CHAPITRE
VI

L'algorithme de Buchberger

Sommaire

§ 1 Introduction

Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$, on suppose que les polynômes f_i sont non nuls. Par définition, l'ensemble $G = \{f_1, \ldots, f_s\}$ forme une base de Gröbner si

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle .$$

Tout polynôme f de I se décompose sous la forme

$$f = h_1 f_1 + \ldots + h_s f_s,$$

où les h_i sont des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$. Une obstruction à être une base de Gröbner apparaît lorsque le terme dominant dans une telle décomposition n'est pas dans l'idéal engendré par les $\mathrm{lt}(f_i)$, comme l'illustre l'exemple suivant.

VI.1.1. Exemple.— Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x,y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2 y - 2y^2 + x$. Pour l'ordre lexicographique gradué, l'ensemble $F = \{f_1, f_2\}$ n'est pas une base de Gröbner. En effet, les termes dominants $\mathrm{lt}(f_1) = x^3$ et $\mathrm{lt}(f_2) = x^2 y$

s'annulent dans l'expression suivante :

$$yf_1 - xf_2 = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2 \in I.$$

Le terme dominant $\mathrm{lt}(yf_1 - xf_2) = -x^2$ n'est pas divisible par $\mathrm{lt}(f_1)$ ou $\mathrm{lt}(f_2)$, par suite, $\mathrm{lt}(-x^2)$ n'est pas dans l'idéal $\langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle$.

Pour former une base de Gröbner de I à partir de l'ensemble générateur $\{f_1, f_2\}$, il faudrait corriger cette obstruction en rajoutant le polynôme $f_3 = -x^2$ à l'ensemble générateur. À ce stade, rien ne nous assure que $\{f_1, f_2, f_3\}$ constitue une base de Gröbner. Le polynôme f_3 est-il source de nouvelles obstructions ?

Dans ce chapitre, nous introduisons la notion de *S-polynôme* permettant de décrire et calculer ces obstructions. On présentera ensuite, l'algorithme de Buchberger qui calcule une base de Gröbner, par une méthode de complétion de l'ensemble générateur par de nouveaux générateurs permettant de résoudre toutes les obstructions.

VI.1.2. Paires critiques.— On peut comprendre aussi l'obstruction qu'il y a pour $\{f_1, f_2\}$ de former une base de Gröbner de I, en utilisant la notion de « *paire critique* ». Cette notion est équivalente à celle de S-polynôme et permet de mettre en évidence les obstructions en utilisant la relation de *réduction par division*.

La division du polynôme $f_1 = x^3 - 2xy \in I$ par lui-même est de reste nul, autrement dit

$$x^3 - 2xy \xrightarrow{f_1} 0.$$

Avec l'ordre monomial choisi, on a $\mathrm{lt}(f_1) = x^3$, la division de x^3 par f_1 est de reste $2xy$, en terme de réduction on a

$$x^3 \xrightarrow{f_1} 2xy.$$

Ainsi, on peut interpréter la division par f_1 comme une *réduction* par f_1. Par exemple, on a

$$x^4 + 3x^3y = (x+3y)(x^3 - 2xy) + (2x^2y + 6xy^2).$$

Dans l'expression $x^4 + 3x^3y$, on remplace les occurences du terme x^3 par le terme $2xy$:

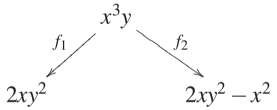
$$x^4 + 3x^3y \xrightarrow{f_1} x(2xy) + 3x^3y \xrightarrow{f_1} x(2xy) + 3(2xy)y = 2x^2y + 6xy^2.$$

Le polynôme $2x^2y + 6xy^2$ ne possède pas de terme divisible par x^3, on dira qu'il est en *forme normale* pour la réduction par f_1.

De la même façon, la relation $f_2 = x^2y - 2y^2 + x$, avec pour terme dominant $\mathrm{lt}(f_2) = x^2y$, s'écrit

$$x^2y \xrightarrow{f_2} 2y^2 - x.$$

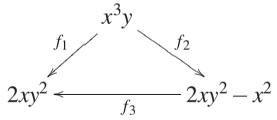
On appellera *paire critique*, l'interaction de deux telles réductions sur un même terme



Rajouter le polynôme $f_3 = x^2$, consiste à rajouter la réduction

$$x^2 \xrightarrow{f_3} 0.$$

Ainsi, le diagramme formé par la paire critique devient « *confluent* » :



VI.1.3. Exemple.— Soient $f_1 = xy - y$ et $f_2 = x - y^2$ des polynômes de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique donné par $y < x$. Soit I l'idéal engendré par $F = \{f_1, f_2\}$. On a $\mathrm{lt}(f_1) = xy$ et $\mathrm{lt}(f_2) = -x$, dans l'expression suivante, ces deux termes dominants s'annulent :

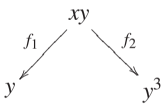
$$f_1 - yf_2 = (xy - y) - y(x - y^2) = -y + y^3.$$

Comme combinaison des polynômes f_1 et f_2, le polynôme $f_3 = -y + y^3$ est dans I. On a cependant $\mathrm{lt}(f_3) = y^3$ non divisible par $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$, donc F n'est pas une base de Gröbner de I. Le polynôme f_3 forme ainsi une obstruction à ce que l'ensemble F soit une base de Gröbner pour I. On peut corriger cela en rajoutant le polynôme f_3 à l'ensemble générateur F. On cherche alors les obstructions à ce que l'ensemble $F' = \{f_1, f_2, f_3\}$ soit une base de Gröbner pour I.

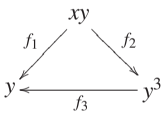
Interprètons ces obstructions en terme de paires critiques. On considère les deux régles

$$xy \xrightarrow{f_1} y, \qquad x \xrightarrow{f_2} y^2.$$

Il apparaît une paire critique

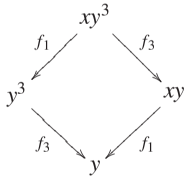


Cette paire critique est confluente lorsque l'on rajoute la règle f_3 :



Avec la règle $y^3 \xrightarrow{f_3} y$, il apparaît une nouvelle paire critique entre les règles f_1 et f_3,

cette paire critique est confluente



Il n'y a alors plus de nouvelle paire critique, nous allons voir que cela suffit à montrer que $\{f_1, f_2, f_3\}$ forme une base de Gröbner de I.

§ 2 Division et réduction

VI.2.1. Réduction.— Soient f, g, h trois polynômes de $\mathbb{K}[x_1, \ldots, x_n]$, avec g non nul. On dit que f se *réduit en une étape* en h modulo g et on note

$$f \xrightarrow{g} h,$$

si $\mathrm{lm}(g)$ divise un terme non nul X de f et que

$$h = f - \frac{X}{\mathrm{lt}(g)} g.$$

En particulier, un ordre monomial fixé, on a, pour tout polynôme f,

$$\mathrm{lt}(f) \xrightarrow{f} \mathrm{lt}(f) - f.$$

Par exemple, si $f = x^3y^2 - x^2y^3 + x$, avec l'ordre lexicographique gradué et $y < x$, on a

$$x^3y^2 \xrightarrow{f} x^2y^3 - x.$$

VI.2.2. Exemple.— Considérons les polynômes $f = 6x^2y - x + 4y^3 - 1$ et $g = 2xy + y^3$ de $\mathbb{Q}[x, y]$, avec l'ordre lexicographique induit par $y < x$. On a $\mathrm{lm}(g) = xy$ qui divise $6x^2y$, d'où la réduction

$$f \xrightarrow{g} -3xy^3 - x + 4y^3 - 1.$$

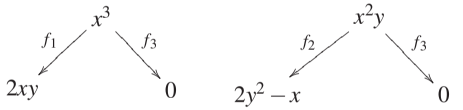
Si l'on considère l'ordre lexicographique gradué avec $y < x$, alors $\mathrm{lm}(g) = y^3$ et la réduction

$$f \xrightarrow{g} 6x^2y - 8xy - x - 1.$$

Noter que, dans ce cas, la réduction ne porte pas sur le terme dominant de f.

VI.2.3. Définition.— Soient f, h des polynômes de $\mathbb{K}[x_1, \ldots, x_n]$ et $F = \{f_1, \ldots, f_s\}$ une famille de polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$. On dit que f se *réduit* en h modulo F et

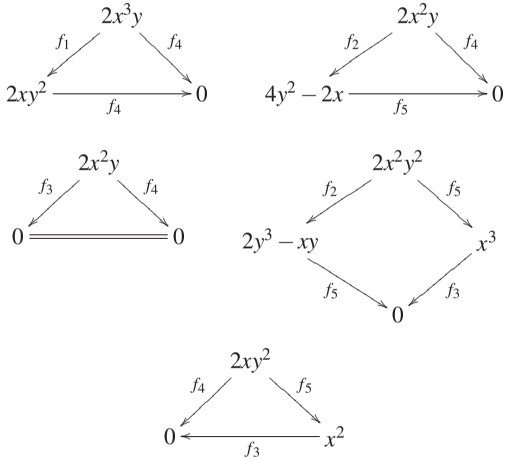
Étape 5. On examine les nouvelles paires critiques :



Étape 6. Pour compléter ces diagrammes, on rajoute les règles

$$2xy \xrightarrow{f_4} 0, \qquad 2y^2 \xrightarrow{f_5} x.$$

Étape 7. On examine les nouvelles paires critiques



Il n'y a plus d'autre paire critique, par suite $G = \{f_1, f_2, f_3, f_4, f_5\}$ est une base de Gröbner de I.

Exercice 9. — Pour les idéaux suivants, construire une base de Gröbner en utilisant l'ordre lexicographique, puis l'ordre lexicographique gradué.

1. $I = \langle x^2y - 1, xy^2 - x \rangle$,
2. $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3 \rangle$,
3. $I = \langle x - z^4, y - z^5 \rangle$.

INITIALISATION : $G := \{f_1, f_2\}, \mathscr{G} := \{\{f_1, f_2\}$

première passage de la boucle **TANT QUE :**

$\mathscr{G} := \emptyset$

$S(f_1, f_2) \xrightarrow{G} x^3 - x$

comme $r \neq 0$, on pose $f_3 := x - x$

$\mathscr{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

second passage de la boucle **TANT QUE :**

$\mathscr{G} := \{\{f_2, f_3\}\}$

$S(f_1, f_3) \xrightarrow{G} 0$

troisième passage de la boucle **TANT QUE :**

$\mathscr{G} := \emptyset$

$S(f_2, f_3) \xrightarrow{G} 0$

Arrêt de la boucle **TANT QUE :** , car $\mathscr{G} = \emptyset$.

D'après le théorème VI.5, l'ensemble $\{f_1, f_2, f_3\}$ forme une base de Gröbner de l'idéal $I = \langle f_1, f_2 \rangle$.

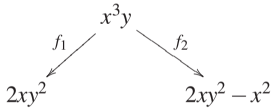
VI.4.5. Complétion des paires critiques.— L'algorithme de Buchberger consiste à compléter progressivement les paires critiques associées aux S-polynômes. Reprenons la construction de la base de Gröbner dans l'exemple VI.4.1. On souhaite construire une base de Gröbner pour l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x,y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$.

Étape 1. On fixe un ordre, par exemple l'ordre lexicographique gradué.

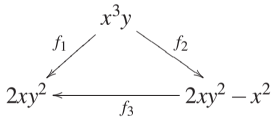
Étape 2. On oriente les relations par rapport à cet ordre

$$x^3 \xrightarrow{f_1} 2xy, \qquad x^2y \xrightarrow{f_2} 2y^2 - x.$$

Étape 3. On calcule les paires critiques. Ici, il n'y a qu'une paire critique formée par f_1 et f_2 :



Étape 4. On rajoute la règle $x^2 \xrightarrow{f_3} 0$, pour obtenir un diagramme confluent :



on note

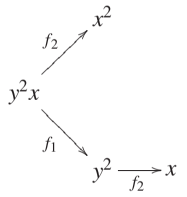
$$f \xrightarrow{F} h,$$

s'il existe une suite de réductions en une étape

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \dots h_{i_{k-1}} \xrightarrow{f_{i_k}} h,$$

où $f_{i_j} \in F$ et $h_j \in \mathbb{K}[x_1, \dots, x_n]$.

VI.2.4. Exemple.— Soient $f_1 = yx - y$ et $f_2 = y^2 - x$ des polynômes de $\mathbb{Q}[x,y]$, avec l'ordre lexicographique gradué associé à $y < x$. Soit $F = \{f_1, f_2\}$ et $f = y^2x$. On a

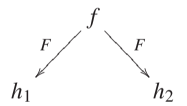


VI.2.5. Définitions.— Un polynôme r est dit en *forme normale* par rapport à un ensemble $F = \{f_1, \dots, f_s\}$ de polynômes non nuls, si $r = 0$ ou s'il n'y a pas de monômes dans r divisible par un $\mathrm{lm}(f_i)$, $i \in [\![1, s]\!]$. On dit aussi que le polynôme r ne peut pas être réduit modulo F.

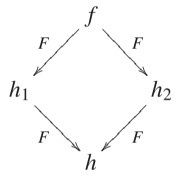
VI.2.6. Remarque.— Pour un polynôme f de $\mathbb{K}[x_1, \dots, x_n]$, si $f \xrightarrow{F} r$, où r est en forme normale relativement à F, alors r est le reste d'une division de f modulo F. De la proposition V.9, on déduit une nouvelle caractérisation, non immédiate mais admise, des bases de Gröbner :

VI.1 Proposition. — Soit $G = \{g_1, \dots, g_t\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1, \dots, x_n]$. Alors G est une base de Gröbner si, et seulement si, pour tout polynôme f de $\mathbb{K}[x_1, \dots, x_n]$, le reste de la division de f modulo G est unique.

VI.2.7. Confluence.— Soit $F = \{f_1, \dots, f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1, \dots, x_n]$. On dit que la relation de réduction $\xrightarrow{F}$ est *confluente* si, pour tout couple de réductions sur un même polynôme f



il existe un couple de réductions vers un même polynôme



§ 3 Les S-polynômes et le critère de Buchberger

VI.3.1. Plus petit commun multiple.— On fixe un ordre monomial sur $\mathscr{M}[x_1,\dots,x_n]$. Soient f et g deux polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. Le *plus petit commun multiple* (ppcm) des polynômes f et g, noté $\mathrm{ppcm}(f,g)$, est l'unique polynôme m de $\mathbb{K}[x_1,\dots,x_n]$ vérifiant les trois assertions suivantes

i) f divise m et g divise m,

ii) si f et g divisent un polynôme h de $\mathbb{K}[x_1,\dots,x_n]$, alors m divise h,

iii) $\mathrm{lc}(m)=1$.

L'existence du ppcm sera admise. Dans le cas particulier de monômes, cette existence est immédiate.

VI.3.2. Les S-polynômes.— Soient f et g des polynômes non nuls de $\mathbb{K}[x_1,\dots,x_n]$. Notons $\alpha=\mathrm{multideg}(f)$ et $\beta=\mathrm{multideg}(g)$. Le ppcm de $\mathrm{lm}(f)$ et $\mathrm{lm}(g)$ est le monôme

$$x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g)),$$

où $\gamma=(\gamma_1,\dots,\gamma_n)$, avec $\gamma_i=\max(\alpha_i,\beta_i)$, pour tout $i\in[\![1,n]\!]$.

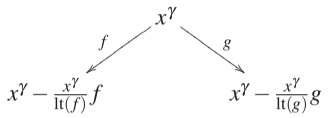
On appelle *S-polynôme* de f et g le polynôme

$$S(f,g)=\frac{x^\gamma}{\mathrm{lt}(f)}f-\frac{x^\gamma}{\mathrm{lt}(g)}g.$$

VI.3.3. Remarque.— Étant donnés deux polynômes f et g de $\mathbb{K}[x_1,\dots,x_n]$, et $x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g))$, alors

$$\mathrm{multideg}(S(f,g))<\gamma.$$

VI.3.4. Les paires critiques.— En terme de réduction, la notion de S-polynôme s'interprète comme un couple de réductions qui « *chevauchent* » sur un même monôme. Un tel couple de réductions est appelé une *paire critique* :



ment par ajout de polynômes, on a ainsi une suite strictement croissante

$$G_1\subsetneq G_2\subsetneq G_3\subsetneq\dots$$

avec $G_i:=G_{i-1}\cup\{r\}$, où r est un polynôme de I, tel que $S(f,g)\xrightarrow{G_{i-1}}r$, où f et g sont deux polynômes de G_{i-1}. Le polynôme r est en forme normale relativement à la division par rapport à G_{i-1}, d'où $\mathrm{lt}(r)\notin\mathrm{lt}(G_{i-1})$. Par suite

$$\mathrm{lt}(G_1)\subsetneq\mathrm{lt}(G_2)\subsetneq\mathrm{lt}(G_3)\subsetneq\dots$$

forme une suite strictement croissante d'idéaux, qui est en contradiction avec la propriété des suites croissantes d'idéaux de $\mathbb{K}[x_1,\dots,x_n]$, théorème V.6 . Ainsi, l'algorithme termine.

Montrons que l'ensemble G obtenu est une base de Gröbner de I. On a $F\subseteq G\subset I$, donc G forme un ensemble de générateurs pour l'idéal I. Par ailleurs, par construction, pour tous $g_i,g_k\in G$, on a $S(g_i,g_k)\xrightarrow{G}0$. D'après le critère de Buchberger, G forme une base de Gröbner de I. □

VI.4.3. Algorithme de Buchberger.—

ENTRÉE : $F=\{f_1,\dots,f_s\}$ une base de I, avec $f_i\neq0$, pour $i\in[\![1,s]\!]$.

SORTIE : une base de Gröbner G de I avec $F\subset G$.

INITIALISATION : $G:=F$

$$\mathscr{G}:=\{\,\{f_i,f_j\}\mid f_i,f_j\in G\text{ et }f_i\neq f_j\}$$

TANT QUE : $\mathscr{G}\neq\emptyset$ **FAIRE**

prendre $\{f,g\}\in\mathscr{G}$

$\mathscr{G}:=\mathscr{G}-\{\{f,g\}\}$

$S(f,g)\xrightarrow{G}r$, où r est en forme normale

SI $r\neq0$ **ALORS**

$\mathscr{G}:=\mathscr{G}\cup\{\{f,r\}\mid\text{pour tout }f\in G\}$

$G:=G\cup\{r\}$

VI.4.4. Exemple.— On exécute l'algorithme de Buchberger sur les polynômes $f_1=xy-x$ et $f_2=-y+x^2$ de $\mathbb{Q}[x,y]$, en considérant l'ordre lexicographique avec $x<y$.

VI.4.2. L'algorithme de Buchberger.— L'idée de Buchberger est de compléter la base F de I en résolvant toute les obstructions, pour obtenir une base de Gröbner. Les relations rajoutées doivent rester redondantes, cela revient à compléter avec des polynômes de I. Dans l'exemple VI.4.1, l'obstruction à ce que $\{f_1, f_2\}$ soit une base de Gröbner est que le reste de la division

$$S(f_1, f_2) \xrightarrow{\{f_1,f_2\}} -x^2$$

est non nul. Comme $S(f_1, f_2) = -x^2 \in I$, on peut inclure ce reste comme générateur et considérer l'ensemble générateur $F' = \{f_1, f_2, f_3\}$ avec $f_3 = -x^2$. On a alors

$$S(f_1, f_2) \xrightarrow{F'} 0.$$

Testons le critère de Buchberger avec les nouveaux S-polynômes $S(f_1, f_3)$ et $S(f_2, f_3)$. On a

$$S(f_1, f_3) = \frac{x^3}{x^3}(x^3 - 2xy) - \frac{x^3}{-x^2}(-x^2) = -2xy.$$

Donc

$$S(f_1, f_3) \xrightarrow{F'} -2xy.$$

On rajoute alors le polynôme $f_4 = -2xy$ comme générateur et on considère l'ensemble $f'' = \{f_1, f_2, f_3, f_4\}$. On a alors

$$S(f_1, f_2) \xrightarrow{F''} 0, \quad S(f_1, f_3) \xrightarrow{F''} 0.$$

On a

$$S(f_1, f_4) = \frac{x^3 y}{x^3}(x^3 - 2xy) - \frac{x^3 y}{-2xy}(-2xy) = -2xy^2 = y f_4.$$

Ainsi $S(f_1, f_4) \xrightarrow{F''} 0$. On

$$S(f_2, f_3) = \frac{x^2 y}{x^2 y}(x^2 y - 2y^2 + x) - \frac{x^2 y}{-x^2}(-x^2) = -2y^2 + x.$$

On rajoute alors le polynôme $f_5 = -2y^2 + x$. En posant $G = \{f_1, f_2, f_3, f_4, f_5\}$, on a

$$S(f_i, f_j) \xrightarrow{G} 0,$$

pour tout $i, j \in [\![1, 5]\!]$. D'après le critère de Buchberger, G est une base de Gröbner de I.

VI.5 Théorème. — Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal non nul de $\mathbb{K}[x_1, \ldots, x_n]$, avec $f_i \neq 0$, pour $i \in [\![1, s]\!]$. L'algorithme de Buchberger construit une base de Gröbner de I en un nombre fini d'étapes.

Preuve. Montrons que l'algorithme termine. Par l'absurde, supposons que l'algorithme ne termine pas. Dans l'affectation $G := G \cup \{r\}$, l'ensemble G se construit progressive-

VI.3.5. Exemple.— Considérons les polynômes

$$f = x^3y^2 - x^2y^3 + x, \qquad g = 3x^4y + y^2$$

de $\mathbb{R}[x, y]$ avec l'ordre lexicographique gradué et $y < x$. Alors $\mathrm{lm}(f) = x^3y^2$ et $\mathrm{lm}(g) = x^4y$ et

$$\mathrm{ppcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = x^4y^2.$$

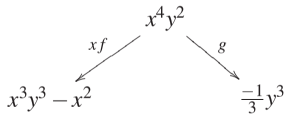
D'où

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g, \\ &= xf - \frac{1}{3} yg, \\ &= x^4y^2 - x^3y^3 + x^2 - x^4y^2 - \frac{1}{3}y^3, \\ &= -x^3y^3 + x^2 - \frac{1}{3}y^3. \end{aligned}$$

En terme de paires critiques, avec les réductions

$$x^3y^2 \xrightarrow{f} x^2y^3 - x, \qquad 3x^4y \xrightarrow{g} -y^2$$

on a la paire critique



Cet exemple illustre que les S-polynômes annulent les termes dominants dans les combinaisons de générateurs.

Exercice 1. — En considérant l'ordre lexicographique, Calculer le S-polynôme $S(f, g)$ dans les cas suivants

1. $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$,
2. $f = x^4y - z^2$, $g = 3xz^2 - y$,
3. $f = x^7y^2z + 2xyz$, $g = 2x^7y^2z + 4$,
4. $f = xy + z^3$, $g = z^2 - 3z$.

Exercice 2. — Étant donnés deux polynômes f et g de $\mathbb{K}[x_1, \ldots, x_n]$, le S-polynôme $S(f, g)$ dépend-t-il de l'ordre monomial ? Illustrer à l'aide d'un exemple.

Exercice 3. — Montrer la remarque VI.3.3

Le résultat suivant montre que toute élimination de termes dominants entre des polynômes qui ont le même multidegré peut s'exprimer en terme de S-polynômes.

VI.2 Proposition. — Soit une combinaison linéaire

$$f = c_1 f_1 + \ldots + c_s f_s, \quad c_i \in \mathbb{K},$$

telle que, pour tout $i \in [\![1,s]\!]$, multideg$(f_i) = \delta \in \mathbb{N}^n$. Si multideg$(f) < \delta$, alors

i) f est une combinaison linéaire à coefficients dans $\mathbb{K}$ de S-polynômes $S(f_i, f_k)$, $i,k \in [\![1,s]\!]$;

ii) de plus, pour tous $i,k \in [\![1,s]\!]$, multideg$\big(S(f_i,f_k)\big) < \delta$.

Preuve. Montrons l'assertion **i)**. Pour tout $i \in [\![1,s]\!]$, on a $\mathrm{lc}(c_i f_i) = c_i \mathrm{lc}(f_i)$ et multideg$(c_i f_i)$ = multideg$(f_i) = \delta$. Or, par hypothèse multideg$(c_1 f_1 + \ldots + c_s f_s) < \delta$, donc nécessairement

$$c_1 \mathrm{lc}(f_1) + \ldots + c_s \mathrm{lc}(f_s) = 0. \tag{VI.1}$$

On a

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i \mathrm{lc}(f_i) \frac{f_i}{\mathrm{lc}(f_i)} \\
&= c_1 \mathrm{lc}(f_1) \left(\frac{f_1}{\mathrm{lc}(f_1)} - \frac{f_2}{\mathrm{lc}(f_2)} \right) + (c_1 \mathrm{lc}(f_1) + c_2 \mathrm{lc}(f_2)) \left(\frac{f_2}{\mathrm{lc}(f_2)} - \frac{f_3}{\mathrm{lc}(f_3)} \right) \\
&\quad + \ldots + (c_1 \mathrm{lc}(f_1) + \ldots + c_{s-1} \mathrm{lc}(f_{s-1})) \left(\frac{f_{s-1}}{\mathrm{lc}(f_{s-1})} - \frac{f_s}{\mathrm{lc}(f_s)} \right) \\
&\quad + (c_1 \mathrm{lc}(f_1) + \ldots + c_s \mathrm{lc}(f_s)) \frac{f_s}{\mathrm{lc}(f_s)}.
\end{aligned}$$

Avec l'équation (VI.1), on obtient

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= c_1 \mathrm{lc}(f_1) \left(\frac{f_1}{\mathrm{lc}(f_1)} - \frac{f_2}{\mathrm{lc}(f_2)} \right) + (c_1 \mathrm{lc}(f_1) + c_2 \mathrm{lc}(f_2)) \left(\frac{f_2}{\mathrm{lc}(f_2)} - \frac{f_3}{\mathrm{lc}(f_3)} \right) \\
&\quad + \ldots + (c_1 \mathrm{lc}(f_1) + \ldots + c_{s-1} \mathrm{lc}(f_{s-1})) \left(\frac{f_{s-1}}{\mathrm{lc}(f_{s-1})} - \frac{f_s}{\mathrm{lc}(f_s)} \right).
\end{aligned} \tag{VI.2}$$

Par ailleurs, pour tout $i \in [\![1,s]\!]$, $\mathrm{lt}(f_i) = \mathrm{lc}(f_i) x^\delta$, donc

$$\mathrm{ppcm}(\mathrm{lm}(f_j), \mathrm{lm}(f_k)) = x^\delta,$$

pour tous $j,k \in [\![1,s]\!]$. D'où

$$\begin{aligned}
S(f_j, f_k) &= \frac{x^\delta}{\mathrm{lt}(f_j)} f_j - \frac{x^\delta}{\mathrm{lt}(f_k)} f_k \\
&= \frac{f_j}{\mathrm{lc}(f_j)} - \frac{f_k}{\mathrm{lc}(f_k)}
\end{aligned}$$

FIGURE VI.1.: Bruno Buchberger (1942-)

Bruno Buchberger est un mathématicien autricien né en 1942. Il introduit la théorie des bases de Gröbner dans sa thèse soutenue en 1965. Il nomme ces bases ainsi en l'honneur de son directeur de thèse Wolfgang Gröbner. Il donne un algorithme, appelé algorithme de Buchberger, qui calcule les bases de Gröbner.

§ 4 L'algorithme de Buchberger

D'après la proposition V.8, tout idéal non nul de $\mathbb{K}[x_1, \ldots, x_n]$ admet une base de Gröbner. La preuve donnée n'est pas constructive ; elle n'indique pas le moyen de construire une base de Gröbner. L'algorithme de Buchberger construit une base de Gröbner d'un idéal à partir d'une base de cet idéal.

VI.4.1. Exemple.— Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x,y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2 y - 2y^2 + x$. Nous avons vu en VI.1.1, que pour l'ordre lexicographique gradué, l'ensemble $F = \{f_1, f_2\}$ n'est pas une base de Gröbner. On peut le montrer en utilisant le critère de Buchberger, on calcule le S-polynôme

$$\begin{aligned}
S(f_1, f_2) &= \frac{x^3 y}{x^3}(x^3 - 2xy) - \frac{x^3 y}{x^2 y}(x^2 y - 2y^2 + x), \\
&= -x^2.
\end{aligned}$$

Comme $-x^2$ n'est pas divisible par $\mathrm{lt}(f_1)$ et $\mathrm{lt}(f_2)$, la forme normale de $S(f_1, f_2)$ est x^2 :

$$S(f_1, f_2) \xrightarrow{F} -x^2$$

et d'après le critère de Buchberger, F n'est pas une base de Gröbner de I.

avec $z < y < x$. En effet, on calcule de S-polynôme

$$\begin{aligned} S(f_1,f_2) &= \frac{yx}{y}(y-z^2) - \frac{yx}{x}(x-z^3), \\ &= xy - xz^2 - xy + yz^3, \\ &= -xz^2 + yz^3, \end{aligned}$$

où $\text{ppcm}(\text{lm}(f_1),\text{lm}(f_2)) = \text{ppcm}(y,x) = yx$. Par ailleurs, la division de $S(f_1,f_2)$ par G donne

$$S(f_1,f_2) = z^3(y-z^2) - z^2(x-z^3) + 0.$$

Par suite $S(f_1,f_2) \xrightarrow{G} 0$ et donc G est une base de Gröbner d'après le théorème VI.3.

Exercice 4.— Montrer que l'ensemble G de l'exemple VI.3.7 ne forme pas une base de Gröbner pour l'ordre lexicographique avec l'ordre alphabétique $x < y < z$.

Exercice 5.— Soient G et G' deux bases de Gröbner d'un idéal I de $\mathbb{K}[x_1,\ldots,x_n]$, relativement à un même ordre monomial. Montrer que pour tout polynôme f de $\mathbb{K}[x_1,\ldots,x_n]$, si $f \xrightarrow{G} r$ et $f \xrightarrow{G'} r'$, où r et r' sont en forme normale, alors $r = r'$.

Exercice 6.— Montrer que $\{y-x^2, z-x^3\}$ n'est pas une base de Gröbner pour l'ordre lexicographique induit par $z < y < x$.

Exercice 7.— L'ensemble $\{x^2-y, x^3-z\}$ est-il une base de Gröbner pour un ordre lexicographique ?

Exercice 8.— Soit I un idéal de $\mathbb{K}[x_1,\ldots,x_n]$ et G une base de Gröbner de I. On note $\widehat{f}^G$, le reste de la division de f par G.

1. Montrer que $\widehat{f}^G = \widehat{g}^G$ si, et seulement si, $f-g \in I$.
2. Montrer que
$$\widehat{f+g}^G = \widehat{f}^G + \widehat{g}^G.$$
3. Montrer que
$$\widehat{fg}^G = \widehat{\widehat{f}^G \widehat{g}^G}^G.$$

L'équation (VI.2) s'écrit alors

$$\sum_{i=1}^{s} c_i f_i = c_1 \text{lc}(f_1) S(f_1,f_2) + (c_1\text{lc}(f_1) + c_2\text{lc}(f_2)) S(f_2,f_3) \qquad \text{(VI.3)}$$
$$+ \ldots + (c_1\text{lc}(f_1) + \ldots + c_{s-1}\text{lc}(f_{s-1})) S(f_{s-1},f_s).$$

L'assertion **ii)** suit de la remarque VI.3.3.
□

VI.3 Théorème (Critère de Buchberger).— Soit I un idéal de $\mathbb{K}[x_1,\ldots,x_n]$. Une base $G = \{g_1,\ldots,g_t\}$ de I est une base de Gröbner de I si, et seulement si, pour tout couple (i,j), avec $i \neq j$

$$S(g_i,g_j) \xrightarrow{G} 0.$$

Preuve. Si G est une base de Gröbner de I, comme tout S-polynôme $S(g_i,g_j)$ est dans I, d'après la proposition V.10, on a $S(g_i,g_j) \xrightarrow{G} 0$.

Montrons la réciproque. Supposons que $G = \{g_1,\ldots,g_t\}$ soit une base de I et que, pour tout couple (i,j), avec $i \neq j$, $S(g_i,g_j) \xrightarrow{G} 0$. Montrons alors G est une base de Gröbner de I. Il suffit de montrer que

$$\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1),\ldots,\text{lt}(g_s) \rangle .$$

Considérons donc un polynôme $f \in I$ et montrons que $\text{lt}(f) \in \langle \text{lt}(g_1),\ldots,\text{lt}(g_s) \rangle$. Il existe une décomposition

$$f = h_1 g_1 + \ldots + h_t g_t, \qquad \text{(VI.4)}$$

où les h_i sont des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$. Posons

$$\delta = \max\{\text{multideg}(h_1 g_1), \ \ldots \ , \text{multideg}(h_t g_t)\}. \qquad \text{(VI.5)}$$

D'après l'exercice IV.10, on a $\text{multideg}(f) \leq \delta$.

Il existe plusieurs décompositions de f sous la forme (VI.4). Pour chaque décomposition, on a un $\delta \in \mathbb{N}^n$, comme défini en (VI.5). On considère une décomposition de f telle que δ soit minimal ; il est possible de faire un tel choix du fait qu'un ordre monomial est un bon ordre.

Si $\text{multideg}(f) = \delta$, c'est-à-dire, il existe un $i \in [\![1,s]\!]$, tel que $\text{multideg}(f) = \text{multideg}(h_i g_i)$, alors $\text{lt}(f)$ est divisible par $\text{lt}(g_i)$. Par suite,

$$\text{lt}(f) \in \langle \text{lt}(g_1),\ldots,\text{lt}(g_s) \rangle .$$

Reste à montrer que $\text{multideg}(f) = \delta$. Pour cela, procèdons par l'absurde, supposons que $\text{multideg}(f) < \delta$. En posant $m(i) = \text{multideg}(h_i g_i)$, on a une décomposition

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i.$$

Soit

$$f = \sum_{m(i)=\delta} \mathrm{lt}(h_i)\, g_i + \sum_{m(i)=\delta} (h_i - \mathrm{lt}(h_i))g_i + \sum_{m(i)<\delta} h_i g_i. \qquad \text{(VI.6)}$$

Or, si $m(i)=\delta$, alors $\mathrm{multideg}((h_i-\mathrm{lt}(h_i))g_i) < \delta$ et si $m(i)<\delta$, alors $\mathrm{multideg}(h_i g_i) < \delta$. Les deux dernières sommes dans (VI.6) sont ainsi de multidegré strictement inférieur à δ. Comme par hypothèse $\mathrm{multideg}(f) < \delta$, on a alors nécessairement

$$\mathrm{multideg}\left(\sum_{m(i)=\delta} \mathrm{lt}(h_i)\, g_i\right) < \delta.$$

En posant, $\mathrm{lt}(h_i) = c_i x^{\alpha(i)}$, avec $c_i \in \mathbb{K}$, on a

$$\sum_{m(i)=\delta} \mathrm{lt}(h_i)\, g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i.$$

Comme pour tout i tel que $m(i)=\delta$, on a $\mathrm{multideg}(\mathrm{lt}(h_i)\, g_i) = \delta$, la somme $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ satisfait aux hypothèses de la proposition VI.2, cette somme se décompose alors en une combinaison linéaire à coefficients dans $\mathbb{K}$ de S-polynômes $S(x^{\alpha(i)}g_i, x^{\alpha(k)}g_k)$:

$$\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k),$$

où $c_{jk} \in \mathbb{K}$. Or

$$\begin{aligned} S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) &= \frac{x^\delta}{x^{\alpha(j)}\mathrm{lt}(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)}\mathrm{lt}(g_k)} x^{\alpha(k)} g_k, \\ &= \frac{x^\delta}{\mathrm{lt}(g_j)} g_j - \frac{x^\delta}{\mathrm{lt}(g_k)} g_k, \\ &= \frac{x^\delta}{\mathrm{ppcm}(\mathrm{lm}(g_j), \mathrm{lm}(g_k))} S(g_j, g_k). \end{aligned}$$

On obtient ainsi une décomposition

$$\sum_{m(i)=\delta} \mathrm{lt}(h_i)\, g_i = \sum_{j,k} c_{jk} \frac{x^\delta}{\mathrm{ppcm}(\mathrm{lm}(g_j), \mathrm{lm}(g_k))} S(g_j, g_k). \qquad \text{(VI.7)}$$

Or, par hypothèse, pour tous j,k

$$S(g_j, g_k) \xrightarrow{G} 0.$$

Ainsi le reste de la division de $S(g_j,g_k)$ par G est nul et le S-polynôme $S(g_j,g_k)$ peut s'écrire sous la forme

$$S(g_j, g_k) = \sum_{i=1}^{t} k_{ijk} g_i,$$

où les k_{ijk} sont des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$ qui satisfont, pour tous i,j,k, à

$$\mathrm{multideg}(k_{ijk} g_i) \leq \mathrm{multideg}(S(g_j, g_k)).$$

On a alors

$$\frac{x^\delta}{\mathrm{ppcm}(\mathrm{lm}(g_j), \mathrm{lm}(g_k))} S(g_j, g_k) = \sum_{i=1}^{t} l_{ijk} g_i,$$

avec $l_{ijk} = \frac{x^\delta}{\mathrm{ppcm}(\mathrm{lm}(g_j), \mathrm{lm}(g_k))} k_{ijk}$. On a donc

$$\mathrm{multideg}(l_{ijk} g_i) \leq \mathrm{multideg}\left(\frac{x^\delta}{\mathrm{ppcm}(\mathrm{lm}(g_j), \mathrm{lm}(g_k))} S(g_j, g_k)\right) < \delta.$$

L'équation (VI.7) s'écrit alors

$$\begin{aligned} \sum_{m(i)=\delta} \mathrm{lt}(h_i)\, g_i &= \sum_{j,k} c_{jk} \left(\sum_{i=1}^{t} l_{ijk} g_i\right) \\ &= \sum_{i=1}^{t} \widetilde{h}_i g_i. \end{aligned}$$

Les polynômes $\widetilde{h}_i$ vérifient

$$\mathrm{multideg}(\widetilde{h}_i g_i) < \delta.$$

Ainsi le multidegré de $\sum_{m(i)=\delta} \mathrm{lt}(h_i)\, g_i$ est strictement inférieur à δ, par suite dans la décomposition (VI.6) tous les termes ont un multidegré strictement inférieur à δ. Ceci contredit l'hypothèse sur la minimalité de δ, par suite, $\mathrm{multideg}(f) = \delta$, ce qui termine la preuve du théorème. □

VI.3.6. Remarque.— On peut montrer que le critère de Buchberger est équivalent à la confluence de la relation de réduction $\xrightarrow{G}$.

VI.4 Théorème (admis !).— Une base $G = \{g_1,\ldots,g_t\}$ d'un idéal I est une base de Gröbner de I si, et seulement si, la relation de réduction $\xrightarrow{G}$ est confluente.

VI.3.7. Exemple.— Considérons l'idéal $I = \langle f_1, f_2\rangle$ de $\mathbb{R}[x,y,z]$ avec $f_1 = y - z^2$ et $f_2 = x - z^3$. Alors $G = \{f_1, f_2\}$ est une base de Gröbner pour l'ordre lexicographique