Gröbner-baser

Bachelorforsvar ved Kristian

Fredag d. 27. marts 2015

Disposition

1. Motivation og baggrund
2. Idéerne kort fortalt
3. Division af polynomier
4. Gröbner-baser
5. Anvendelser
6. Lyn-opsummering

Disposition

1. Motivation og baggrund
2. Idéerne kort fortalt
3. Division af polynomier
4. Gröbner-baser
5. Anvendelser
6. Lyn-opsummering

$\left.\right\}$ 25 min.

Disposition

1. Motivation og baggrund
2. Idéerne kort fortalt
3. Division af polynomier
4. Gröbner-baser
5. Anvendelser
6. Lyn-opsummering
7. Spørgsmål

$\left.\begin{matrix}1\\2\\3\\4\\5\\6\end{matrix}\right\}$ 25 min.

1. Motivation og baggrund

Løsning af systemer af ikke-lineære polynomiumsligninger

1. Motivation og baggrund

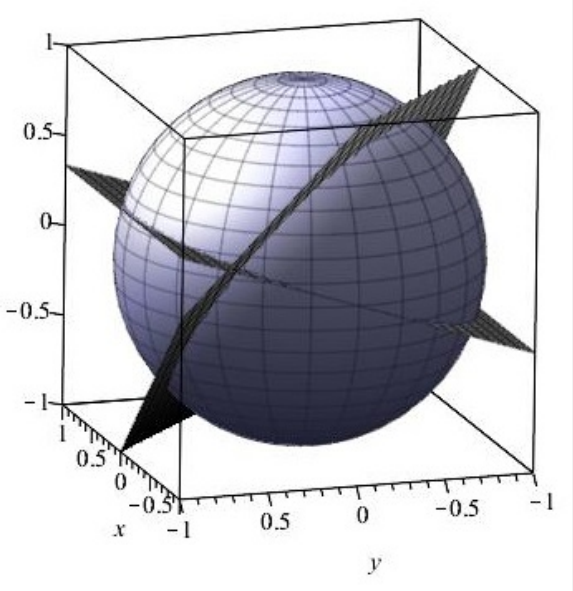
Løsning af systemer af ikke-lineære polynomiumsligninger

$$
\begin{aligned}
x^2 + y^2 + z^2 - 1 &= 0, \\
x + y + z &= 0, \\
y - 3z &= 0.
\end{aligned}
$$

1. Motivation og baggrund

Løsning af systemer af ikke-lineære polynomiumsligninger

$$
\begin{aligned}
x^2 + y^2 + z^2 - 1 &= 0, \\
x + y + z &= 0, \\
y - 3z &= 0.
\end{aligned}
$$



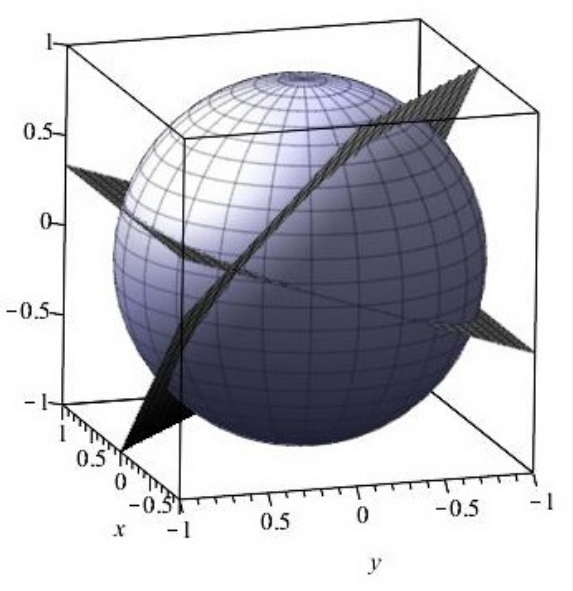
1. Motivation og baggrund

Løsning af systemer af ikke-lineære polynomiumsligninger

$$
\begin{aligned}
x^2 + y^2 + z^2 - 1 &= 0, \\
x + y + z &= 0, \\
y - 3z &= 0.
\end{aligned}
$$

$\downarrow$ *Gröbner basen*

$$
\begin{aligned}
26z^2 - 1 &= 0, \\
y - 3z &= 0, \\
x + y + z &= 0.
\end{aligned}
$$



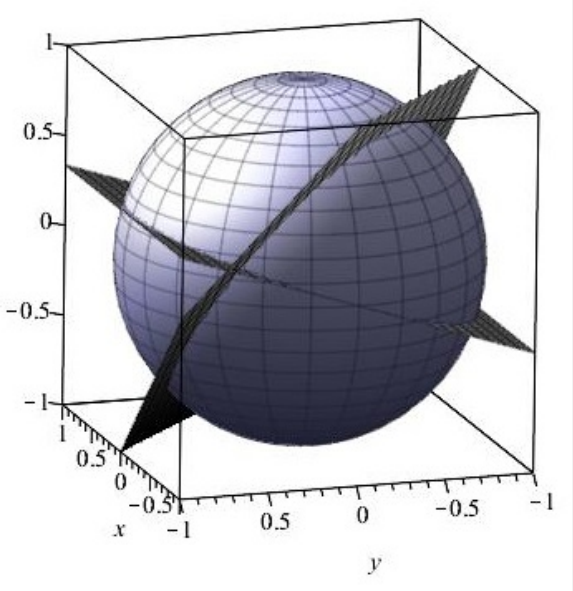
1. Motivation og baggrund

Løsning af systemer af ikke-lineære polynomiumsligninger

$$x^2 + y^2 + z^2 - 1 = 0,$$
$$x + y + z = 0,$$
$$y - 3z = 0.$$

↓ *Gröbner basen*

$$26z^2 - 1 = 0,$$
$$y - 3z = 0,$$
$$x + y + z = 0.$$



God gammeldags Algebra

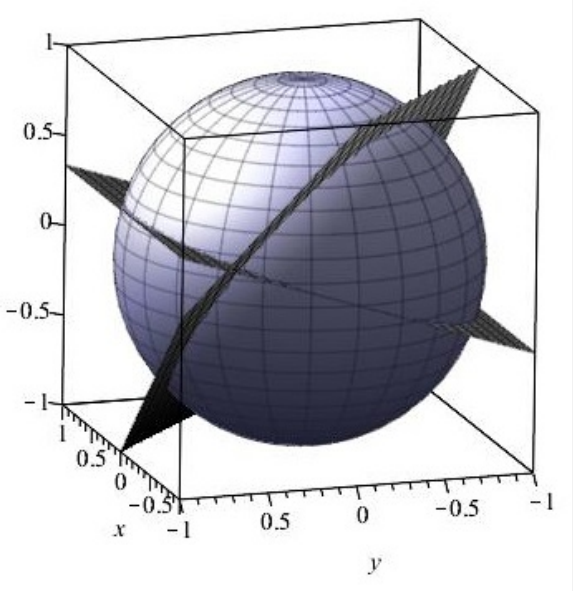
1. Motivation og baggrund

Løsning af systemer af ikke-lineære polynomiumsligninger

$$x^2 + y^2 + z^2 - 1 = 0,$$
$$x + y + z = 0,$$
$$y - 3z = 0.$$

↓ *Gröbner basen*

$$26z^2 - 1 = 0,$$
$$y - 3z = 0,$$
$$x + y + z = 0.$$



God gammeldags Algebra

1. Motivation og baggrund

Hironaka (1931 -)

Buchberger (1942 -)

1. Motivation og baggrund

Hironaka (1931 -)

Buchberger (1942 -)

Gröbner (1899 - 1980)

2. Idéerne kort fortalt

Givet
$$\begin{aligned} p_1 &= 0, \quad \text{i } K[x_1, \ldots, x_n] \\ p_2 &= 0, \\ &\vdots \\ p_m &= 0. \end{aligned}$$

2. Idéerne kort fortalt

Givet
$$\begin{aligned} p_1 &= 0, \quad \text{i } K[x_1, \ldots, x_n] \\ p_2 &= 0, \\ &\vdots \\ p_m &= 0. \end{aligned}$$

$$I = \langle p_1, \ldots, p_m \rangle, \quad p \in I \Leftrightarrow p = a_1 p_1 + \cdots + a_m p_m$$

2. Idéerne kort fortalt

Givet
$$\begin{aligned} p_1 &= 0, \quad \text{i } K[x_1, \ldots, x_n] \\ p_2 &= 0, \\ &\vdots \\ p_m &= 0. \end{aligned}$$

$$I = \langle p_1, \ldots, p_m \rangle, \quad p \in I \Leftrightarrow p = a_1 p_1 + \cdots + a_m p_m$$

$$P = \{p_1, \ldots, p_s\} \subseteq I$$

2. Idéerne kort fortalt

Givet
$$\begin{aligned} p_1 &= 0, \quad \text{i } K[x_1, \ldots, x_n] \\ p_2 &= 0, \\ &\vdots \\ p_m &= 0. \end{aligned}$$

$$I = \langle p_1, \ldots, p_m \rangle, \quad p \in I \Leftrightarrow p = a_1 p_1 + \cdots + a_m p_m$$

$$P = \{p_1, \ldots, p_s\} \subseteq I$$

For ethvert $p \in I$ skal findes $p_i \in P$ så
"$p_i \cdot a = p$"

2. Idéerne kort fortalt

Givet $\quad p_1 = 0, \quad$ i $K[x_1, \ldots, x_n]$

$$p_2 = 0,$$

$$\vdots$$

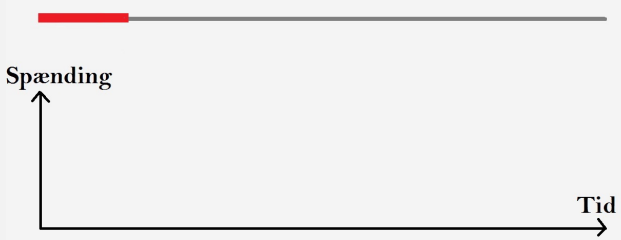
$$p_m = 0.$$

$$I = \langle p_1, \ldots, p_m \rangle, \quad p \in I \Leftrightarrow p = a_1 p_1 + \cdots + a_m p_m$$

$$P = \{p_1, \ldots, p_s\} \subseteq I$$

For ethvert $p \in I$ skal findes $p_i \in P$ så
"$p_i \cdot a = p$"

S-polynomiet.

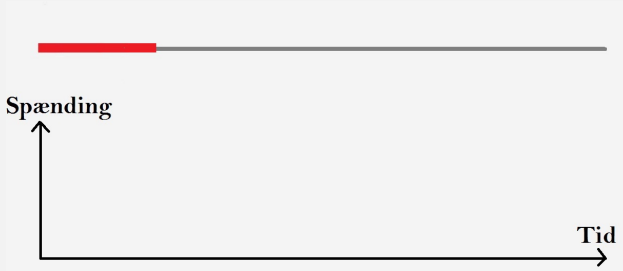


3. Division af polynomier

$$xy^4 + 3x^4 + 5 \ : \ x^2 - 2y^2 \ = \ ?$$

3. Division af polynomier

Vi har brug for det *betydende led* (eng.: initial term)



3. Division af polynomier

Vi har brug for det *betydende led* (eng.: initial term)

Definition (**Betydende led**)

Lad $p \in K[x_1, \ldots, x_n]$ *være givet ved*

$$p = \sum_{v \in \mathbb{N}_0^n} a_v X^v.$$

Lad desuden $u = \max_{\leq} \{v \in \mathbb{N}_0^n \mid a_v \neq 0\}$. *Det betydende led i polynomiet* p *er*

$$\mathrm{in}_{\leq}(p) = a_u p^u.$$

3. Division af polynomier

Vi har brug for en *ledordning* (eng.: term ordering).

3. Division af polynomier

Vi har brug for en *ledordning* (eng.: term ordering).

Ex. på en ledordning:

Definition (**Lexicografiske ordning**)

3. Division af polynomier

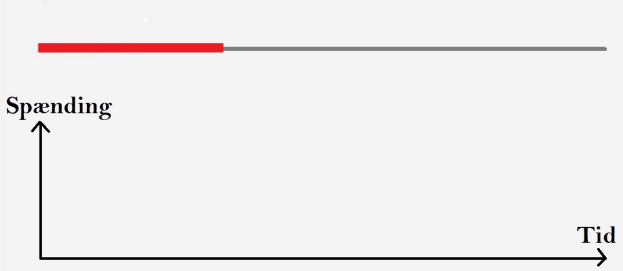
Vi har brug for en *ledordning* (eng.: term ordering).

Ex. på en ledordning:

Definition (**Lexicografiske ordning**)

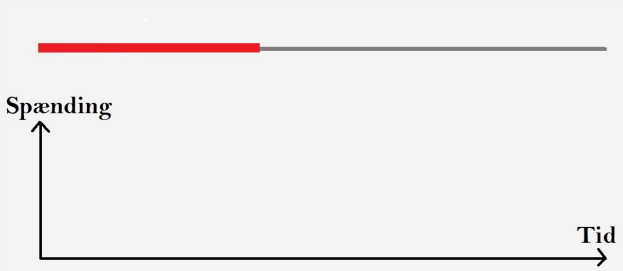
Lad $x = (x_1, \ldots, x_n) \in \mathbb{N}_0^n$ *og* $y = (y_1, \ldots, y_n) \in \mathbb{N}_0^n$.

$$
\begin{aligned}
x \leq_{\text{lex}} y \quad \Leftrightarrow \quad & x_1 < y_1 \ \textit{eller} \\
x \leq y \qquad\qquad & x_1 = y_1 \ \textit{og} \ x_2 < y_2 \ \textit{eller} \\
& x_1 = y_1 \ \textit{og} \ x_2 = y_2 \ \textit{og} \ x_3 < y_3 \ \textit{eller} \\
& \quad \vdots \\
& x_1 = y_1 \ \textit{og} \ x_2 = y_2 \ \textit{og} \ \ldots \ \textit{og} \ x_n = y_n.
\end{aligned}
$$



3. Division af polynomier

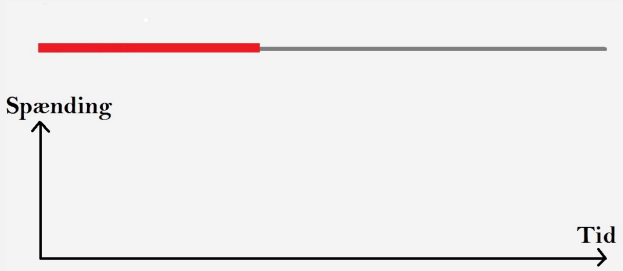
$$x^3y^2 + xy + z \ : \ \{x^2y + 2 \ , \ x + z\} \ = \ \{ \ , \ \} \, .$$



3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \left\{x^2y + 2 \ , \ x + z\right\} \ = \ \{xy \ , \ \}\,.$$

$$\underline{x^3y^2 + 2xy}$$

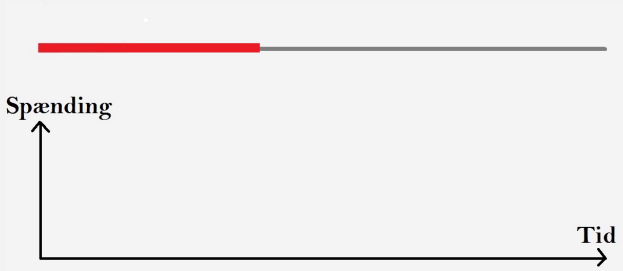


3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \{x^2y + 2 \ , \ x + z\} \ = \ \{xy \ , \ \}.$$

$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$



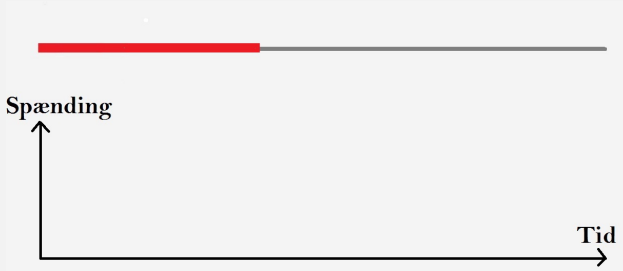
3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \{x^2y + 2 \ , \ x + z\} \ = \ \{xy \ , \ -y\} \, .$$

$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$

$$\underline{-xy - yz}$$



3. Division af polynomier

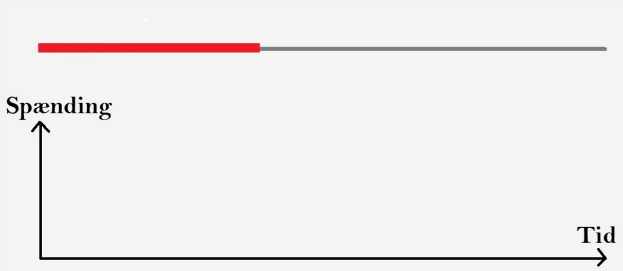
$$x^3y^2 + xy + z \ : \ \left\{x^2y + 2 \ , \ x + z\right\} \ = \ \{xy \ , \ -y\} \, .$$

$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$

$$\underline{-xy - yz}$$

$$\underline{yz + z}$$



3. Division af polynomier

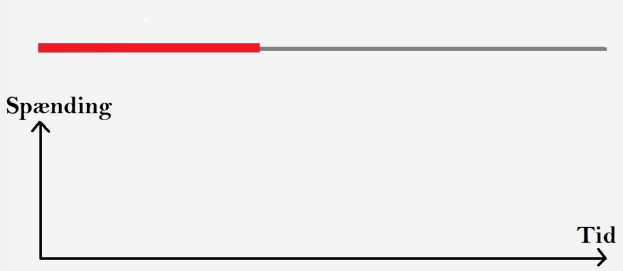
$$x^3y^2 + xy + z \ : \ \left\{x^2y + 2 \ , \ x + z\right\} \ = \ \{xy \ , \ -y\} \, .$$

$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$

$$\underline{-xy - yz}$$

$$\underline{yz + z} \longrightarrow yz$$



3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \left\{x^2y + 2 \ , \ x + z\right\} \ = \ \{xy \ , \ -y\} \, .$$

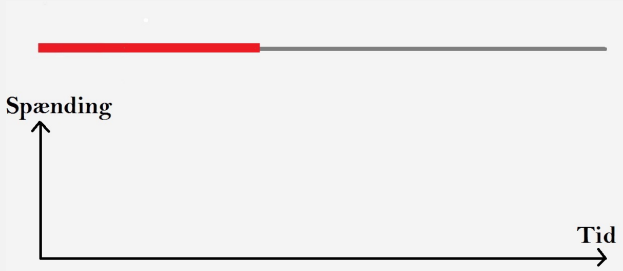
$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$

$$\underline{-xy - yz}$$

$$\underline{yz + z} \longrightarrow yz$$

$$\underline{z}$$



3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \left\{x^2y + 2 \ , \ x + z\right\} \ = \ \{xy \ , \ -y\} \, .$$

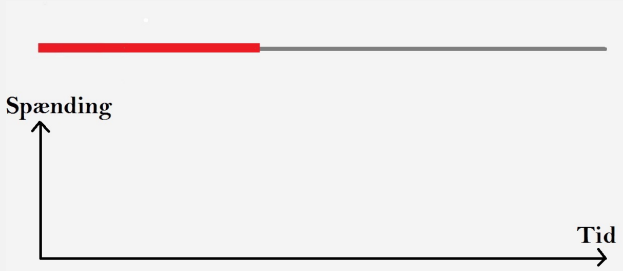
$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$

$$\underline{-xy - yz}$$

$$\underline{yz + z} \longrightarrow yz$$

$$\underline{z} \longrightarrow yz + z$$



3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \left\{x^2y + 2 \ , \ x + z\right\} \ = \ \{xy \ , \ -y\} \, .$$

$$\underline{x^3y^2 + 2xy}$$

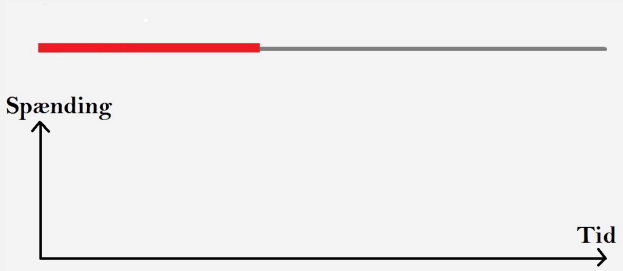
$$-xy + z$$

$$\underline{-xy - yz}$$

$$\underline{yz + z} \longrightarrow yz$$

$$\underline{z} \longrightarrow yz + z$$

$$0.$$



3. Division af polynomier

$$x^3y^2 + xy + z \ : \ \{x^2y + 2 \ , \ x + z\} \ = \ \{xy \ , \ -y\} \, .$$

$$\underline{x^3y^2 + 2xy}$$

$$-xy + z$$

$$\underline{-xy - yz}$$

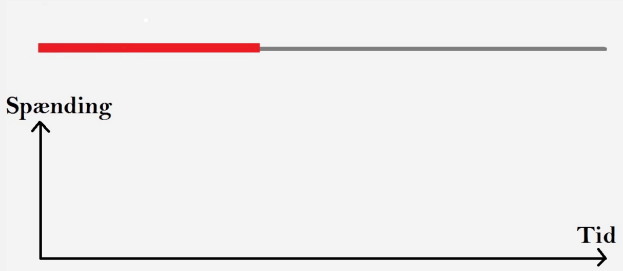
$$\underline{yz + z} \longrightarrow yz$$

$$\underline{z} \longrightarrow yz + z$$

$$0.$$

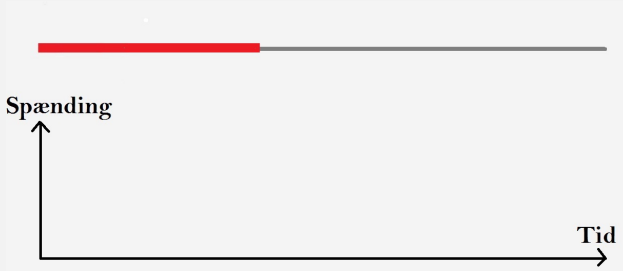
Dvs.

$$p = x^3y^2 + xy + z = \overbrace{xy(x^2y + 2)}^{a_1p_1} + \overbrace{-y(x + z)}^{a_2p_2} + \overbrace{yz + z}^{r} \, .$$



3. Division af polynomier

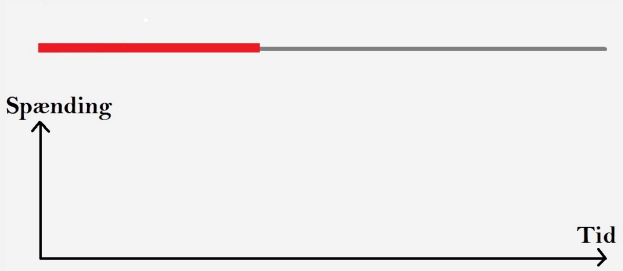
$$p = x^3y^2 + xy + z = \overbrace{xy(x^2y+2)}^{a_1p_1} + \overbrace{-y(x+z)}^{a_2p_2} + \overbrace{yz+z}^{r}.$$



3. Division af polynomier

$$p = x^3y^2 + xy + z = \overbrace{xy(x^2y+2)}^{a_1p_1} + \overbrace{-y(x+z)}^{a_2p_2} + \overbrace{yz+z}^{r}.$$

Bemærk, at $\mathrm{in}_{\leq}(p_1) \nmid yz$ og $\mathrm{in}_{\leq}(p_1) \nmid z$

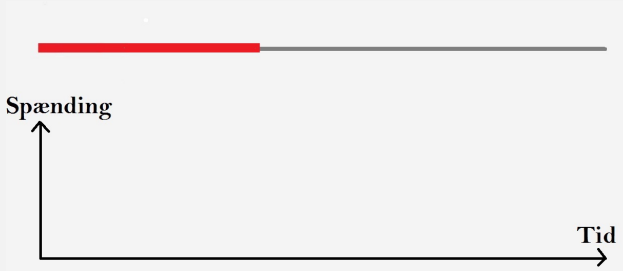


3. Division af polynomier

$$p = x^3y^2 + xy + z = \overbrace{xy(x^2y+2)}^{a_1p_1} + \overbrace{-y(x+z)}^{a_2p_2} + \overbrace{yz+z}^{r}.$$

Bemærk, at $\mathrm{in}_{\leq}(p_1) \nmid yz$ og $\mathrm{in}_{\leq}(p_1) \nmid z$

$\mathrm{in}_{\leq}(p_2) \nmid yz$ og $\mathrm{in}_{\leq}(p_2) \nmid z$

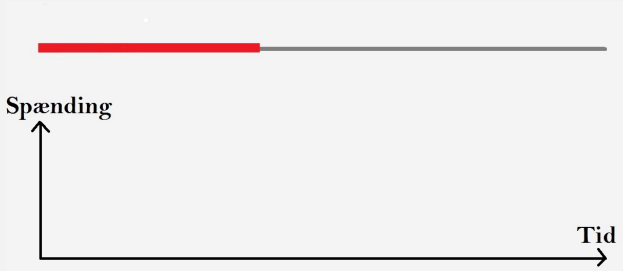


3. Division af polynomier

$$p = x^3y^2 + xy + z = \overbrace{xy(x^2y+2)}^{a_1p_1} + \overbrace{-y(x+z)}^{a_2p_2} + \overbrace{yz+z}^{r}.$$

Bemærk, at $\mathrm{in}_{\leq}(p_1) \nmid yz$ og $\mathrm{in}_{\leq}(p_1) \nmid z$
$\mathrm{in}_{\leq}(p_2) \nmid yz$ og $\mathrm{in}_{\leq}(p_2) \nmid z$

Hvis $P = \{p_1, p_2\}$, så skriver vi $r = p^P$



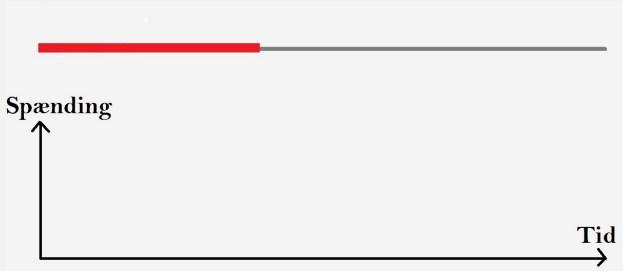
4. Gröbner-baser

Definition (**Gröbner-basis**)

Lad $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$. *Vi har, at* P *er en Gröbner-basis for et ideal* I *mht. en ledordning* $\leq$, *hvis*

$G1$ $P \subseteq I$ *og*

$G2$ *hvis der for alle* $p \in I$ *eksisterer et* $p_i \in \{p_1, \ldots, p_m\}$ *sådan, at* $\mathrm{in}_{\leq}(p_i) \mid \mathrm{in}_{\leq}(p)$.



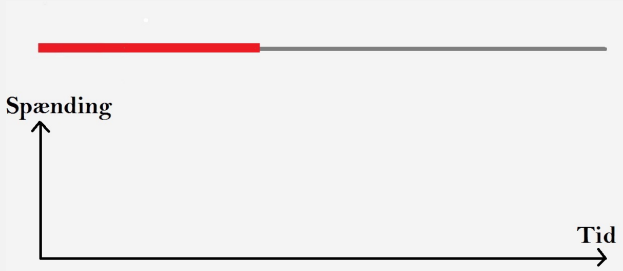
4. Gröbner-baser

Definition (**Gröbner-basis**)

Lad $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$. *Vi har, at* P *er en Gröbner-basis for et ideal* I *mht. en ledordning* $\leq$, *hvis*

- $G1$ $P \subseteq I$ *og*
- $G2$ *hvis der for alle* $p \in I$ *eksisterer et* $p_i \in \{p_1, \ldots, p_m\}$ *sådan, at* $\mathrm{in}_{\leq}(p_i) \mid \mathrm{in}_{\leq}(p)$.

Hvis intet andet er givet, da er $I = \langle p_1, \ldots, p_m \rangle$.



4. Gröbner-baser

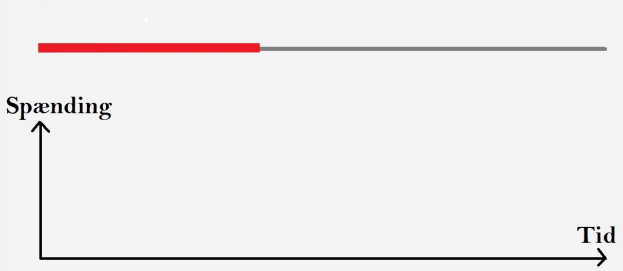
Definition (**Gröbner-basis**)

Lad $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$. *Vi har, at* P *er en Gröbner-basis for et ideal* I *mht. en ledordning* $\leq$, *hvis*

- $G1$ $P \subseteq I$ *og*
- $G2$ *hvis der for alle* $p \in I$ *eksisterer et* $p_i \in \{p_1, \ldots, p_m\}$ *sådan, at* $\mathrm{in}_{\leq}(p_i) \mid \mathrm{in}_{\leq}(p)$.

Hvis intet andet er givet, da er $I = \langle p_1, \ldots, p_m \rangle$.

Lad os se et eksempel på en Gröbner-basis!

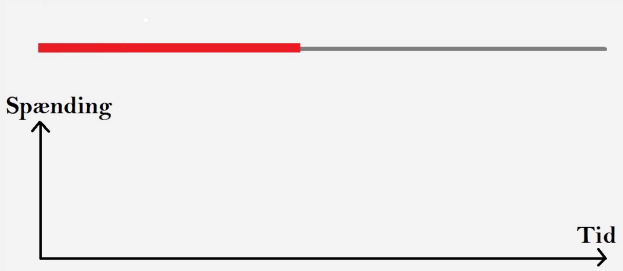


4. Gröbner-baser

Sætning

Lad $I \subseteq K[x_1, \ldots, x_n]$ og $\leq$ være en ledordning. Da gælder

1. *I har en Gröbner-basis*
2. *I er endelig frembragt.*

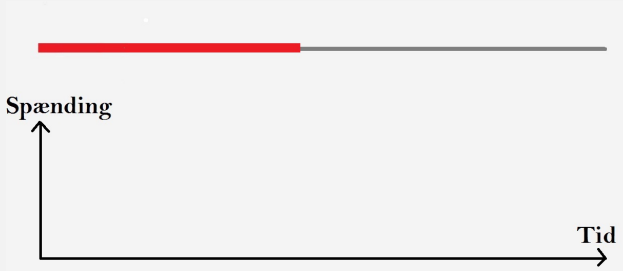


4. Gröbner-baser

Sætning

Lad $I \subseteq K[x_1, \ldots, x_n]$ og $\leq$ være en ledordning. Da gælder

1. *I har en Gröbner-basis*
2. *I er endelig frembragt.* ***Hilberts basissætning***



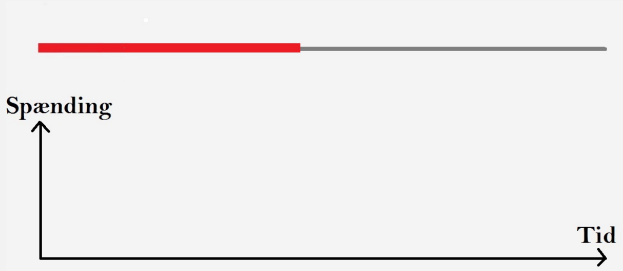
4. Gröbner-baser

Sætning

Lad $I \subseteq K[x_1, \ldots, x_n]$ og $\leq$ være en ledordning. Da gælder

1. *I har en Gröbner-basis*
2. *I er endelig frembragt.* ***Hilberts basissætning***

Beviset bruger *Dicksons lemma*



4. Gröbner-baser

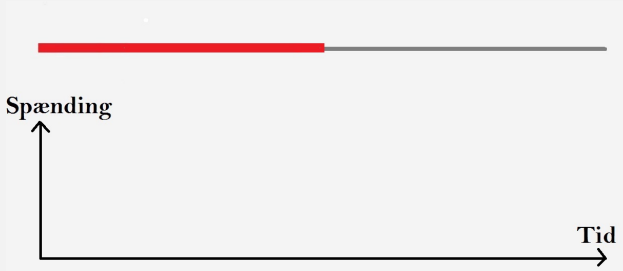
Definition (**Reducere til 0**)

Lad $p \in K[x_1, \ldots, x_n]$ *og* $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$.
Hvis der findes $a_1, \ldots, a_m \in K[x_1, \ldots, x_n]$ *sådan, at*

1. $p = a_1 p_1 + \cdots + a_m p_m$ *og*
2. $\mathrm{in}_{\leq}(a_i p_i) \leq \mathrm{in}_{\leq}(p)$,

så siger vi

$$p \to_P 0.$$



4. Gröbner-baser

Definition (**Reducere til 0**)

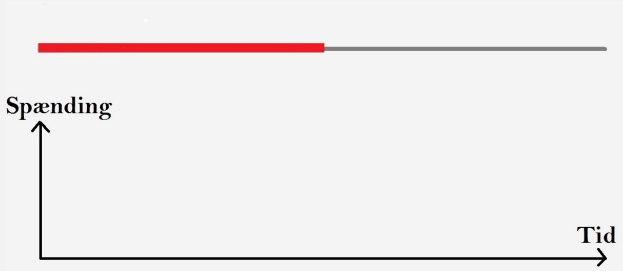
Lad $p \in K[x_1, \ldots, x_n]$ *og* $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$.
Hvis der findes $a_1, \ldots, a_m \in K[x_1, \ldots, x_n]$ *sådan, at*

1. $p = a_1 p_1 + \cdots + a_m p_m$ *og*
2. $\mathrm{in}_{\leq}(a_i p_i) \leq \mathrm{in}_{\leq}(p)$,

så siger vi

$$p \to_P 0.$$

Bemærk sammenhængen mellem $p^P = 0$ og $p \to_P 0$.



4. Gröbner-baser

Definition (**Reducere til 0**)

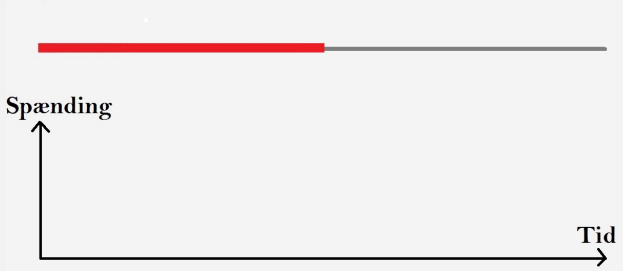
Lad $p \in K[x_1, \ldots, x_n]$ *og* $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n] \setminus \{0\}$.
Hvis der findes $a_1, \ldots, a_m \in K[x_1, \ldots, x_n]$ *sådan, at*

1. $p = a_1 p_1 + \cdots + a_m p_m$ *og*
2. $\mathrm{in}_{\leq}(a_i p_i) \leq \mathrm{in}_{\leq}(p)$,

så siger vi

$$p \to_P 0.$$

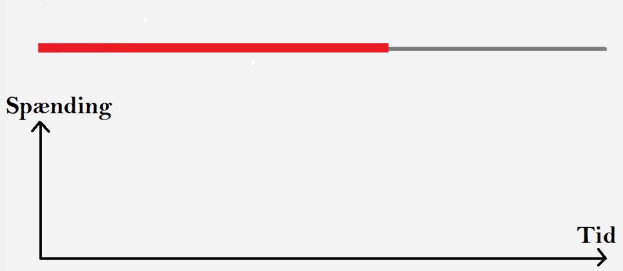
Bemærk sammenhængen mellem $p^P = 0$ og $p \to_P 0$.
Der gælder følgende sætning



4. Gröbner-baser

Sætning

$P = \{p_1, \ldots, p_m\}$ *og* $I = \langle p_1, \ldots, p_m \rangle$. *Hvis der for alle* $p \in I$ *gælder, at* $p \to_P 0$, ***så er*** P ***en Gröbner-basis for*** I.



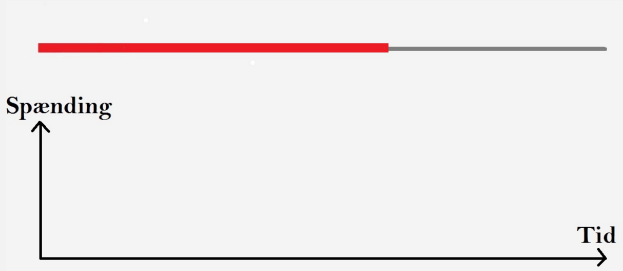
4. Gröbner-baser

Sætning

$P = \{p_1, \ldots, p_m\}$ og $I = \langle p_1, \ldots, p_m \rangle$. Hvis der for alle $p \in I$ gælder, at $p \to_P 0$, ***så er P en Gröbner-basis for I.***

Hvis P er en Gröbner-basis for I, så gælder der for alle $p \in I$, at

$$p \to_P 0 \quad \Leftrightarrow \quad p^P = 0.$$



4. Gröbner-baser

Sætning

$P = \{p_1, \ldots, p_m\}$ og $I = \langle p_1, \ldots, p_m \rangle$. Hvis der for alle $p \in I$ gælder, at $p \to_P 0$, ***så er P en Gröbner-basis for I.***

Hvis P er en Gröbner-basis for I, så gælder der for alle $p \in I$, at

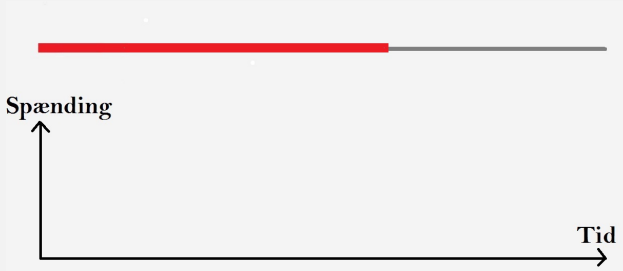
$$p \to_P 0 \quad \Leftrightarrow \quad p^P = 0.$$

Vi skal altså se på

$$p = a_1 p_1 + \cdots + a_m p_m \in I$$

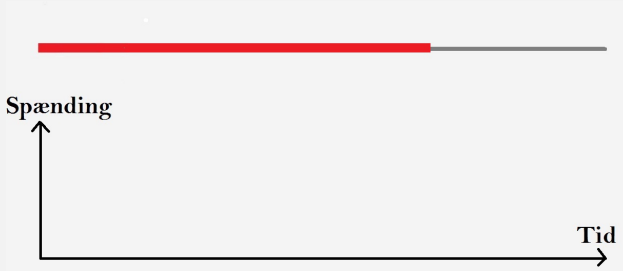
Reducere til 0.

1. $p = a_1 p_1 + \cdots + a_m p_m$og
2. $\mathrm{in}_{\leq}(a_i p_i) \leq \mathrm{in}_{\leq}(p)$



4. Gröbner-baser

Vi har brug for *S-polynomiet* !



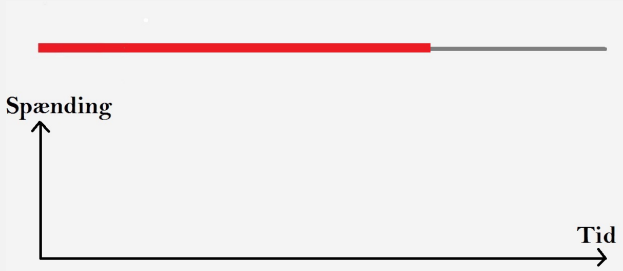
4. Gröbner-baser

Vi har brug for *S-polynomiet* !

Definition

Sæt $\mathrm{mfm}\big(\mathrm{in}_{\leq}(p), \mathrm{in}_{\leq}(q)\big) := X^{\xi}$. *Så er S-polynomiet af p og q mht. en ledordning* $\leq$ *givet ved*

$$S(p,q) = X^{\xi}\left(\frac{p}{\mathrm{in}_{\leq}(p)} - \frac{q}{\mathrm{in}_{\leq}(q)}\right).$$



4. Gröbner-baser

Vi har brug for *S-polynomiet* !

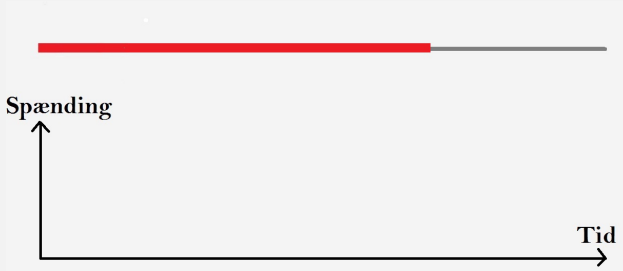
Definition

Sæt $\mathrm{mfm}\big(\mathrm{in}_{\leq}(p), \mathrm{in}_{\leq}(q)\big) := X^{\xi}$. *Så er S-polynomiet af p og q mht. en ledordning* $\leq$ *givet ved*

$$S(p,q) = X^{\xi}\left(\frac{p}{\mathrm{in}_{\leq}(p)} - \frac{q}{\mathrm{in}_{\leq}(q)}\right).$$

Eksempel

Vi vil finde S-polynomiet af $p_1 = x^2 + y^2 + z^2 - 1$ og $p_2 = x + y + z$.



4. Gröbner-baser

$$
\begin{aligned}
S(p_1, p_2) &= \operatorname{mfm}\big(\operatorname{in}_{\leq}(p_1), \operatorname{in}_{\leq}(p_2)\big)\left(\frac{p_1}{\operatorname{in}_{\leq}(p_1)} - \frac{p_2}{\operatorname{in}_{\leq}(p_2)}\right) \\
&= \operatorname{mfm}(x^2, x)\left(\frac{x^2+y^2+z^2-1}{x^2} - \frac{x+y+z}{x}\right) \\
&= x^2\left(\frac{x^2+y^2+z^2-1}{x^2} - \frac{x+y+z}{x}\right) \\
&= x^2+y^2+z^2-1-x^2-xy-xz \\
&= -xy-xz+y^2+z^2-1
\end{aligned}
$$

4.

then P is a Gröbner basis for I.
On the other hand: If P is a Gröbner basis for I then for all $p \in I$ it is true that

$$p \to_P 0 \quad \Rightarrow \quad p^P = 0.$$

Proof.
Let $p \in I \setminus \{0\}$. In order to show that P is a Gröbner basis we need to show that (G1) and (G2) from the definition of a Gröbner basis are satisfied.
It is clear that $P \subseteq I$. That is (G1).
(G2) is fulfilled because $p \to_P 0$ for all $p \in I$. This means that $\mathrm{in}_\leq(a_i p_i) \leq \mathrm{in}_\leq(p)$ when $a_i p_i \neq 0$ and we are able to write

$$p = a_1 p_1 + \cdots + a_m p_m,$$

for $a_1, \ldots, a_m \in K[x_1, \ldots, x_n]$. All initial terms $\mathrm{in}_\leq(a_i p_i)$ are less than or equal to the initial term of p so we have seen on the pages before that $\mathrm{in}_\leq(p_i) \mid \mathrm{in}_\leq(p)$ for some $p_i \in P$. Hence P must be a Gröbner basis.
The second statement: If P is a Gröbner basis then

$$p \to_P 0 \Rightarrow p^P = 0.$$

Now we assume that $p \to_P 0$. We know that P is a Gröbner basis for $I = \langle p_1, \ldots, p_m \rangle$ and that $p \in I$. Now proposition 3.3 says that $p^P = 0$. □

Right before this proposition we were about to look at the situation where $v < \delta$. We will carry on with our calculations and reach a point where we have created a nice polynomial which will help us. We let

$$p = a_1 p_1 + \cdots + a_m p_m \in I = \langle p_1, \ldots, p_m \rangle,$$

where $a_1, \ldots, a_m \in K[x_1, \ldots, x_n]$. We define $C := \mathrm{in}_\leq(a_1)p_1 + \cdots + \mathrm{in}_\leq(a_r)p_r$ for $1 < r < m$. We are then allowed to express p like

$$\begin{aligned} p = & C + (a_1 - \mathrm{in}_\leq(a_1))p_1 + \cdots + (a_r - \mathrm{in}_\leq(a_r))p_r \\ & + a_{r+1}p_{r+1} + \cdots + a_m p_m. \end{aligned} \tag{4.2}$$

We observe that p is the sum of C and polynomials whose initial terms are strictly less the δ.
We have seen that whenever $b_1 c_1 + \cdots + b_r c_r \neq 0$ we have no cancellation among the initial terms on the right hand side of (4.1). This led to the fact that there exists $p_i \in \{p_1, \ldots, p_m\}$ such that

$$\mathrm{in}_\leq(p_i) \mid \mathrm{in}_\leq(p).$$

On the other hand: $b_1 c_1 + \cdots + b_r c_r = 0$. Then we were not sure if there existed an initial term which divided the initial term of p. We will fix this problem by creating the S-polynomials.

4.

We put $q_i := X^{w_i}\frac{p_i}{c_i}$. First we want to express C in terms of the q_i's.

$$\begin{aligned} C &= \mathrm{in}_{\leq}(a_1)p_1 + \cdots + \mathrm{in}_{\leq}(a_r)p_r \\ &= b_1 X^{w_1} p_1 + \cdots + b_r X^{w_r} p_r \\ &= b_1 c_1 q_q + \cdots + b_r c_r q_r. \end{aligned}$$

Next we want to express C as a linear combination of $q_i - q_j = X^{w_i}\frac{p_i}{c_i} - X^{w_j}\frac{p_j}{c_j}$. We underline the terms that occur above. The rest will cancel out.

$$\begin{aligned} C =& \overbrace{\underline{b_1c_1q_1} - b_1c_1q_2 + b_1c_1q_2}^{=0} + \underline{b_2c_2q_2} \overbrace{- b_1c_1q_3 - b_2c_2q_3 + b_1c_1q_3 + b_2c_2q_3}^{=0} \\ &+ \underline{b_3c_3q_3} - b_1c_1q_4 - b_2c_2q_4 - b_3c_3q_4 + \cdots \\ &+ (b_1c_1q_{r-1} + \cdots + \underline{b_{r-1}c_{r-1}q_{r-1}}) - (b_1c_1q_r + \cdots + b_{r-1}c_{r-1}q_r) \\ &+ (b_1c_1q_r + \cdots + \underline{b_rc_rq_r}). \end{aligned}$$

$$\begin{aligned} =& b_1c_1(q_1 - q_2) + (b_1c_1 + b_2c_2)(q_2 - q_3) + (b_1c_1 + b_2c_2 + b_3c_3)(q_3 - q_4) \\ &+ \cdots + (b_1c_1 + \cdots + b_{r-1}c_{r-1})(q_{r-1} - q_r) + (b_1c_1 + \cdots + b_rc_r)q_r \end{aligned}$$

$$\begin{aligned} =& b_1c_1(q_1 - q_2) + (b_1c_1 + b_2c_2)(q_2 - q_3) + (b_1c_1 + b_2c_2 + b_3c_3)(q_3 - q_4) \\ &+ \cdots + (b_1c_1 + \cdots + b_{r-1}c_{r-1})(q_{r-1} - q_r). \end{aligned}$$

We have reached a point where we have expressed C as a linear combination of

$$q_i - q_j = X^{w_i}\frac{p_i}{c_i} - X^{w_j}\frac{p_j}{c_j}.$$

This is quite nice because $w_i + u_i = w_j + u_j \in \mathbb{N}_0^n$, which means that $\mathrm{in}_{\leq}(q_i)$ and $\mathrm{in}_{\leq}(q_j)$ cancel each other. That is nice!
We put $X^{\xi} := \mathrm{lcm}(X^{u_i}, X^{u_j})$. Let us rewrite $q_i - q_j$ in preparation for the construction of the famous S-polynomials.

$$\begin{aligned} q_i - q_j &= X^{w_i}\frac{p_i}{c_i} - X^{w_j}\frac{p_j}{c_j} \\ &= X^{w_i}\frac{X^{u_i}}{c_iX^{u_i}}p_i - X^{w_j}\frac{X^{u_j}}{c_jX^{u_j}}p_j \\ &= X^{\varphi}\left(\frac{X^{\xi}}{c_iX^{u_i}}p_i - \frac{X^{\xi}}{c_jX^{u_j}}p_j\right) \\ &= X^{\varphi}X^{\xi}\left(\frac{p_i}{\mathrm{in}_{\leq}(p_i)} - \frac{p_j}{\mathrm{in}_{\leq}(p_j)}\right), \end{aligned}$$

where $\varphi + \xi = u_i + v_i = u_j + v_j$. Leading us to the general definition of the S-polynomial of two non-zero polynomials.

Definition 4.4 (S-**polynomial**)
Let $p, q \in K[x_1, \ldots, x_n] \setminus \{0\}$. Put $\mathrm{lcm}(\mathrm{in}_{\leq}(p), \mathrm{in}_{\leq}(q)) := X^{\xi}$. Now the S-polynomial

4.

of p and q with respect to a term ordering $\leq$ is given by

$$S(p,q) = X^{\xi}\left(\frac{p}{\mathrm{in}_{\leq}(p)} - \frac{q}{\mathrm{in}_{\leq}(q)}\right).$$

Because of the S-polynomials we can write

$$q_i - q_j = X^{\varphi} S(p_i, p_j).$$

Which allows us to write C in yet another way.

$$\begin{aligned} C &= d_1(q_1 - q_2) + d_2(q_2 - q_3) + \cdots + d_{r-1}(q_{r-1} - q_r) \\ &= d_1 X^{\varphi_1} S(p_1, p_2) + \cdots + d_{r-1} X^{\varphi_{r-1}} S(p_{r-1}, p_r) \end{aligned} \tag{4.3}$$

We know that for all $i \in \{1, \ldots, r-1\}$

$$\mathrm{in}_{\leq}\big(X^{\varphi_i} S(p_i, p_{i+1})\big) < \delta.$$

This is exactly what we wanted and we will use it in the proof of the following theorem which is the foundation for Buchberger's algorithm that tells us how to find Gröbner bases.

Buchberger's theorem

Let us go straight to the theorem.

Theorem 4.5 (Buchberger)
Let $P = \{p_1, \ldots, p_m\} \subseteq K[x_1, \ldots, x_n]$. P is a Gröbner basis if and only if $S(p_i, p_j) \to_P 0$ for $1 \leq i < j \leq m$.

Proof.
Take $p \in I = \langle p_1, \ldots, p_m \rangle$. We may put

$$p = a_1 p_1 + \cdots + a_m p_m$$

for $a_1, \ldots, a_m \in K[x_1, \ldots, x_n]$. Since $S(p_i, p_j) \to_P 0$ the definition says

$$S(p_i, p_j) = e_1 p_1 + \cdots + e_m p_m, \tag{4.4}$$

for $e_1, \ldots, e_m \in K[x_1, \ldots, x_n]$ and with

$$\mathrm{in}_{\leq}(e_k p_k) \leq \mathrm{in}_{\leq}\big(S(p_i, p_j)\big)$$

for $k \in \{1, \ldots, m\}$.

According to (4.2) we were able to put p like

$$\begin{aligned} p = &C + \big(a_1 - \mathrm{in}_{\leq}(a_1)\big)p_1 + \cdots + \big(a_r - \mathrm{in}_{\leq}(a_r)\big)p_r \\ &+ a_{r+1}p_{r+1} + \cdots + a_m p_m, \end{aligned}$$

4. Gröbner-baser

Sætning (**Buchbergers sætning**)

Lad $P = \{p_1, \ldots, p_m\}$. P *er en Gröbner-basis hvis og kun hvis der for* $1 \leq i < j \leq m$ *gælder, at* $S(p_i, p_j) \to_P 0$.

4. Gröbner-baser

Sætning (**Buchbergers sætning**)

Lad $P = \{p_1, \ldots, p_m\}$. P *er en Gröbner-basis hvis og kun hvis der for* $1 \leq i < j \leq m$ *gælder, at* $S(p_i, p_j) \to_P 0$.

Beviset bruger netop den lækre egenskab ved S-polynomiet.

4. Gröbner-baser

Sætning (**Buchbergers sætning**)

Lad $P = \{p_1, \ldots, p_m\}$. *P er en Gröbner-basis hvis og kun hvis der for* $1 \leq i < j \leq m$ *gælder, at* $S(p_i, p_j) \to_P 0$.

Beviset bruger netop den lækre egenskab ved S-polynomiet.

Sammenhængen mellem $p \to_P 0$ og $p^P = 0$ giver os S-kriteriet:

Sætning (**S-kriteriet**)

Lad $P = \{p_1, \ldots, p_m\}$. *P er en Gröbner-basis hvis og kun hvis der for* $1 \leq i < j \leq m$ *gælder, at* $S(p_i, p_j)^P = 0$.

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

Så tilføjer vi $S(p_k, p_l)^P$ til mængden af polynomier og får

$$P' = P \cup \left\{S(p_k, p_l)^P\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P\right\}.$$

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

Så tilføjer vi $S(p_k, p_l)^P$ til mængden af polynomier og får

$$P' = P \cup \left\{S(p_k, p_l)^P\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P\right\}.$$

Finder $p_r, p_s \in P'$, så $S(p_r, p_s)^{P'} \neq 0$.

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

Så tilføjer vi $S(p_k, p_l)^P$ til mængden af polynomier og får

$$P' = P \cup \left\{S(p_k, p_l)^P\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P\right\}.$$

Finder $p_r, p_s \in P'$, så $S(p_r, p_s)^{P'} \neq 0$.

Vi tilføjer blot

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

Så tilføjer vi $S(p_k, p_l)^P$ til mængden af polynomier og får

$$P' = P \cup \left\{S(p_k, p_l)^P\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P\right\}.$$

Finder $p_r, p_s \in P'$, så $S(p_r, p_s)^{P'} \neq 0$.

Vi tilføjer blot

$$P'' = P' \cup \left\{S(p_r, p_s)^{P'}\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P, S(p_r, p_s)^{P'}\right\}$$

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

Så tilføjer vi $S(p_k, p_l)^P$ til mængden af polynomier og får

$$P' = P \cup \left\{S(p_k, p_l)^P\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P\right\}.$$

Finder $p_r, p_s \in P'$, så $S(p_r, p_s)^{P'} \neq 0$.

Vi tilføjer blot

$$P'' = P' \cup \left\{S(p_r, p_s)^{P'}\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P, S(p_r, p_s)^{P'}\right\}$$

Stopper det på et tidspunkt?

4. Gröbner-baser

Buchbergers algoritme

$P = \{p_1, \ldots, p_m\}$. Finder p_k og p_l, så $S(p_k, p_l)^P \neq 0$.

Så tilføjer vi $S(p_k, p_l)^P$ til mængden af polynomier og får

$$P' = P \cup \left\{S(p_k, p_l)^P\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P\right\}.$$

Finder $p_r, p_s \in P'$, så $S(p_r, p_s)^{P'} \neq 0$.

Vi tilføjer blot

$$P'' = P' \cup \left\{S(p_r, p_s)^{P'}\right\} = \left\{p_1, \ldots, p_m, S(p_k, p_l)^P, S(p_r, p_s)^{P'}\right\}$$

Stopper det på et tidspunkt?

Ja! Dicksons lemma sikrer os endnu en gang.

4. Gröbner-baser

Vi er *altid* i stand til at finde Gröbner-basen for et ideal!

4. Gröbner-baser

Vi er *altid* i stand til at finde Gröbner-basen for et ideal!

Kan det bruges til noget?

5. Anvendelser

- Robotvidenskab
- Generel optimering

5. Anvendelser

- Robotvidenskab
- Generel optimering

			4
4		2	
	3		1

5. Anvendelser

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8

x_9	x_{10}	x_{11}	x_{12}
x_{13}	x_{14}	x_{15}	x_{16}

5. Anvendelser

$$(x_1 - 1)(x_1 - 2)(x_1 - 3)(x_1 - 4) = 0$$

$$\vdots$$

$$(x_{16} - 1)(x_{16} - 2)(x_{16} - 3)(x_{16} - 4) = 0.$$

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	x_{11}	x_{12}
x_{13}	x_{14}	x_{15}	x_{16}

5. Anvendelser

$$(x_1-1)(x_1-2)(x_1-3)(x_1-4)=0$$

$$\vdots$$

$$(x_{16}-1)(x_{16}-2)(x_{16}-3)(x_{16}-4)=0$$

$$x_1x_2x_3x_4-24=0$$

$$\vdots$$

$$x_{11}x_{12}x_{15}x_{16}-24=0.$$

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	x_{11}	x_{12}
x_{13}	x_{14}	x_{15}	x_{16}

5. Anvendelser

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	x_{11}	x_{12}
x_{13}	x_{14}	x_{15}	x_{16}

$$
\begin{aligned}
(x_1-1)(x_1-2)(x_1-3)(x_1-4) &= 0\\
&\vdots\\
(x_{16}-1)(x_{16}-2)(x_{16}-3)(x_{16}-4) &= 0\\
x_1x_2x_3x_4-24 &= 0\\
&\vdots\\
x_{11}x_{12}x_{15}x_{16}-24 &= 0\\
x_1+x_2+x_3+x_4-10 &= 0\\
&\vdots\\
x_{11}+x_{12}+x_{15}+x_{16}-10 &= 0.
\end{aligned}
$$

40 ligninger.

5. Anvendelser

			4
4		2	
	3		1

De 40 ligninger sammen med:

$$x_4 - 4 = 0$$

$$x_5 - 4 = 0$$

$$x_7 - 2 = 0$$

$$x_{10} - 3 = 0$$

$$x_{12} - 1 = 0$$

5. Anvendelser

Vi finder Gröbner-basen for idealet frembragt af de 45 ligninger vha. en computer og får et nyt ligningssystem.

$$
\begin{array}{ll}
x_1 - 3 = 0 & x_2 - 2 = 0 \\
x_3 - 1 = 0 & x_4 - 4 = 0 \\
x_5 - 4 = 0 & x_6 - 1 = 0 \\
x_7 - 2 = 0 & x_8 - 3 = 0 \\
x_9 - 2 = 0 & x_{10} - 3 = 0 \\
x_{11} - 4 = 0 & x_{12} - 1 = 0 \\
x_{13} - 1 = 0 & x_{14} - 4 = 0 \\
x_{15} - 3 = 0 & x_{16} - 2 = 0.
\end{array}
$$

6. Lyn-opsummering