$ be polynomials in $R$ with $g \neq 0$. Let $G$ be a collection of nonzero polynomials in $R$. Fix a monomial ordering $\tau$ on $R$. We say that:

- $f$ **directly reduces** to $h$ with respect to $g$ if $\mu \mathbf{x}^{\mathbf{A}} = \mathrm{lt}_\tau(g)$ divides a nonzero term $\lambda \mathbf{x}^{\mathbf{B}}$ of $f$ and $h = f - (\frac{\lambda}{\mu})\mathbf{x}^{\mathbf{B}-\mathbf{A}} g$.
    - Notation: $f \underset{g}{\longrightarrow} h$

# Reduction

## Definition

Let $f, g, h$ be polynomials in $R$ with $g \neq 0$. Let $G$ be a collection of nonzero polynomials in $R$. Fix a monomial ordering $\tau$ on $R$. We say that:

- $f$ **directly reduces** to $h$ with respect to $g$ if $\mu \boldsymbol{x}^{\boldsymbol{A}} = \mathrm{lt}_\tau(g)$ divides a nonzero term $\lambda \boldsymbol{x}^{\boldsymbol{B}}$ of $f$ and $h = f - (\frac{\lambda}{\mu})\boldsymbol{x}^{\boldsymbol{B}-\boldsymbol{A}} g$.
  - Notation: $f \underset{g}{\longrightarrow} h$
- $f$ **reduces** to $h$ with respect to $G$ if there is a chain $f \underset{g_1}{\longrightarrow} h_1 \underset{g_2}{\longrightarrow} h_2 \underset{g_3}{\longrightarrow} \cdots \underset{g_k}{\longrightarrow} h$ where each $g_i \in G$
  - Notation: $f \underset{G}{\longrightarrow} h$

# Reduction

## Definition

Let $f, g, h$ be polynomials in $R$ with $g \neq 0$. Let $G$ be a collection of nonzero polynomials in $R$. Fix a monomial ordering $\tau$ on $R$. We say that:

- $f$ **directly reduces** to $h$ with respect to $g$ if $\mu \mathbf{x}^{\mathbf{A}} = \mathrm{lt}_\tau(g)$ divides a nonzero term $\lambda \mathbf{x}^{\mathbf{B}}$ of $f$ and $h = f - (\frac{\lambda}{\mu})\mathbf{x}^{\mathbf{B}-\mathbf{A}} g$.
    - Notation: $f \underset{g}{\longrightarrow} h$
- $f$ **reduces** to $h$ with respect to $G$ if there is a chain $f \underset{g_1}{\longrightarrow} h_1 \underset{g_2}{\longrightarrow} h_2 \underset{g_3}{\longrightarrow} \cdots \underset{g_k}{\longrightarrow} h$ where each $g_i \in G$
    - Notation: $f \underset{G}{\longrightarrow} h$
- $h$ is **reduced with respect to** $G$ if no term in $h$ is divisible by $\mathrm{in}_\tau(g_i)$ for any $g_i \in G$

# The Division Algorithm

**Theorem**

*Let* $G = \{g_1, \ldots, g_k\}$ *be a collection of nonzero polynomials in* $R$ *and* $f$ *be any polynomial in* $R$.

# The Division Algorithm

**Theorem**

*Let* $G = \{g_1, \ldots, g_k\}$ *be a collection of nonzero polynomials in* $R$ *and* $f$ *be any polynomial in* $R$*. There are polynomials* $u_1, \ldots, u_k, r \in R$ *such that we can write*

$$f = \sum_{i=1}^{k} u_i g_i + r \qquad (\star)$$

*where* $r$ *is reduced with respect to* $G$ *and*

$$\mathrm{in}_\tau(f) \geq \max\{\mathrm{in}_\tau(u_1 g_1), \ldots, \mathrm{in}_\tau(u_k g_k))\}$$

.

# The Division Algorithm

**Theorem**

*Let $G = \{g_1, \dots, g_k\}$ be a collection of nonzero polynomials in $R$ and $f$ be any polynomial in $R$. There are polynomials $u_1, \dots, u_k, r \in R$ such that we can write*

$$f = \sum_{i=1}^{k} u_i g_i + r \qquad (\star)$$

*where $r$ is reduced with respect to $G$ and*

$$\text{in}_\tau(f) \geq \max\{\text{in}_\tau(u_1 g_1), \dots, \text{in}_\tau(u_k g_k))\}$$

.

$r$ : remainder w.r.t. $G$

# The Division Algorithm

**Theorem**

*Let $G = \{g_1, \ldots, g_k\}$ be a collection of nonzero polynomials in $R$ and $f$ be any polynomial in $R$. There are polynomials $u_1, \ldots, u_k, r \in R$ such that we can write*

$$f = \sum_{i=1}^{k} u_i g_i + r \qquad (\star)$$

*where $r$ is reduced with respect to $G$ and*

$$\text{in}_\tau(f) \geq \max\{\text{in}_\tau(u_1 g_1), \ldots, \text{in}_\tau(u_k g_k))\}$$

.

$r$ : remainder w.r.t. $G$ (is it unique?)

# The Division Algorithm

**Theorem**

*Let $G = \{g_1, \ldots, g_k\}$ be a collection of nonzero polynomials in $R$ and $f$ be any polynomial in $R$. There are polynomials $u_1, \ldots, u_k, r \in R$ such that we can write*

$$f = \sum_{i=1}^{k} u_i g_i + r \qquad (\star)$$

*where $r$ is reduced with respect to $G$ and*

$$\text{in}_\tau(f) \geq \max\{\text{in}_\tau(u_1 g_1), \ldots, \text{in}_\tau(u_k g_k))\}$$

.

$r$ : remainder w.r.t. $G$ (is it unique?)

Notation: $r = \overline{f}^G$.

# Gröbner Basis

**Definition**

A Gröbner basis of an ideal $I$ in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ with respect to the monomial ordering $\tau$ is a set $\{f_1, \ldots, f_m\} \subset I$ such that

$$\mathrm{in}_\tau(I) = \Big(\mathrm{in}_\tau(f_1), \ldots, \mathrm{in}_\tau(f_m)\Big).$$

# Gröbner Basis

**Definition**

A Gröbner basis of an ideal $I$ in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ with respect to the monomial ordering $\tau$ is a set $\{f_1, \ldots, f_m\} \subset I$ such that

$$\mathrm{in}_\tau(I) = \Big(\mathrm{in}_\tau(f_1), \ldots, \mathrm{in}_\tau(f_m)\Big).$$

- It turns out that $\overline{f}^G$ is indeed unique if $G$ is a Gröbner Basis !

# Gröbner Basis

**Definition**

A Gröbner basis of an ideal $I$ in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ with respect to the monomial ordering $\tau$ is a set $\{f_1, \ldots, f_m\} \subset I$ such that

$$\mathrm{in}_\tau(I) = \Big(\mathrm{in}_\tau(f_1), \ldots, \mathrm{in}_\tau(f_m)\Big).$$

- It turns out that $\overline{f}^G$ is indeed unique if $G$ is a Gröbner Basis !
- Recall that we found $\mathrm{in}_\tau(I) = (x, y)$ for $I = (x - y + z, x + y - z)$.

# Gröbner Basis

**Definition**

A Gröbner basis of an ideal $I$ in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ with respect to the monomial ordering $\tau$ is a set $\{f_1, \ldots, f_m\} \subset I$ such that

$$\mathrm{in}_\tau(I) = \Big(\mathrm{in}_\tau(f_1), \ldots, \mathrm{in}_\tau(f_m)\Big).$$

- It turns out that $\overline{f}^G$ is indeed unique if $G$ is a Gröbner Basis !

- Recall that we found $\mathrm{in}_\tau(I) = (x, y)$ for $I = (x - y + z, x + y - z)$.
Hence a Gröbner Basis is given $\{x + y - z, 2y - 2z\}$.

# Gröbner Basis Generates $I$

**Theorem**

*Let $J, I$ be ideals of $R$ such that $J \subset I$. Let $\tau$ be a monomial ordering on $R$. Then*

$$\mathrm{in}_\tau(I) = \mathrm{in}_\tau(J) \iff I = J.$$

# Gröbner Basis Generates $I$

**Theorem**

*Let $J, I$ be ideals of $R$ such that $J \subset I$. Let $\tau$ be a monomial ordering on $R$. Then*

$$\mathrm{in}_\tau(I) = \mathrm{in}_\tau(J) \iff I = J.$$

**Corollary**

*If $G = \{g_1, \ldots, g_r\}$ is a Gröbner basis of the ideal $I$, then $G$ generates $I$.*

# Criterion for Ideal Membership

**Theorem**

*Let $I \subseteq R$ be an ideal and let $G = \{g_1, \ldots, g_k\} \subseteq I, g_i \neq 0$ for all $i$. Then the following are equivalent:*

1. *$G$ is a Gröbner basis for $I$.*
2. *$f \in I$ if and only if $f \xrightarrow[G]{} 0$.*

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(f)} f - \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(g)} g.$$

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(f)} f - \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(g)} g.$$

## Example

Let $R = k[x, y, z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$.

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(f)} f - \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(g)} g.$$

## Example

Let $R = k[x, y, z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\operatorname{in}_\tau(g_1) = xy$ and $\operatorname{in}_\tau(g_2) = xz$

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{in}_\tau(f), \mathrm{in}_\tau(g))}{\mathrm{lt}_\tau(f)} f - \frac{\mathrm{lcm}(\mathrm{in}_\tau(f), \mathrm{in}_\tau(g))}{\mathrm{lt}_\tau(g)} g.$$

## Example

Let $R = k[x, y, z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\mathrm{in}_\tau(g_1) = xy$ and $\mathrm{in}_\tau(g_2) = xz$

$$S(g_1, g_2) = \frac{\mathrm{lcm}(xy, xz)}{xy}(xy - z^2) - \frac{\mathrm{lcm}(xy, xz)}{-xz}(y^2 - xz)$$

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\text{lcm}(\text{in}_\tau(f), \text{in}_\tau(g))}{\text{lt}_\tau(f)} f - \frac{\text{lcm}(\text{in}_\tau(f), \text{in}_\tau(g))}{\text{lt}_\tau(g)} g.$$

**Example**

Let $R = k[x, y, z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$

$$\begin{aligned} S(g_1, g_2) &= \frac{\text{lcm}(xy, xz)}{xy}(xy - z^2) - \frac{\text{lcm}(xy, xz)}{-xz}(y^2 - xz) \\ &= \frac{xyz}{xy}(xy - z^2) - \frac{xyz}{-xz}(y^2 - xz) \end{aligned}$$

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{in}_\tau(f), \mathrm{in}_\tau(g))}{\mathrm{lt}_\tau(f)} f - \frac{\mathrm{lcm}(\mathrm{in}_\tau(f), \mathrm{in}_\tau(g))}{\mathrm{lt}_\tau(g)} g.$$

## Example

Let $R = k[x, y, z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\mathrm{in}_\tau(g_1) = xy$ and $\mathrm{in}_\tau(g_2) = xz$

$$\begin{aligned} S(g_1, g_2) &= \frac{\mathrm{lcm}(xy, xz)}{xy}(xy - z^2) - \frac{\mathrm{lcm}(xy, xz)}{-xz}(y^2 - xz) \\ &= \frac{xyz}{xy}(xy - z^2) - \frac{xyz}{-xz}(y^2 - xz) = z(xy - z^2) + y(y^2 - xz) \end{aligned}$$

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(f)} f - \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(g)} g.$$

**Example**

Let $R = k[x, y, z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\operatorname{in}_\tau(g_1) = xy$ and $\operatorname{in}_\tau(g_2) = xz$

$$\begin{aligned} S(g_1, g_2) &= \frac{\operatorname{lcm}(xy, xz)}{xy}(xy - z^2) - \frac{\operatorname{lcm}(xy, xz)}{-xz}(y^2 - xz) \\ &= \frac{xyz}{xy}(xy - z^2) - \frac{xyz}{-xz}(y^2 - xz) = z(xy - z^2) + y(y^2 - xz) \\ &= xyz - z^3 + (y^3 - xyz) \end{aligned}$$

# The $S$ polynomials: Key Definition

Fix a monomial ordering $\tau$ on $R$. Let $f, g$ be polynomials in $R$. The $S$ *polynomial*:

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(f)} f - \frac{\operatorname{lcm}(\operatorname{in}_\tau(f), \operatorname{in}_\tau(g))}{\operatorname{lt}_\tau(g)} g.$$

## Example

Let $R = k[x,y,z]$. $\tau$: deglex with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ where $g_1 = xy - z^2$ and $g_2 = y^2 - xz$. $\operatorname{in}_\tau(g_1) = xy$ and $\operatorname{in}_\tau(g_2) = xz$

$$\begin{aligned} S(g_1,g_2) &= \frac{\operatorname{lcm}(xy,xz)}{xy}(xy - z^2) - \frac{\operatorname{lcm}(xy,xz)}{-xz}(y^2 - xz) \\ &= \frac{xyz}{xy}(xy - z^2) - \frac{xyz}{-xz}(y^2 - xz) = z(xy - z^2) + y(y^2 - xz) \\ &= xyz - z^3 + (y^3 - xyz) = y^3 - z^3. \end{aligned}$$

**Theorem (Buchberger's Criterion)**

*Let $\tau$ be a monomial ordering on $R$ and $I = (g_1, \ldots, g_s)$ be an ideal. Let $G = \{g_1, \ldots, g_s\}$. Fix remainders of $S(g_i, g_j)$ with respect to $G$, say $\overline{S(g_i, g_j)}^G$. Then $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis for $I$ if and only if $\overline{S(g_i, g_j)}^G = 0$ for all $i, j$ where $1 \leq i < j \leq s$.*

# Buchberger's Algorithm

Buchberger's Criterion can be turned into an algorithm:

# Buchberger's Algorithm

Buchberger's Criterion can be turned into an algorithm: Given

$g_1, \ldots, g_s \in I$:

# Buchberger's Algorithm

Buchberger's Criterion can be turned into an algorithm: Given

$g_1, \ldots, g_s \in I$:

1. Compute $\overline{S(g_i, g_j)}^G = h_{ij}$. If $h_{ij} = 0$, then we are done.

# Buchberger's Algorithm

Buchberger's Criterion can be turned into an algorithm: Given

$g_1, \ldots, g_s \in I$:

1. Compute $\overline{S(g_i, g_j)}^G = h_{ij}$. If $h_{ij} = 0$, then we are done.
2. If $h_{ij} \neq 0$, replace $\{g_1, \ldots, g_s\}$ by $\{g_1, \ldots, g_s, h_{ij}\}$ and repeat (that way the nonzero $\overline{S(g_i, g_j)}^G = h_{ij}$ will now reduce to 0).

# Buchberger's Algorithm

Buchberger's Criterion can be turned into an algorithm: Given

$g_1, \ldots, g_s \in I$:

1. Compute $\overline{S(g_i, g_j)}^G = h_{ij}$. If $h_{ij} = 0$, then we are done.
2. If $h_{ij} \neq 0$, replace $\{g_1, \ldots, g_s\}$ by $\{g_1, \ldots, g_s, h_{ij}\}$ and repeat (that way the nonzero $\overline{S(g_i, g_j)}^G = h_{ij}$ will now reduce to 0).

This process stops.
**Reason:** We get an ascending chain

$$(\mathrm{in}_\tau(g_1), \ldots, \mathrm{in}_\tau(g_s)) \subseteq (\mathrm{in}_\tau(g_1), \ldots, \mathrm{in}_\tau(g_s), \mathrm{in}_\tau(h_{ij})) \subseteq \ldots$$

in the Noetherian ring $R$,

# Buchberger's Algorithm

Buchberger's Criterion can be turned into an algorithm: Given

$g_1, \ldots, g_s \in I$:

1. Compute $\overline{S(g_i, g_j)}^G = h_{ij}$. If $h_{ij} = 0$, then we are done.
2. If $h_{ij} \neq 0$, replace $\{g_1, \ldots, g_s\}$ by $\{g_1, \ldots, g_s, h_{ij}\}$ and repeat (that way the nonzero $\overline{S(g_i, g_j)}^G = h_{ij}$ will now reduce to 0).

This process stops.
**Reason:** We get an ascending chain

$$(\mathrm{in}_\tau(g_1), \ldots, \mathrm{in}_\tau(g_s)) \subseteq (\mathrm{in}_\tau(g_1), \ldots, \mathrm{in}_\tau(g_s), \mathrm{in}_\tau(h_{ij})) \subseteq \ldots$$

in the Noetherian ring $R$, hence stabilizes i.e. the $S$-polynomials reduce to 0 after finitely many steps.

### Example

Let $R = k[x, y, z]$, $\tau$: *deglex* with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$.

### Example

Let $R = k[x, y, z]$, $\tau$: *deglex* with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$.

Let $G = \{g_1, g_2\}$. We calculated $S(g_1, g_2) = y^3 - z^3$.

## Example

Let $R = k[x, y, z]$, $\tau$: *deglex* with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$.

Let $G = \{g_1, g_2\}$. We calculated $S(g_1, g_2) = y^3 - z^3$.
$\text{in}_\tau(g_1) \nmid \text{in}_\tau(y^3 - z^3)$

### Example

Let $R = k[x, y, z]$, $\tau$: *deglex* with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$.

Let $G = \{g_1, g_2\}$. We calculated $S(g_1, g_2) = y^3 - z^3$. $\text{in}_\tau(g_1) \nmid \text{in}_\tau(y^3 - z^3)$ and $\text{in}_\tau(g_2) \nmid \text{in}_\tau(y^3 - z^3)$

### Example

Let $R = k[x, y, z]$, $\tau$: *deglex* with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$.

Let $G = \{g_1, g_2\}$. We calculated $S(g_1, g_2) = y^3 - z^3$.
$\text{in}_\tau(g_1) \nmid \text{in}_\tau(y^3 - z^3)$ and $\text{in}_\tau(g_2) \nmid \text{in}_\tau(y^3 - z^3)$
So $y^3 - z^3$ is reduced with respect to $G$, i.e. $\overline{S(g_1, g_2)}^G \neq 0$.

## Example

Let $R = k[x, y, z]$, $\tau$: *deglex* with $x >_\tau y >_\tau z$. Let $I = (g_1, g_2)$ with $g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$.

Let $G = \{g_1, g_2\}$. We calculated $S(g_1, g_2) = y^3 - z^3$.
$\text{in}_\tau(g_1) \nmid \text{in}_\tau(y^3 - z^3)$ and $\text{in}_\tau(g_2) \nmid \text{in}_\tau(y^3 - z^3)$
So $y^3 - z^3$ is reduced with respect to $G$, i.e. $\overline{S(g_1, g_2)}^G \neq 0$.

Now we start the process over again adjoining $S(g_1, g_2) = y^3 - z^3$ to $G$.

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4$;

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4$;
  $\overline{S(g_2, g_3)}^G$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4$;
  $\overline{S(g_2, g_3)}^G = \overline{xz^4 - y^5 \qquad\qquad\qquad\qquad\qquad\qquad}$

### Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4$;
  $\overline{S(g_2, g_3)}^G = \overline{xz^4 - y^5 + z^3(y^2 - xz) \qquad\qquad\qquad\qquad}$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4;$
  $\overline{S(g_2, g_3)}^G = \overline{xz^4 - y^5 + z^3(y^2 - xz) + y^2(y^3 - z^3)}^G$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4$;
  $\overline{S(g_2, g_3)}^G = \overline{xz^4 - y^5 + z^3(y^2 - xz) + y^2(y^3 - z^3)}^G = 0$

## Example (Cntd.)

$g_1 = xy - z^2$ and $g_2 = y^2 - xz$, $\text{in}_\tau(g_1) = xy$ and $\text{in}_\tau(g_2) = xz$
Now let $g_3 = y^3 - z^3$, $G = \{g_1, g_2, g_3\}$, $\text{in}_\tau(g_3) = y^3$.

- $S(g_1, g_2) = y^3 - z^3 \Rightarrow \overline{S(g_1, g_2)}^G = 0$
- $S(g_1, g_3) = xz^3 - y^2z^2 = z^2(xz - y^2) = z^2 g_2 \Rightarrow \overline{S(g_1, g_3)}^G = 0$
- $S(g_2, g_3) = -y^5 + xz^4$;
  $\overline{S(g_2, g_3)}^G = \overline{xz^4 - y^5 + z^3(y^2 - xz) + y^2(y^3 - z^3)}^G = 0$

Therefore $\{g_1, g_2, g_3\}$ is a Gröbner basis for $I$.

## Corollary

*Let $\tau$ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

## Corollary

*Let $\tau$ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

1. *Any set of monomials is a Gröbner basis for the ideals they generate.*

## Corollary

*Let $\tau$ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

1. *Any set of monomials is a Gröbner basis for the ideals they generate.*
2. *If $I$ is generated by binomials (i.e. elements of the form $\lambda_A \mathbf{x}^A + \lambda_B \mathbf{x}^B$), then $I$ has a Gröbner basis of binomials.*

## Corollary

*Let $\tau$ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

1. *Any set of monomials is a Gröbner basis for the ideals they generate.*
2. *If $I$ is generated by binomials (i.e. elements of the form $\lambda_A \mathbf{x}^A + \lambda_B \mathbf{x}^B$), then $I$ has a Gröbner basis of binomials.*
3. *If $I$ is homogeneous, $I$ has a homogeneous Gröbner basis.*

## Corollary

*Let $\tau$ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

1. *Any set of monomials is a Gröbner basis for the ideals they generate.*
2. *If $I$ is generated by binomials (i.e. elements of the form $\lambda_A \mathbf{x}^A + \lambda_B \mathbf{x}^B$), then $I$ has a Gröbner basis of binomials.*
3. *If $I$ is homogeneous, $I$ has a homogeneous Gröbner basis.*
4. *If $(g_1, \ldots, g_s) = I$ and $(\mathrm{in}_\tau(g_i), \mathrm{in}_\tau(g_j)) = 1$ whenever $i \neq j$, then $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $I$.*

## Corollary

*Let $\tau$ be a monomial ordering on $R = k[x_1, \ldots, x_n]$. Then*

1. *Any set of monomials is a Gröbner basis for the ideals they generate.*
2. *If $I$ is generated by binomials (i.e. elements of the form $\lambda_A \mathbf{x}^A + \lambda_B \mathbf{x}^B$), then $I$ has a Gröbner basis of binomials.*
3. *If $I$ is homogeneous, $I$ has a homogeneous Gröbner basis.*
4. *If $(g_1, \ldots, g_s) = I$ and $(\mathrm{in}_\tau(g_i), \mathrm{in}_\tau(g_j)) = 1$ whenever $i \neq j$, then $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $I$.*
5. *If $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $I = (g_1, \ldots, g_s)$ and $k \subseteq L$ is a field extension, then $\{g_1, \ldots, g_s\}$ is a Gröbner basis for $IL[x_1, \ldots, x_n]$.*

**Theorem (Elimination)**

*Let $\tau$ be a lex order on $R$ and $I \subset R$. Then:*

**Theorem (Elimination)**

*Let $\tau$ be a lex order on $R$ and $I \subset R$. Then:*

1. $\mathrm{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] = \mathrm{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$.

**Theorem (Elimination)**

*Let $\tau$ be a lex order on $R$ and $I \subset R$. Then:*

1. $\mathrm{in}_\tau(I) \cap k[x_i, x_{i+1}, \ldots, x_n] = \mathrm{in}_\tau(I \cap k[x_i, x_{i+1}, \ldots, x_n])$.
2. *Let $\{f_1, \ldots, f_s\}$ be a Gröbner basis of $I$. Then*

$$\{f_1, \ldots, f_s\} \cap k[x_i, x_{i+1}, \ldots, x_n]$$

*is a Gröbner basis of $I \cap k[x_i, x_{i+1}, \ldots, x_n]$.*

# Application of Elimination Theorem

**Theorem**

*Let* $S = k[t_1, \ldots, t_n]$ *be a polynomial ring and* $f_1, \ldots, f_m \in S$*.*

# Application of Elimination Theorem

**Theorem**

*Let $S = k[t_1, \ldots, t_n]$ be a polynomial ring and $f_1, \ldots, f_m \in S$. Let $\phi$ be the map*

$$\phi : k[x_1, \ldots, x_m] \to k[f_1, \ldots, f_m]$$

$$\phi(x_i) = f_i$$

# Application of Elimination Theorem

**Theorem**

*Let $S = k[t_1, \ldots, t_n]$ be a polynomial ring and $f_1, \ldots, f_m \in S$. Let $\phi$ be the map*

$$\phi : k[x_1, \ldots, x_m] \to k[f_1, \ldots, f_m]$$

$$\phi(x_i) = f_i$$

*Let $J = (x_1 - f_1, x_2 - f_2, \ldots, x_n - f_n)$ be an ideal in the polynomial ring $k[t_1, \ldots, t_n, x_1, \ldots, x_m]$.*

# Application of Elimination Theorem

**Theorem**

*Let $S = k[t_1, \ldots, t_n]$ be a polynomial ring and $f_1, \ldots, f_m \in S$. Let $\phi$ be the map*

$$\phi : k[x_1, \ldots, x_m] \to k[f_1, \ldots, f_m]$$

$$\phi(x_i) = f_i$$

*Let $J = (x_1 - f_1, x_2 - f_2, \ldots, x_n - f_n)$ be an ideal in the polynomial ring $k[t_1, \ldots, t_n, x_1, \ldots, x_m]$. Then $K = \ker \phi = J \cap k[x_1, \ldots, x_m]$.*


Thank
You