Résolution de systèmes polynomiaux à l'aide de bases de Gröbner

Vanessa VITSE

Université de Versailles Saint-Quentin, Laboratoire PRISM

8 octobre 2009

Bases de Gröbner, pour quoi faire ?

$I = \langle f_1, \ldots, f_k \rangle$ idéal de $K[X_1, \ldots, X_n]$

Objectifs

- déterminer si $f \in K[X_1, \ldots, X_n]$ est un élément de I (membership)
- déterminer un analogue de la division euclidienne en plusieurs variables
- trouver un bon système de représentants de $K[X_1, \ldots, X_n]/I$
- implicitation d'une courbe ou surface paramétrée
- résoudre un système polynomial en plusieurs variables

Bases de Gröbner, pour quoi faire ?

$I = \langle f_1, \ldots, f_k \rangle$ idéal de $K[X_1, \ldots, X_n]$

Objectifs

- déterminer si $f \in K[X_1, \ldots, X_n]$ est un élément de I (membership)
- déterminer un analogue de la division euclidienne en plusieurs variables
- trouver un bon système de représentants de $K[X_1, \ldots, X_n]/I$
- implicitation d'une courbe ou surface paramétrée
- résoudre un système polynomial en plusieurs variables
  - cryptanalyse HFE
  - calcul d'index sur courbes elliptiques ou hyperelliptiques
  - ...

Division de polynômes multivariés

Objectif

Trouver un analogue de la division euclidienne sur $K[X]$ dans $K[X_1, \ldots, X_n] \leftrightarrow$ Diviser $f \in K[X_1, \ldots, X_n]$ par une famille de polynômes $G = \{g_1, \ldots, g_s\}$

Division de polynômes multivariés

Objectif

Trouver un analogue de la division euclidienne sur $K[X]$ dans $K[X_1, \ldots, X_n] \leftrightarrow$ Diviser $f \in K[X_1, \ldots, X_n]$ par une famille de polynômes $G = \{g_1, \ldots, g_s\}$

Ordre sur les monômes

- l'ordre doit être total, compatible à la multiplication et bien ordonné
- $lex_{X_1 > X_2 > \ldots > X_n}$: le plus grand monôme est celui qui contient le plus de X_1, puis le plus de X_2... Ex : $X_1 > X_2^4$
- $deglex_{X_1 > X_2 > \ldots > X_n}$: par degré puis par ordre $lex_{X_1 > X_2 > \ldots > X_n}$.
  Ex : $X_1^4 > X_2^4 > X_1$
- $degrevlex_{X_1 > X_2 > \ldots > X_n}$: par degré puis par ordre $lex_{X_1 > X_2 > \ldots > X_n}$ "inversé" $\longrightarrow$ le plus petit monôme est celui qui contient le plus de X_n, puis le plus de X_{n-1}...
  Ex : $X_2^4 > X_1 X_3$ mais $X_1^2 X_2^2 X_3 > X_1^3 X_3^2$

Algorithme de division en plusieurs variables

ENTRÉE : $f \in K[X_1, \ldots, X_n]$ à diviser par une liste de polynômes $G = \{g_1, \ldots, g_s\}$
SORTIE : r le reste de la division de f par G

1. $r \leftarrow 0$
2. **tant que** $f \neq 0$ **faire**
3. **pour** $i = 1$ à s **faire**
4. **si** $\mathrm{lt}(g_i) | \mathrm{lt}(f)$ **alors**
5. $f \leftarrow f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g_i)} g_i$
6. $i \leftarrow 0$
7. **fin si**
8. **fin pour**
9. $r \leftarrow r + \mathrm{lt}(f)$
10. $f \leftarrow f - \mathrm{lt}(f)$
11. **fin tant que**
12. **retourner** r

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

$f \leftarrow f - yg_1 = x + y^2 + y$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

$f \leftarrow f - yg_1 = x + y^2 + y$

$r \leftarrow r + x = x$

$f \leftarrow f - x = y^2 + y$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

$f \leftarrow f - yg_1 = x + y^2 + y$

$r \leftarrow r + x = x$

$f \leftarrow f - x = y^2 + y$

$f \leftarrow f - g_2 = y + 1$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

$f \leftarrow f - yg_1 = x + y^2 + y$

$r \leftarrow r + x = x$

$f \leftarrow f - x = y^2 + y$

$f \leftarrow f - g_2 = y + 1$

$r \leftarrow r + y = x + y$

$f \leftarrow f - y = 1$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

$f \leftarrow f - yg_1 = x + y^2 + y$

$r \leftarrow r + x = x$

$f \leftarrow f - x = y^2 + y$

$f \leftarrow f - g_2 = y + 1$

$r \leftarrow r + y = x + y$

$f \leftarrow f - y = 1$

$r \leftarrow r + 1 = x + y + 1$

$f \leftarrow f - 1 = 0$

Exemple

Division de $f = x^2y + xy^2 + y^2$ par $G = \{xy - 1, y^2 - 1\}$ pour $lex_{x>y}$

Init : $f \leftarrow x^2y + xy^2 + y^2$; $r \leftarrow 0$

$f \leftarrow f - xg_1 = xy^2 + x + y^2$

$f \leftarrow f - yg_1 = x + y^2 + y$

$r \leftarrow r + x = x$

$f \leftarrow f - x = y^2 + y$

$f \leftarrow f - g_2 = y + 1$

$r \leftarrow r + y = x + y$

$f \leftarrow f - y = 1$

$r \leftarrow r + 1 = x + y + 1$

$f \leftarrow f - 1 = 0$

$$f = (x + y)g_1 + g_2 + (x + y + 1)$$

Algorithme de division

Remarque

A la fin de l'algorithme, on trouve un reste $r = \overline{f}^G$ non divisible par les termes de tête des $g_i \in G$.

Exemple : $G = \{xy - 1, y^2 - 1\}$ et $\overline{f}^G = x + y + 1$ pour $lex_{x>y}$

Algorithme de division

Remarque

A la fin de l'algorithme, on trouve un reste $r = \overline{f}^G$ non divisible par les termes de tête des $g_i \in G$.

Exemple : $G = \{xy - 1, y^2 - 1\}$ et $\overline{f}^G = x + y + 1$ pour $lex_{x>y}$

Unicité du reste ?

- l'algorithme dépend de l'ordre monomial choisi et de l'ordre suivant lequel on considère les g_i dans G
- le reste sera unique si $G = \{g_1, \ldots, g_s\}$ est une base de Gröbner

Exemple : $G = \{y^2 - 1, xy - 1\}$ et $\overline{f}^G = 2x + 1$ pour $lex_{x>y}$

Bases de Gröbner

On fixe un ordre monomial.

Définitions

Soit $I = \langle f_1, \ldots, f_m \rangle$ un idéal de $K[X_1, \ldots, X_n]$

- $\mathrm{LT}(I) = \langle \{\mathrm{lt}(f) : f \in I\} \rangle$ est appelé **idéal initial** de I
- $\{g_1, \ldots, g_s\} \subset I$ est une **base de Gröbner** de I si

$$\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle = \mathrm{LT}(I)$$

En particulier, $I = \langle g_1, \ldots, g_s \rangle$.

Bases de Gröbner

On fixe un ordre monomial.

Définitions

Soit $I = \langle f_1, \ldots, f_m \rangle$ un idéal de $K[X_1, \ldots, X_n]$

- $\mathrm{LT}(I) = \langle \{\mathrm{lt}(f) : f \in I\} \rangle$ est appelé **idéal initial** de I
- $\{g_1, \ldots, g_s\} \subset I$ est une **base de Gröbner** de I si

$$\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle = \mathrm{LT}(I)$$

En particulier, $I = \langle g_1, \ldots, g_s \rangle$.

Propriétés des bases de Gröbner

$f \in K[X_1, \ldots, X_n]$, G est base de Gröbner de $I = \langle f_1, \ldots, f_m \rangle$

- $\overline{f}^G = 0 \Leftrightarrow f \in I$
- unicité du reste $\overline{f}^G$ dans la division de f par G

Théorie de l'élimination

Objectif

Faire un analogue de l'élimination gaussienne de systèmes linéaires pour des systèmes polynomiaux multivariés.

Théorie de l'élimination

Objectif

Faire un analogue de l'élimination gaussienne de systèmes linéaires pour des systèmes polynomiaux multivariés.

l-ème idéal d'élimination

$I_l = I \cap K[X_{l+1}, \ldots, X_n]$ est un idéal de $K[X_{l+1}, \ldots, X_n]$ appelé l-ème **idéal d'élimination**.

Théorie de l'élimination

Objectif

Faire un analogue de l'élimination gaussienne de systèmes linéaires pour des systèmes polynomiaux multivariés.

l-ème idéal d'élimination

$I_l = I \cap K[X_{l+1}, \ldots, X_n]$ est un idéal de $K[X_{l+1}, \ldots, X_n]$ appelé l-ème **idéal d'élimination**.

- Idée : calculer progressivement $V(I_{n-1}), V(I_{n-2}), \ldots, V(I_0)$
- Outils :
  - bases de Gröbner pour obtenir I_k
  - théorème d'extension des solutions pour passer de $V(I_l)$ à $V(I_{l-1})$

Résolution de systèmes

1. Calcul d'une base de Gröbner de I_k :
   Si G base de Gröbner de I pour l'ordre $lex_{X_1>\ldots>X_n}$ alors
   $G \cap K[X_{l+1}, \ldots X_n]$ est une base de Gröbner de I_l

Résolution de systèmes

1. Calcul d'une base de Gröbner de I_k :
   Si G base de Gröbner de I pour l'ordre $lex_{X_1>\ldots>X_n}$ alors
   $G \cap K[X_{l+1}, \ldots X_n]$ est une base de Gröbner de I_l
2. Remontée des solutions de $V(I_l)$ à $V(I_{l-1})$:

Théorème d'extension

Soit la projection

$$\begin{array}{rccc} \pi_l : & K^{n-l+1} & \rightarrow & K^{n-l} \\ & (x_l, \ldots, x_n) & \rightarrow & (x_{l+1}, \ldots, x_n) \end{array}$$

alors

$$U \subset \pi_l\left(V(I_{l-1})\right) \subset V(I_l)$$

où U est un ouvert dense de $V(I_l)$.

Exemple

Résoudre le système suivant

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

Exemple

Résoudre le système suivant

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

1. Base de Gröbner pour $lex_{x>y>z}$:

$$G = \left\{ \begin{array}{l} g_1 = x + y + z^2 - 1 \\ g_2 = y^2 - y - z^2 + z \\ g_3 = 2yz^2 + z^4 - z^2 \\ g_4 = z^6 - 4z^4 + 4z^3 - z^2 \end{array} \right\}$$

Exemple

Résoudre le système suivant

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

1. Base de Gröbner pour $lex_{x>y>z}$:

$$G = \left\{ \begin{array}{l} g_1 = x + y + z^2 - 1 \\ g_2 = y^2 - y - z^2 + z \\ g_3 = 2yz^2 + z^4 - z^2 \\ g_4 = z^6 - 4z^4 + 4z^3 - z^2 \end{array} \right\}$$

2. Théorème d'extension :
   - $I_2 = I \cap K[z] = \langle g_4 = z^2(z-1)^2(z^2+2z-1) \rangle$
     $V(I_2) = \{0, 1, -1 \pm \sqrt{2}\}$

2. Théorème d'extension :
   - $I_2 = I \cap \mathbb{R}[z] = \langle z^2(z-1)^2(z^2+2z-1) \rangle$
     $V(I_2) = \{0, 1, -1 \pm \sqrt{2}\}$

2. Théorème d'extension :
   - $I_2 = I \cap \mathbb{R}[z] = \langle z^2(z-1)^2(z^2+2z-1) \rangle$
     $V(I_2) = \{0, 1, -1 \pm \sqrt{2}\}$
   - $I_1 = I \cap \mathbb{R}[y,z] = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^2(z-1)^2(z^2+2z-1) \rangle$
     $z = 0 \Rightarrow y = 0$ ou $y = 1$
     $z = 1 \Rightarrow y = 0$
     $z = -1 + \sqrt{2} \Rightarrow y = -1 + \sqrt{2}$
     $z = -1 - \sqrt{2} \Rightarrow y = -1 - \sqrt{2}$
     $V(I_1) = \{(0,0), (0,1), (-1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2})\}$

2. Théorème d'extension :
   - $I_2 = I \cap \mathbb{R}[z] = \langle z^2(z-1)^2(z^2+2z-1) \rangle$
     $V(I_2) = \{0, 1, -1 \pm \sqrt{2}\}$
   - $I_1 = I \cap \mathbb{R}[y,z] = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^2(z-1)^2(z^2+2z-1) \rangle$
     $z = 0 \Rightarrow y = 0$ ou $y = 1$
     $z = 1 \Rightarrow y = 0$
     $z = -1 + \sqrt{2} \Rightarrow y = -1 + \sqrt{2}$
     $z = -1 - \sqrt{2} \Rightarrow y = -1 - \sqrt{2}$
     $V(I_1) = \{(0,0), (0,1), (-1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2})\}$
   - $y = z = 0 \Rightarrow x = 1$
     $y = 1, z = 0 \Rightarrow x = 0$
     $y = 0, z = 1 \Rightarrow x = 0$
     $y = z = -1 + \sqrt{2} \Rightarrow x = -1 + \sqrt{2}$
     $y = z = -1 - \sqrt{2} \Rightarrow x = -1 - \sqrt{2}$

2. Théorème d'extension :
   - $I_2 = I \cap \mathbb{R}[z] = \langle z^2(z-1)^2(z^2+2z-1) \rangle$
     $V(I_2) = \{0, 1, -1 \pm \sqrt{2}\}$
   - $I_1 = I \cap \mathbb{R}[y,z] = \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^2(z-1)^2(z^2+2z-1) \rangle$
     $z = 0 \Rightarrow y = 0$ ou $y = 1$
     $z = 1 \Rightarrow y = 0$
     $z = -1 + \sqrt{2} \Rightarrow y = -1 + \sqrt{2}$
     $z = -1 - \sqrt{2} \Rightarrow y = -1 - \sqrt{2}$
     $V(I_1) = \{(0,0), (0,1), (-1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2})\}$
   - $y = z = 0 \Rightarrow x = 1$
     $y = 1, z = 0 \Rightarrow x = 0$
     $y = 0, z = 1 \Rightarrow x = 0$
     $y = z = -1 + \sqrt{2} \Rightarrow x = -1 + \sqrt{2}$
     $y = z = -1 - \sqrt{2} \Rightarrow x = -1 - \sqrt{2}$
3. Solutions :

$$V(I) = \{(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})\}$$

Cas particulier de la dimension 0

Contexte de l'exemple et prochain exposé

$$\dim_K V(I) = 0 \Leftrightarrow V(I) = \{a_1, \ldots, a_k\}$$

En particulier,

$$\pi_l\left(V(I_{l-1})\right) = \overline{\pi_l\left(V(I_{l-1})\right)} = V(I_l)$$

$\Rightarrow$ la remontée ne pose pas de problème

Cas particulier de la dimension 0

Contexte de l'exemple et prochain exposé

$$\dim_{\overline{K}} V(I) = 0 \Leftrightarrow V(I) = \{a_1, \ldots, a_k\}$$

En particulier,

$$\pi_l\left(V(I_{l-1})\right) = \overline{\pi_l\left(V(I_{l-1})\right)} = V(I_l)$$

$\Rightarrow$ la remontée ne pose pas de problème

Problème en pratique

- Le calcul de bases de Gröbner pour l'ordre $lex_{X_1>\ldots>X_n}$ est très coûteux...
- Changement d'ordre possible en dimension 0 avec l'algorithme FGLM

Algorithmes de calcul des BG

Soit $I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots X_n]$.

Théorème de Buchberger

- On définit le **S-polynôme** de $f, g \in K[X_1, \ldots X_n]$ par :

$$S(f,g) = \frac{\gamma}{\mathrm{lt}(f)} f - \frac{\gamma}{\mathrm{lt}(g)} g \quad \text{où} \quad \gamma = \mathrm{lm}(f) \vee \mathrm{lm}(g).$$

Algorithmes de calcul des BG

Soit $I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots X_n]$.

Théorème de Buchberger

- On définit le **S-polynôme** de $f, g \in K[X_1, \ldots X_n]$ par :
$$S(f,g) = \frac{\gamma}{\mathrm{lt}(f)} f - \frac{\gamma}{\mathrm{lt}(g)} g \quad \text{où} \quad \gamma = \mathrm{lm}(f) \vee \mathrm{lm}(g).$$
- $G = \{g_1, \ldots, g_s\}$ est une base de Gröbner (pour un ordre donné) de I si (et seulement si)
$$\forall i, j, \quad \overline{S(g_i, g_j)}^{G} = 0.$$

Algorithmes de calcul des BG

Soit $I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots X_n]$.

Théorème de Buchberger

- On définit le **S-polynôme** de $f, g \in K[X_1, \ldots X_n]$ par :
$$S(f,g) = \frac{\gamma}{\mathrm{lt}(f)} f - \frac{\gamma}{\mathrm{lt}(g)} g \quad \text{où} \quad \gamma = \mathrm{lm}(f) \vee \mathrm{lm}(g).$$
- $G = \{g_1, \ldots, g_s\}$ est une base de Gröbner (pour un ordre donné) de I si (et seulement si)
$$\forall i, j, \quad \overline{S(g_i, g_j)}^{G} = 0.$$
- Mieux : G est une base de Gröbner de I si (et seulement si)
$$\forall i, j, \quad S(g_i, g_j) = o_G(\mathrm{lm}(g_i) \vee \mathrm{lm}(g_j))$$

où $p = o_G(m)$ si $\exists u_1, \ldots, u_s \in K[X_1, \ldots X_n]$ tq $\begin{cases} p = \sum u_i g_i \\ \mathrm{lm}(u_i g_i) < m \end{cases}$

Algorithme de Buchberger

ENTRÉE : $I = \langle f_1, \ldots, f_k \rangle$
SORTIE : G base de Gröbner de I

1. $G \leftarrow \{f_1, \ldots, f_k\}$
2. $CP \leftarrow \{S(f_i, f_j), 1 \leq i < j \leq k\}$
3. **tant que** $CP \neq \emptyset$ **faire**
4. choisir $s \in CP$
5. $r \leftarrow \overline{s}^G$
6. **si** $r \neq 0$ **alors**
7. $CP \leftarrow CP \cup \{S(g, r) : g \in G\}$
8. $G \leftarrow G \cup \{r\}$
9. **fin si**
10. **fin tant que**
11. **retourner** G

Analyse et améliorations de l'algorithme de Buchberger

Analyse de l'algorithme

- Invariant de boucle : $I = \langle G \rangle$
- Terminaison : à chaque passage de boucle, soit $\langle \mathrm{LT}(G) \rangle$ croît strictement, soit $\#CP$ décroît ; $K[X_1, \ldots X_n]$ noethérien $\Rightarrow$ l'algorithme s'arrête
- A la fin : on a bien une base de Gröbner puisque tous les S-polynômes se réduisent à 0 dans G

Analyse et améliorations de l'algorithme de Buchberger

Analyse de l'algorithme

- Invariant de boucle : $I = \langle G \rangle$
- Terminaison : à chaque passage de boucle, soit $\langle \mathrm{LT}(G) \rangle$ croît strictement, soit $\#CP$ décroît ; $K[X_1, \ldots X_n]$ noethérien $\Rightarrow$ l'algorithme s'arrête
- A la fin : on a bien une base de Gröbner puisque tous les S-polynômes se réduisent à 0 dans G

Amélioration 1 : "purge" de la base

- **base minimale :** $\forall g, g' \in G, \mathrm{lt}(g) \nmid \mathrm{lt}(g')$
  $\longrightarrow$ avant ajout de r à G, éliminer les $g \in G$ tq $\mathrm{lt}(r) | \mathrm{lt}(g)$
  $\Rightarrow$ unicité du nombre de générateurs
- **base réduite :** $\forall g, g' \in G$, $\forall t$ terme de g, $\mathrm{lt}(g') \nmid t \longrightarrow$ réduire également les "queues" des polynômes de la base $\Rightarrow$ unicité de la base

Autres améliorations

- temps de calcul concentré sur les réductions des S-polynômes $\Rightarrow$ diminuer le nombre de paires considérées
- stratégie de choix des paires : difficile de trouver a priori l'approche optimale $\longrightarrow$ on considère les paires par degré du lcm croissant.
- critères de Buchberger pour détecter a priori certaines paires se réduisant à 0

Autres améliorations

- temps de calcul concentré sur les réductions des S-polynômes $\Rightarrow$ diminuer le nombre de paires considérées
- stratégie de choix des paires : difficile de trouver a priori l'approche optimale $\longrightarrow$ on considère les paires par degré du lcm croissant.
- critères de Buchberger pour détecter a priori certaines paires se réduisant à 0

Critères de Buchberger

1. **Critère 1 :**

$$\mathrm{lm}(f) \wedge \mathrm{lm}(g) = 1 \Rightarrow \overline{S(f,g)}^{\{f,g\}} = 0$$

2. **Critère 2 :**
Si $f, g, h \in G$ sont tels que $\mathrm{lm}(f) | (\mathrm{lm}(g) \vee \mathrm{lm}(h))$ et si $S(f,g) = o_G(\mathrm{lm}(f) \vee \mathrm{lm}(g))$ et $S(f,h) = o_G(\mathrm{lm}(f) \vee \mathrm{lm}(h))$, alors

$$S(g,h) = o_G(\mathrm{lm}(g) \vee \mathrm{lm}(h))$$

Algorithme F4 de Faugère

Idées principales

1. utiliser l'algèbre linéaire pour faire les réductions de plusieurs paires critiques simultanément et obtenir une base minimale réduite
   - construction de la matrice (par lcm décroissant) :

     colonnes de la matrice $\leftrightarrow$ monômes
     lignes de la matrice $\leftrightarrow$ polynômes des paires critiques + ceux utiles pour réduction complète
   - pivot de Gauss pour obtenir une forme échelon

Algorithme F4 de Faugère

Idées principales

1. utiliser l'algèbre linéaire pour faire les réductions de plusieurs paires critiques simultanément et obtenir une base minimale réduite
   - construction de la matrice (par lcm décroissant) :

     colonnes de la matrice $\leftrightarrow$ monômes
     lignes de la matrice $\leftrightarrow$ polynômes des paires critiques + ceux utiles pour réduction complète
   - pivot de Gauss pour obtenir une forme échelon

2. lignes avec nouveaux termes de tête $\longrightarrow$ à ajouter dans la base

Algorithme F4 de Faugère

Idées principales

1. utiliser l'algèbre linéaire pour faire les réductions de plusieurs paires critiques simultanément et obtenir une base minimale réduite
   - construction de la matrice (par lcm décroissant) :

     colonnes de la matrice $\leftrightarrow$ monômes
     lignes de la matrice $\leftrightarrow$ polynômes des paires critiques + ceux utiles pour réduction complète
   - pivot de Gauss pour obtenir une forme échelon
2. lignes avec nouveaux termes de tête $\longrightarrow$ à ajouter dans la base
3. autres lignes à mémoriser car réutilisables dans les prochains calculs

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$$f_1 = x + 2y + 2z - 1$$
$$f_2 = xy + yz + 3y$$
$$f_3 = x^2 + 2y^2 + 2z^2 - x$$

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

$CP \leftarrow \{[S(f_1, f_2), xy]\}$

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$f_2 = xy + yz + 3y \leftarrow$ purgé par f_1

$f_3 = x^2 + 2y^2 + 2z^2 - x$

$CP \leftarrow \{[S(f_1, f_2), xy]\}$

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$f_3 = x^2 + 2y^2 + 2z^2 - x$

$CP \leftarrow \{[S(f_1, f_2), xy], [S(f_1, f_3), x^2]\}$

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$f_3 = x^2 + 2y^2 + 2z^2 - x \leftarrow$ purgé par f_1

$CP \leftarrow \{[S(f_1, f_2), xy], [S(f_1, f_3), x^2]\}$

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{[S(f_1, f_2), xy], [S(f_1, f_3), x^2]\}$ $\quad$ $G \leftarrow \{f_1\}$

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{[S(f_1, f_2), xy], \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	z^2	x
xf_1	1	2	0	2	0	6
f_3	1	0	2	0	2	6

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y
xf_1	1	2	0	2	0	0	6	0
f_3	1	0	2	0	0	2	6	0
yf_1	0	1	2	0	2	0	0	6
f_2	0	1	0	0	1	0	0	3

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y
xf_1	1	2	0	2	0	0	6	0
f_3	1	0	2	0	0	2	6	0
yf_1	0	1	2	0	2	0	0	6
f_2	0	1	0	0	1	0	0	3

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y	z
xf_1	1	2	0	2	0	0	6	0	0
f_3	1	0	2	0	0	2	6	0	0
yf_1	0	1	2	0	2	0	0	6	0
f_2	0	1	0	0	1	0	0	3	0
zf_1	0	0	0	1	2	2	0	0	6

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y	z
xf_1	1	2	0	2	0	0	6	0	0
f_3	1	0	2	0	0	2	6	0	0
yf_1	0	1	2	0	2	0	0	6	0
f_2	0	1	0	0	1	0	0	3	0
zf_1	0	0	0	1	2	2	0	0	6

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y	z	1
xf_1	1	2	0	2	0	0	6	0	0	0
f_3	1	0	2	0	0	2	6	0	0	0
yf_1	0	1	2	0	2	0	0	6	0	0
f_2	0	1	0	0	1	0	0	3	0	0
zf_1	0	0	0	1	2	2	0	0	6	0
f_1	0	0	0	0	0	0	1	2	2	6

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y	z	1
	1	0	0	0	0	6	0	1	3	6
	0	1	0	0	0	3	0	1	6	0
	0	0	1	0	0	5	0	4	3	0
(*Gauss*)	0	0	0	1	0	1	0	3	4	0
	0	0	0	0	1	4	0	2	1	0
	0	0	0	0	0	0	1	2	2	6

Illustration par l'exemple de F4

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$

$CP \leftarrow \{\cancel{[S(f_1, f_2), xy]}, \cancel{[S(f_1, f_3), x^2]}\}$ $\qquad$ $G \leftarrow \{f_1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y	z	1
	1	0	0	0	0	6	0	1	3	6
	0	1	0	0	0	3	0	1	6	0
$\rightarrow$	0	0	1	0	0	5	0	4	3	0
	0	0	0	1	0	1	0	3	4	0
$\rightarrow$	0	0	0	0	1	4	0	2	1	0
	0	0	0	0	0	0	1	2	2	6

Katsura 3 par F4 (suite)

$CP \leftarrow \emptyset$ $\quad$ $G \leftarrow \{f_1 = x + 2y + 2z - 1\}$

	x^2	xy	y^2	xz	yz	z^2	x	y	z	1
	1	0	0	0	0	6	0	1	3	6
	0	1	0	0	0	3	0	1	6	0
$\rightarrow$	0	0	1	0	0	5	0	4	3	0
	0	0	0	1	0	1	0	3	4	0
$\rightarrow$	0	0	0	0	1	4	0	2	1	0
	0	0	0	0	0	0	1	2	2	6

nouveaux générateurs

$f_4 = y^2 + 5z^2 + 4y + 3z$

$f_5 = yz + 4z^2 + 2y + z$

calculs à mémoriser

$xf_1 \xrightarrow[G]{} x^2 + 6z^2 + y + 3z + 6$

$yf_1 \xrightarrow[G]{} xy + 3z^2 + y + 6z$

$zf_1 \xrightarrow[G]{} xz + z^2 + 3y + 4z$

Katsura 3 par F4 (suite)

$CP \leftarrow \emptyset \qquad G \leftarrow \{f_1 = x + 2y + 2z - 1\}$

nouveaux générateurs	calculs à mémoriser
$f_4 = y^2 + 5z^2 + 4y + 3z$	$xf_1 \xrightarrow[G]{} x^2 + 6z^2 + y + 3z + 6$
$f_5 = yz + 4z^2 + 2y + z$	$yf_1 \xrightarrow[G]{} xy + 3z^2 + y + 6z$
	$zf_1 \xrightarrow[G]{} xz + z^2 + 3y + 4z$

Paires à considérer :

- $S(f_4, f_1), xy^2$
- $S(f_5, f_1), xyz$
- $S(f_5, f_4), y^2z$

Katsura 3 par F4 (suite)

$CP \leftarrow \emptyset \qquad G \leftarrow \{f_1 = x + 2y + 2z - 1\}$

nouveaux générateurs	calculs à mémoriser
$f_4 = y^2 + 5z^2 + 4y + 3z$	$xf_1 \xrightarrow[G]{} x^2 + 6z^2 + y + 3z + 6$
$f_5 = yz + 4z^2 + 2y + z$	$yf_1 \xrightarrow[G]{} xy + 3z^2 + y + 6z$
	$zf_1 \xrightarrow[G]{} xz + z^2 + 3y + 4z$

Paires à considérer :

- ~~$S(f_4, f_1), xy^2$~~ (critère 1)
- ~~$S(f_5, f_1), xyz$~~ (critère 1)
- $S(f_5, f_4), y^2z \rightarrow$ critère 2 ne s'applique pas

Katsura 3 par F4 (suite)

$CP \leftarrow \{S(f_5, f_4), y^2z\}$

$G \leftarrow \{f_1 = x+2y+2z-1, f_4 = y^2+5z^2+4y+3z, f_5 = yz+4z^2+2y+z\}$

On retient que :

$xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$

$yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$

$zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$

	y^2z	yz^2	z^3	y^2	yz	z^2
zf_4	1	0	5	0	4	3
yf_5	1	4	0	2	1	0

Katsura 3 par F4 (suite)

$CP \leftarrow \{S(f_5, f_4), y^2z\}$

$G \leftarrow \{f_1 = x+2y+2z-1, f_4 = y^2+5z^2+4y+3z, f_5 = yz+4z^2+2y+z\}$

On retient que :

$xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$

$yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$

$zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$

	y^2z	yz^2	z^3	y^2	yz	z^2
zf_4	1	0	5	0	4	3
yf_5	1	4	0	2	1	0

Katsura 3 par F4 (suite)

$CP \leftarrow \{S(f_5, f_4), y^2z\}$

$G \leftarrow \{f_1 = x+2y+2z-1, f_4 = y^2+5z^2+4y+3z, f_5 = yz+4z^2+2y+z\}$

On retient que :

$xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$

$yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$

$zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$

	y^2z	yz^2	z^3	y^2	yz	z^2	y	z
zf_4	1	0	5	0	4	3	0	0
yf_5	1	4	0	2	1	0	0	0
zf_5	0	1	4	0	2	1	0	0
f_4	0	0	0	1	0	5	4	3
f_5	0	0	0	0	1	4	2	1

Katsura 3 par F4 (suite)

$CP \leftarrow \{S(f_5, f_4), y^2z\}$

$G \leftarrow \{f_1 = x+2y+2z-1, f_4 = y^2+5z^2+4y+3z, f_5 = yz+4z^2+2y+z\}$

On retient que :

$xf_1 \longrightarrow_G x^2+6z^2+y+3z+6$

$yf_1 \longrightarrow_G xy+3z^2+y+6z$

$zf_1 \longrightarrow_G xz+z^2+3y+4z$

	y^2z	yz^2	z^3	y^2	yz	z^2	y	z
	1	0	5	0	0	0	6	1
(*Gauss*)	0	1	4	0	0	0	3	5
	0	0	0	1	0	0	4	0
	0	0	0	0	1	0	2	0
	0	0	0	0	0	1	0	2

Katsura 3 par F4 (suite)

$CP \leftarrow \{S(f_5, f_4), y^2z\}$

$G \leftarrow \{f_1 = x+2y+2z-1, f_4 = y^2+5z^2+4y+3z, f_5 = yz+4z^2+2y+z\}$

On retient que :

$xf_1 \longrightarrow_G x^2+6z^2+y+3z+6$

$yf_1 \longrightarrow_G xy+3z^2+y+6z$

$zf_1 \longrightarrow_G xz+z^2+3y+4z$

	y^2z	yz^2	z^3	y^2	yz	z^2	y	z
	1	0	5	0	0	0	6	1
	0	1	4	0	0	0	3	5
	0	0	0	1	0	0	4	0
	0	0	0	0	1	0	2	0
$\rightarrow$	0	0	0	0	0	1	0	2

Nouveau générateur :

$$f_6 = z^2+2z$$

Katsura 3 par F4 (suite)

$CP \leftarrow \emptyset$

$G \leftarrow \{f_1 = x+2y+2z-1, f_4 = y^2+5z^2+4y+3z, f_5 = yz+4z^2+2y+z\}$

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2+6z^2+y+3z+6$
  - $yf_1 \longrightarrow_G xy+3z^2+y+6z$
  - $zf_1 \longrightarrow_G xz+z^2+3y+4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z+5z^3+6y+z$
  - $zf_5 \longrightarrow_G yz^2+4z^3+3y+5z$
  - $f_4 \longrightarrow_G y^2+4y$
  - $f_5 \longrightarrow_G yz+2y$

- Nouveau générateur :
  - $f_6 = z^2+2z$
- Paires à considérer :
  - $S(f_6, f_1), xz^2$
  - $S(f_6, f_4), y^2z^2$
  - $S(f_6, f_5), yz^2$

Katsura 3 par F4 (suite)

$CP \leftarrow \emptyset$

$G \leftarrow \{f_1 = x + 2y + 2z - 1, f_4 = y^2 + 4y, f_5 = yz + 2y\}$

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- Nouveau générateur :
  - $f_6 = z^2 + 2z$
- Paires à considérer :
  - $S(f_6, f_1), xz^2$
  - $S(f_6, f_4), y^2z^2$
  - $S(f_6, f_5), yz^2$

Katsura 3 par F4 (suite)

$CP \leftarrow \emptyset$

$G \leftarrow \{f_1 = x + 2y + 2z - 1, f_4 = y^2 + 4y, f_5 = yz + 2y\}$

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- Nouveau générateur :
  - $f_6 = z^2 + 2z$
- Paires à considérer :
  - ~~$S(f_6, f_1), xz^2$~~ (critère 1)
  - ~~$S(f_6, f_4), y^2z^2$~~ (critère 1)
  - $S(f_6, f_5), yz^2 \rightarrow$ pas de critère 2

Katsura 3 par F4 (suite)

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- $CP \leftarrow \{S(f_6, f_5), yz^2\}$
- $G \leftarrow \{f_1 = x + 2y + 2z - 1,$
  $f_4 = y^2 + 4y,$
  $f_5 = yz + 2y,$
  $f_6 = z^2 + 2z\}$

	yz^2	z^3	yz	z^2	y	z
zf_5	1	4	0	0	3	5
yf_6	1	0	2	0	0	0

Katsura 3 par F4 (suite)

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- $CP \leftarrow \{S(f_6, f_5), yz^2\}$
- $G \leftarrow \{f_1 = x + 2y + 2z - 1,$
  $f_4 = y^2 + 4y,$
  $f_5 = yz + 2y,$
  $f_6 = z^2 + 2z\}$

	yz^2	z^3	yz	z^2	y	z
zf_5	1	4	0	0	3	5
yf_6	1	0	2	0	0	0

Katsura 3 par F4 (suite)

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- $CP \leftarrow \{S(f_6, f_5), yz^2\}$
- $G \leftarrow \{f_1 = x + 2y + 2z - 1,$
  $f_4 = y^2 + 4y,$
  $f_5 = yz + 2y,$
  $f_6 = z^2 + 2z\}$

	yz^2	z^3	yz	z^2	y	z
zf_5	1	4	0	0	3	5
yf_6	1	0	2	0	0	0
zf_6	0	1	0	2	0	0
f_5	0	0	1	0	2	0
f_6	0	0	0	1	0	2

Katsura 3 par F4 (suite)

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- $CP \leftarrow \{S(f_6, f_5), yz^2\}$
- $G \leftarrow \{f_1 = x + 2y + 2z - 1,$
  $f_4 = y^2 + 4y,$
  $f_5 = yz + 2y,$
  $f_6 = z^2 + 2z\}$

$$
\begin{array}{c|cccccc}
 & yz^2 & z^3 & yz & z^2 & y & z \\
 & 1 & 0 & 0 & 0 & 3 & 0 \\
 & 0 & 0 & 0 & 0 & 0 & 0 \\
(Gauss) & 0 & 1 & 0 & 0 & 0 & 3 \\
 & 0 & 0 & 1 & 0 & 2 & 0 \\
 & 0 & 0 & 0 & 1 & 0 & 2
\end{array}
$$

Katsura 3 par F4 (suite)

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- $CP \leftarrow \{S(f_6, f_5), yz^2\}$
- $G \leftarrow \{f_1 = x + 2y + 2z - 1,$
  $f_4 = y^2 + 4y,$
  $f_5 = yz + 2y,$
  $f_6 = z^2 + 2z\}$

	yz^2	z^3	yz	z^2	y	z
	1	0	0	0	3	0
$\rightarrow$	0	0	0	0	0	0
	0	1	0	0	0	3
	0	0	1	0	2	0
	0	0	0	1	0	2

Katsura 3 par F4 (suite)

- Calculs à mémoriser :
  - $xf_1 \longrightarrow_G x^2 + 6z^2 + y + 3z + 6$
  - $yf_1 \longrightarrow_G xy + 3z^2 + y + 6z$
  - $zf_1 \longrightarrow_G xz + z^2 + 3y + 4z$
  - $zf_4, yf_5 \longrightarrow_G y^2z + 5z^3 + 6y + z$
  - $zf_5 \longrightarrow_G yz^2 + 4z^3 + 3y + 5z$

- $CP \leftarrow \{S(f_6, f_5), yz^2\}$
- $G \leftarrow \{f_1 = x + 2y + 2z - 1,$
  $f_4 = y^2 + 4y,$
  $f_5 = yz + 2y,$
  $f_6 = z^2 + 2z\}$

yz^2	z^3	yz	z^2	y	z
1	0	0	0	3	0
0	0	0	0	0	0
0	1	0	0	0	3
0	0	1	0	2	0
0	0	0	1	0	2

$$G = \{x + 2y + 2z - 1,\ y^2 + 4y,\ yz + 2y,\ z^2 + 2z\}$$

Algorithme F5 de Faugère

Rappel sur l'algorithme de Buchberger

Si $G = \{g_1, \ldots, g_s\}$ générateurs de I tels que

$$\forall i, j,\ S(g_i, g_j) = o_G(lm(g_i) \vee \mathrm{lm}(g_j))$$

Alors G est une base de Gröbner

- En pratique, dans l'algorithme de Buchberger beaucoup de paires critiques se réduisent à 0 (malgré les critères 1 et 2 vus précédemment).
- But de F5 : éliminer a priori ces paires

Comprendre le critère F5 avec les matrices de Macaulay

$I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots X_n]$

Matrice de Macaulay de degré d

colonnes de la matrice	$\leftrightarrow$	monômes
lignes de la matrice	$\leftrightarrow$	mf_i, $\deg(mf_i) \leq d$

Comprendre le critère F5 avec les matrices de Macaulay

$I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots X_n]$

Matrice de Macaulay de degré d

colonnes de la matrice $\leftrightarrow$ monômes

lignes de la matrice $\leftrightarrow$ mf_i, $\deg(mf_i) \leq d$

Résultat de Lazard

Pour d suffisamment grand, la matrice de Macaulay triangularisée correspondante contient une BG de I.

Comprendre le critère F5 avec les matrices de Macaulay

$I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots X_n]$

Matrice de Macaulay de degré d

colonnes de la matrice $\leftrightarrow$ monômes
lignes de la matrice $\leftrightarrow$ mf_i, $\deg(mf_i) \leq d$

Résultat de Lazard

Pour d suffisamment grand, la matrice de Macaulay triangularisée correspondante contient une BG de I.

Lignes inutiles dans Macaulay ?

- **Critère F5 :** si $m \in \mathrm{LT}(\langle f_1, \ldots, f_{i-1} \rangle)$, alors mf_i est une combinaison linéaire des lignes antérieures, i.e. de la forme $m' f_j$ où $j < i$ ou $j = i$ et $m' < m$.
- Algorithme incrémental : calculer une base de Gröbner de $\langle f_1, \ldots, f_{i-1} \rangle$ pour vérifier facilement le critère F5 pour m

Formalisme de F5

$I = \langle f_1, \ldots, f_k \rangle$ idéal de $K[X_1, \ldots, X_n]$

- **polynôme étiqueté** : $[s, p]$ où $p \in K[X_1, \ldots, X_n]$ et la **signature** $s = (m, f_i)$ est la donnée d'un monôme et d'un générateur initial de I

Formalisme de F5

$I = \langle f_1, \ldots, f_k \rangle$ idéal de $K[X_1, \ldots, X_n]$

- **polynôme étiqueté** : $[s, p]$ où $p \in K[X_1, \ldots, X_n]$ et la **signature** $s = (m, f_i)$ est la donnée d'un monôme et d'un générateur initial de I
- **polynôme étiqueté admissible** : $[(m, f_i), p]$ tel que

$$\exists u_1, \ldots u_i, \ p = \sum_{j=1}^{i} u_j f_j \text{ où } \mathrm{lm}(u_i) = m$$

$\longrightarrow$ dans la suite tous les polynômes étiquetés seront admissibles

Formalisme de F5

$I = \langle f_1, \ldots, f_k \rangle$ idéal de $K[X_1, \ldots, X_n]$

- **polynôme étiqueté** : $[s, p]$ où $p \in K[X_1, \ldots, X_n]$ et la **signature** $s = (m, f_i)$ est la donnée d'un monôme et d'un générateur initial de I
- **polynôme étiqueté admissible** : $[(m, f_i), p]$ tel que

$$\exists u_1, \ldots u_i, \ p = \sum_{j=1}^{i} u_j f_j \text{ où } \mathrm{lm}(u_i) = m$$

$\longrightarrow$ dans la suite tous les polynômes étiquetés seront admissibles

- **polynôme étiqueté normalisé** : $[(m, f_i), p]$ tel que $m \notin \mathrm{LT}(\langle f_1, \ldots, f_{i-1} \rangle)$

Formalisme de F5

$I = \langle f_1, \ldots, f_k \rangle$ idéal de $K[X_1, \ldots, X_n]$

- **polynôme étiqueté** : $[s, p]$ où $p \in K[X_1, \ldots, X_n]$ et la **signature** $s = (m, f_i)$ est la donnée d'un monôme et d'un générateur initial de I
- **polynôme étiqueté admissible** : $[(m, f_i), p]$ tel que

$$\exists u_1, \ldots u_i, \ p = \sum_{j=1}^{i} u_j f_j \text{ où } \mathrm{lm}(u_i) = m$$

$\longrightarrow$ dans la suite tous les polynômes étiquetés seront admissibles

- **polynôme étiqueté normalisé** : $[(m, f_i), p]$ tel que $m \notin \mathrm{LT}(\langle f_1, \ldots, f_{i-1} \rangle)$
- **paire critique normalisée** : $CP([s_1, p_1], [s_2, p_2])$ telle que
  - $[(u_1 m_1, f_{i_1}), u_1 p_1]$ et $[(u_2 m_2, f_{i_2}), u_2 p_2]$ sont normalisées, avec $u_i = \mathrm{lm}(p_i)^{-1}(\mathrm{lm}(p_1) \vee \mathrm{lm}(p_2))$
  - $s_1 = (u_1 m_1, f_{i_1}) > s_2 = (u_2 m_2, f_{i_2}) \Leftrightarrow \begin{cases} i_1 > i_2 \text{ ou} \\ i_1 = i_2 \text{ et } u_1 m_1 > u_2 m_2 \end{cases}$

Généralisation de la notion de o

Définition

Soient $G = \{(s_1, p_1), \ldots, (s_k, p_k)\}$ et $r = (s_r, p_r)$, $t = (s_t, p_t)$ des polynômes étiquetés.

- $r = O_G(t)$ si $\exists u_1, \ldots, u_k$ tq $\begin{cases} p_r = \sum u_i p_i \\ \mathrm{lm}(u_i p_i) \leq \mathrm{lm}(p_t) \\ \mathrm{lm}(u_i) s_i \leq s_r \end{cases}$

Généralisation de la notion de o

Définition

Soient $G = \{(s_1, p_1), \ldots, (s_k, p_k)\}$ et $r = (s_r, p_r)$, $t = (s_t, p_t)$ des polynômes étiquetés.

- $r = O_G(t)$ si $\exists u_1, \ldots, u_k$ tq $\begin{cases} p_r = \sum u_i p_i \\ \mathrm{lm}(u_i p_i) \leq \mathrm{lm}(p_t) \\ \mathrm{lm}(u_i) s_i \leq s_r \end{cases}$
- $r = o_G(t)$ si $\exists t' = (s_{t'}, p_{t'})$ admissible tq $\begin{cases} s_{t'} \leq s_t \\ \mathrm{lm}(t') < \mathrm{lm}(t) \\ r = O_G(t') \end{cases}$

Algorithme F5

$I = \langle f_1, \ldots, f_k \rangle \subset K[X_1, \ldots, X_n]$

Théorème (Faugère)

Soit $G = \{r_1, \ldots, r_s\}$ une famille de polynômes étiquetés $(r_i = (s_i, g_i))$ telle que

1. $[(1, f_i), f_i] \in G$ pour tout $i = 1, \ldots, k$
2. r_i admissibles
3. $\forall i, j,\ 1 \leq i, j \leq s$ tels que $CP(r_i, r_j)$ normalisée, on a

$$S(r_i, r_j) := [u_i s_i, u_i g_i - u_j g_j] = o_G(u_i r_i) \text{ où } u_{i,j} = \frac{\mathrm{lm}(g_i) \vee \mathrm{lm}(g_j)}{\mathrm{lm}(g_{i,j})}$$

alors $(g_1, \ldots, g_s)$ est une base de Gröbner.

Algorithme F5

F5 en résumé...

- c'est un algorithme incrémental : on passe du calcul d'une BG de $\{f_1, \ldots, f_i\}$ (step i) à celui de $\{f_1, \ldots, f_{i+1}\}$ (step $i+1$)
- on reprend la trame de l'algorithme de Buchberger en ne considérant que les paires normalisées
- lors de la réduction d'un S-polynôme $S([s_1, p_1], [s_2, p_2])$ par $G = \{[s_1, g_1], \ldots, [s_l, g_l]\}$, on veut que le reste r ait une signature admissible s et que l'écriture donnée par la réduction $u_1 p_1 - u_2 p_2 = \sum h_i g_i + r$ garantisse que

$$S([s_1, p_1], [s_2, p_2]) = o_{G \cup \{[s,r]\}}(u_1 r_1)$$

$\rightarrow$ on ne peut réduire que par des polynômes étiquetés ayant des signatures strictement plus petites

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

1. **Step 1 :** $G_1 = \{r_1 := [(1, f_1), f_1]\}$, $\langle \mathrm{LT}(G_1) \rangle = \langle x \rangle$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

1. **Step 1 :** $G_1 = \{r_1 := [(1, f_1), f_1]\}$, $\langle LT(G_1)\rangle = \langle x\rangle$
2. **Step 2 :** $G_2 \leftarrow \{r_1 = [(1, f_1), f_1], r_2 := [(1, f_2), f_2]\}$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

1. **Step 1 :** $G_1 = \{r_1 := [(1, f_1), f_1]\}$, $\langle LT(G_1)\rangle = \langle x\rangle$
2. **Step 2 :** $G_2 \leftarrow \{r_1 = [(1, f_1), f_1], r_2 := [(1, f_2), f_2]\}$
   - paire à considérer :
     $S(r_2, r_1) = 1.r_2 - yr_1 \rightarrow (1, f_2) \notin LT(G_1) \Rightarrow S(r_2, r_1)$ normalisée
     $\Rightarrow CP \leftarrow \{S(r_2, r_1)\}$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

1. **Step 1 :** $G_1 = \{r_1 := [(1, f_1), f_1]\}$, $\langle LT(G_1)\rangle = \langle x\rangle$
2. **Step 2 :** $G_2 \leftarrow \{r_1 = [(1, f_1), f_1], r_2 := [(1, f_2), f_2]\}$
   - paire à considérer :
     $S(r_2, r_1) = 1.r_2 - yr_1 \rightarrow (1, f_2) \notin LT(G_1) \Rightarrow S(r_2, r_1)$ normalisée
     $\Rightarrow CP \leftarrow \{S(r_2, r_1)\}$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_3 := [(1, f_2), y^2 + 4yz + 5y]$ et $CP \leftarrow \emptyset$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

1. **Step 1 :** $G_1 = \{r_1 := [(1, f_1), f_1]\}$, $\langle LT(G_1)\rangle = \langle x\rangle$
2. **Step 2 :** $G_2 \leftarrow \{r_1 = [(1, f_1), f_1], r_2 := [(1, f_2), f_2]\}$
   - paire à considérer :
     $S(r_2, r_1) = 1.r_2 - yr_1 \rightarrow (1, f_2) \notin LT(G_1) \Rightarrow S(r_2, r_1)$ normalisée
     $\Rightarrow CP \leftarrow \{S(r_2, r_1)\}$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_3 := [(1, f_2), y^2 + 4yz + 5y]$ et $CP \leftarrow \emptyset$
   - paires à considérer :
     $S(r_3, r_1) = xr_3 - y^2 r_1 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_3, r_1)$ éliminée
     $S(r_3, r_2) = xr_3 - yr_2 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_3, r_2)$ éliminée

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

Katsura 3 sur $\mathbb{F}_7$ pour $degrevlex_{x>y>z}$

$f_1 = x + 2y + 2z - 1$
$f_2 = xy + yz + 3y$
$f_3 = x^2 + 2y^2 + 2z^2 - x$

1. **Step 1 :** $G_1 = \{r_1 := [(1, f_1), f_1]\}$, $\langle \mathrm{LT}(G_1) \rangle = \langle x \rangle$
2. **Step 2 :** $G_2 \leftarrow \{r_1 = [(1, f_1), f_1], r_2 := [(1, f_2), f_2]\}$
   - paire à considérer :
     $S(r_2, r_1) = 1.r_2 - yr_1 \rightarrow (1, f_2) \notin LT(G_1) \Rightarrow S(r_2, r_1)$ normalisée
     $\Rightarrow CP \leftarrow \{S(r_2, r_1)\}$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_3 := [(1, f_2), y^2 + 4yz + 5y]$ et $CP \leftarrow \emptyset$
   - paires à considérer :
     $S(r_3, r_1) = xr_3 - y^2 r_1 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_3, r_1)$ éliminée
     $S(r_3, r_2) = xr_3 - yr_2 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_3, r_2)$ éliminée
   - $G_2 = \{r_1, r_2, r_3\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle = \langle x, y^2 \rangle$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4 := [(1, f_3), f_3]\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$
   - paires à considérer :
     $S(r_4, r_1) = r_4 - xr_1 \rightarrow (1, f_3) \notin LT(G_2) \Rightarrow S(r_4, r_1)$ normalisée
     $S(r_4, r_2) = yr_4 - xr_2 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_4, r_2)$ éliminée
     $S(r_4, r_3) = y^2 r_4 - x^2 r_3 \rightarrow (y^2, f_3) \in LT(G_2) \Rightarrow S(r_4, r_3)$ éliminée
     $\Rightarrow CP \leftarrow \{S(r_4, r_1)\}$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4 := [(1, f_3), f_3]\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$
   - paires à considérer :
     $S(r_4, r_1) = r_4 - xr_1 \rightarrow (1, f_3) \notin LT(G_2) \Rightarrow S(r_4, r_1)$ normalisée
     $S(r_4, r_2) = yr_4 - xr_2 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_4, r_2)$ éliminée
     $S(r_4, r_3) = y^2 r_4 - x^2 r_3 \rightarrow (y^2, f_3) \in LT(G_2) \Rightarrow S(r_4, r_3)$ éliminée
     $\Rightarrow CP \leftarrow \{S(r_4, r_1)\}$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_5 := [(1, f_3), yz + 4z^2 + 2y + z]$ et $CP \leftarrow \emptyset$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4 := [(1, f_3), f_3]\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$

   - paires à considérer :
     $S(r_4, r_1) = r_4 - xr_1 \rightarrow (1, f_3) \notin LT(G_2) \Rightarrow S(r_4, r_1)$ normalisée
     $S(r_4, r_2) = yr_4 - xr_2 \rightarrow (x, f_2) \in LT(G_1) \Rightarrow S(r_4, r_2)$ éliminée
     $S(r_4, r_3) = y^2 r_4 - x^2 r_3 \rightarrow (y^2, f_3) \in LT(G_2) \Rightarrow S(r_4, r_3)$ éliminée
     $\Rightarrow CP \leftarrow \{S(r_4, r_1)\}$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_5 := [(1, f_3), yz + 4z^2 + 2y + z]$ et $CP \leftarrow \emptyset$
   - paires à considérer :
     $S(r_5, r_1) = xr_5 - yzr_1 \rightarrow (x, f_3) \in LT(G_2) \Rightarrow S(r_5, r_1)$ éliminée
     $S(r_5, r_2) = xr_5 - zr_2 \rightarrow (x, f_3) \in LT(G_2) \Rightarrow S(r_5, r_2)$ éliminée
     $S(r_5, r_3) = yr_5 - zr_3 \rightarrow (y, f_3) \notin LT(G_2)$ et $(z, f_2) \notin LT(G_1)$
     $\Rightarrow S(r_5, r_3)$ normalisée
     $S(r_5, r_4) = x^2 r_5 - yzr_4 \rightarrow (x^2, f_3) \in LT(G_2) \Rightarrow S(r_5, r_3)$ éliminée
     $\Rightarrow CP \leftarrow \{S(r_5, r_3)\}$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 (suite) :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_6 := [(y, f_3), z^2 + 2z]$ et $CP \leftarrow \emptyset$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 (suite) :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_6 := [(y, f_3), z^2 + 2z]$ et $CP \leftarrow \emptyset$
   - paires à considérer :
     $S(r_6, r_1) = xr_6 - z^2 r_1 \rightarrow (xy, f_3) \in LT(G_2) \Rightarrow S(r_6, r_1)$ éliminée
     $S(r_6, r_2) = xyr_6 - z^2 r_2 \rightarrow (xy^2, f_3) \in LT(G_2) \Rightarrow S(r_6, r_2)$ éliminée
     $S(r_6, r_3) = y^2 r_6 - z^2 r_3 \rightarrow (y^3, f_3) \in LT(G_2) \Rightarrow S(r_6, r_3)$ éliminée
     $S(r_6, r_4) = x^2 r_6 - z^2 r_4 \rightarrow (x^2 y, f_3) \in LT(G_2) \Rightarrow S(r_6, r_4)$ éliminée
     $S(r_6, r_5) = yr_6 - zr_5 \rightarrow (y^2, f_3) \in LT(G_2) \Rightarrow S(r_6, r_5)$ éliminée
     $\Rightarrow CP \leftarrow \emptyset$ et $G = \{x + 2y + 2z - 1,\ xy + yz + 3y,\ y^2 + 4yz + 5y,\ x^2 + 2y^2 + 2z^2 - x,\ yz + 4z^2 + 2y + z, z^2 + 2z\}$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 (suite) :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_6 := [(y, f_3), z^2 + 2z]$ et $CP \leftarrow \emptyset$
   - paires à considérer :
     $S(r_6, r_1) = xr_6 - z^2 r_1 \rightarrow (xy, f_3) \in LT(G_2) \Rightarrow S(r_6, r_1)$ éliminée
     $S(r_6, r_2) = xyr_6 - z^2 r_2 \rightarrow (xy^2, f_3) \in LT(G_2) \Rightarrow S(r_6, r_2)$ éliminée
     $S(r_6, r_3) = y^2 r_6 - z^2 r_3 \rightarrow (y^3, f_3) \in LT(G_2) \Rightarrow S(r_6, r_3)$ éliminée
     $S(r_6, r_4) = x^2 r_6 - z^2 r_4 \rightarrow (x^2 y, f_3) \in LT(G_2) \Rightarrow S(r_6, r_4)$ éliminée
     $S(r_6, r_5) = yr_6 - zr_5 \rightarrow (y^2, f_3) \in LT(G_2) \Rightarrow S(r_6, r_5)$ éliminée
     $\Rightarrow CP \leftarrow \emptyset$ et $G = \{x + 2y + 2z - 1,\ xy + yz + 3y,\ y^2 + 4yz + 5y,\ x^2 + 2y^2 + 2z^2 - x,\ yz + 4z^2 + 2y + z, z^2 + 2z\}$
4. **base minimale :**
   $G = \{x + 2y + 2z - 1,\ y^2 + 4yz + 5y,\ yz + 4z^2 + 2y + z, z^2 + 2z\}$

Calcul avec F5 de la BG de Katsura 3 sur $\mathbb{F}_7$

3. **Step 3 (suite) :** $G_3 \leftarrow \{r_1, r_2, r_3, r_4\}$, $\langle \mathrm{LT}(G_2) \rangle = \langle x, xy, y^2 \rangle$
   - triangularisation + preprocessing ...
     $\Rightarrow$ nouveau générateur : $r_6 := [(y, f_3), z^2 + 2z]$ et $CP \leftarrow \emptyset$
   - paires à considérer :
     $S(r_6, r_1) = xr_6 - z^2 r_1 \rightarrow (xy, f_3) \in LT(G_2) \Rightarrow S(r_6, r_1)$ éliminée
     $S(r_6, r_2) = xyr_6 - z^2 r_2 \rightarrow (xy^2, f_3) \in LT(G_2) \Rightarrow S(r_6, r_2)$ éliminée
     $S(r_6, r_3) = y^2 r_6 - z^2 r_3 \rightarrow (y^3, f_3) \in LT(G_2) \Rightarrow S(r_6, r_3)$ éliminée
     $S(r_6, r_4) = x^2 r_6 - z^2 r_4 \rightarrow (x^2 y, f_3) \in LT(G_2) \Rightarrow S(r_6, r_4)$ éliminée
     $S(r_6, r_5) = yr_6 - zr_5 \rightarrow (y^2, f_3) \in LT(G_2) \Rightarrow S(r_6, r_5)$ éliminée
     $\Rightarrow CP \leftarrow \emptyset$ et $G = \{x + 2y + 2z - 1,\ xy + yz + 3y,\ y^2 + 4yz + 5y,\ x^2 + 2y^2 + 2z^2 - x,\ yz + 4z^2 + 2y + z, z^2 + 2z\}$
4. **base minimale :**
   $G = \{x + 2y + 2z - 1,\ y^2 + 4yz + 5y,\ yz + 4z^2 + 2y + z, z^2 + 2z\}$
5. **base réduite :** $G = \{x + 2y + 2z - 1,\ y^2 + 4y,\ yz + 2y,\ z^2 + 2z\}$