CHAPITRE
V

L'algorithme de Buchberger

Sommaire

On fixe pour tout ce chapitre un ordre monomial sur $\mathscr{M}[x_1,\ldots,x_n]$. On a vu dans le chapitre précédent que tout idéal de $\mathbb{K}[x_1,\ldots,x_n]$ possède une base finie avec de bonnes propriétés (base de Gröbner). L'objectif de ce chapitre est de donner un algorithme permettant de calculer une base de Gröbner d'un idéal à partir d'une famille génératrice finie de cet idéal.

§ 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. Rappelons que 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.

V.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 $f_2=x^2y-2y^2+x$. 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 $\mathrm{lt}(f_2) = x^2y$ 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, $\mathrm{lt}\left(-x^2\right)$ 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 ajoutant 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* et de *paire critique associée* 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.

V.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 permet de mettre en évidence les obstructions en utilisant la relation de *réduction*.

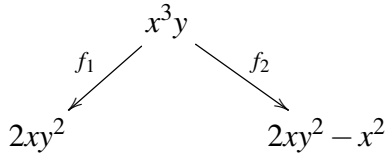
On a naturellement une réduction modulo $f_1 = x^3 - 2xy$ de son terme dominant x^3 :

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

De même pour f_2 :

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

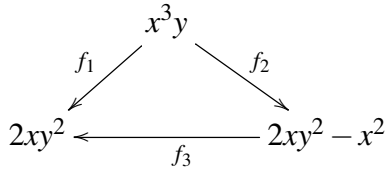
On appellera *paire critique*, l'interaction de deux telles réductions sur le *ppcm* de x^3 et x^2y :



Ajouter le polynôme $f_3 = x^2$, consiste à ajouter la réduction

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

et à rendre confluente cette paire critique :



V.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 :

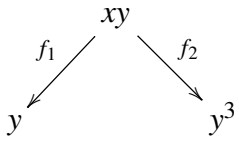
$$f_1 - yf_2 = (xy - y) - y(x - y^2) = -y + y^3.$$

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 ajoutant 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.

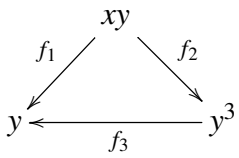
Interprétons ces obstructions en terme de paires critiques. On considère les deux réductions

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

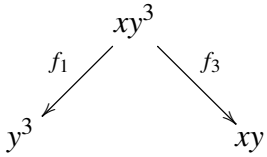
Il apparaît une paire critique



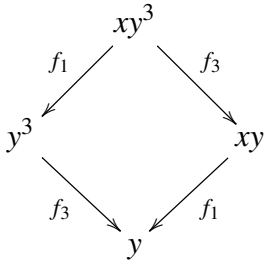
Cette paire critique est confluente lorsque l'on ajoute $f_3 = y^3 - y$:



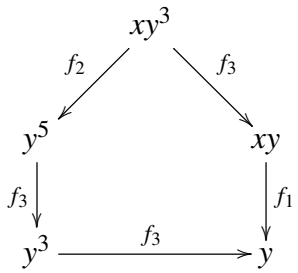
Avec la réduction $y^3 \xrightarrow{f_3} y$, il apparaît une nouvelle paire critique entre les réductions provenant de f_1 et f_3 :



Cette paire critique s'avère être déjà confluente



De même la paire critique associée à f_2 et f_3 est confluente :



Toutes les paires critiques sont alors confluentes. Nous allons voir que cela suffit à montrer que $\{f_1, f_2, f_3\}$ forme une base de Gröbner de I.

§ 2 Les S-polynômes, les paires critiques et le critère de Buchberger

V.2.1. Plus petit commun multiple.— 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.

V.2.2. 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 $i\in[\![1,n]\!]$.

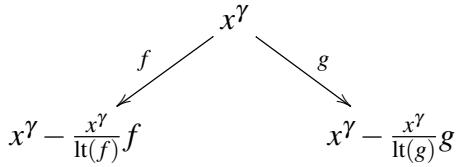
On appelle *S-polynôme* de f et g le polynôme

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

V.2.3. Remarque.— Étant donnés deux polynômes non nuls f et g de $\mathbb{K}[x_1,\dots,x_n]$, et $x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g))$, alors

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

V.2.4. Les paires critiques.— En terme de réductions, la notion de S-polynôme s'interprète comme un couple de réductions qui « *chevauchent* » sur un même monôme. On appelle *paire critique* associée à deux polynômes non nuls f et g (ou paire critique associée au S-polynôme $S(f,g)$), le couple de réductions modulo f et g de $x^\gamma=\mathrm{ppcm}(\mathrm{lm}(f),\mathrm{lm}(g))$:



V.2.5. 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

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

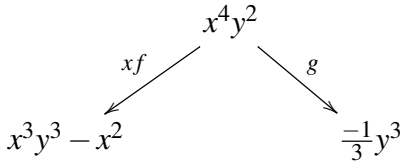
D'où

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

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 91. — 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 92. — 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 93. — Montrer la remarque V.2.3

Exercice 94. — Soient f et g deux polynômes de $\mathbb{K}[x_1,\ldots,x_n]$.

1. Vérifier que

$$S(f,g) = S\left(\frac{f}{\mathrm{lc}(f)}, \frac{g}{\mathrm{lc}(g)}\right).$$

2. Montrer que si $\mathrm{lt}(f)$ divise $\mathrm{lt}(g)$, alors

$$\langle f,g\rangle = \langle f, S(f,g)\rangle.$$

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.

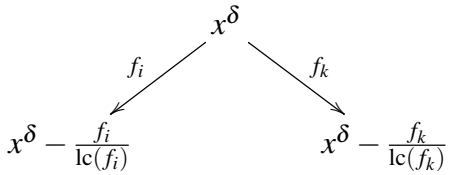
V.1 Proposition. — Soit une combinaison linéaire

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

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

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

ii) de plus, pour tous $i,k \in [\![1,s]\!]$, la paire critique associée à (f_i, f_k) est de la forme



et, en particulier, $\text{multideg}\big(S(f_i,f_k)\big) < \delta$.

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

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

On a

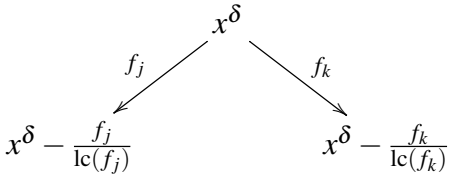
$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i \text{lc}(f_i) \frac{f_i}{\text{lc}(f_i)} \\
&= c_1 \text{lc}(f_1) \left(\frac{f_1}{\text{lc}(f_1)} - \frac{f_2}{\text{lc}(f_2)} \right) + (c_1 \text{lc}(f_1) + c_2 \text{lc}(f_2)) \left(\frac{f_2}{\text{lc}(f_2)} - \frac{f_3}{\text{lc}(f_3)}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

Avec l'équation (V.1), on obtient

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

Par ailleurs, pour tout $i \in [\![1,s]\!]$, $\text{lt}(f_i) = \text{lc}(f_i) x^\delta$. Il suit que, pour tous $j,k \in [\![1,s]\!]$,

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



et

$$S(f_j, f_k) = \frac{f_j}{\mathrm{lc}(f_j)} - \frac{f_k}{\mathrm{lc}(f_k)}.$$

L'équation (V.2) s'écrit alors

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

□

V.2 Proposition.— Soient f et g deux polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$ et $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes non nuls contenant f et g. Soit $\alpha, \beta \in \mathbb{N}^n$.

i) Si $S(f,g) \xrightarrow{F} 0$, alors $S(x^\alpha f, x^\beta g) \xrightarrow{F} 0$.

ii) Si la paire critique associée à (f,g) est confluente modulo F, alors celle associée à $S(x^\alpha f, x^\beta g)$ l'est aussi.

iii) Si la paire critique associée à (f,g) est confluente modulo F, alors on a la décomposition

$$S(f,g) = u_1 f_1 + \ldots + u_s f_s$$

avec pour tout quotient $u_i \neq 0$,

$$\mathrm{multideg}(u_i f_i) < \gamma$$

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

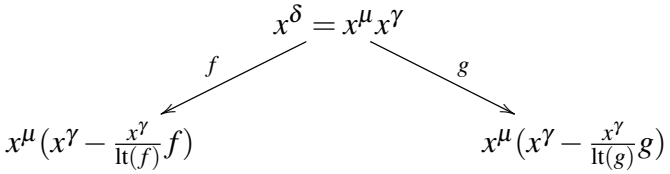
Preuve. Notons que

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

divise

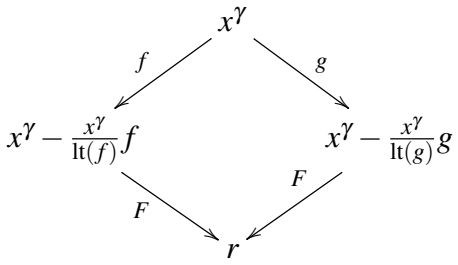
$$x^\delta = \mathrm{ppcm}(x^\alpha \mathrm{lm}(f), x^\beta \mathrm{lm}(g)) = \mathrm{ppcm}(\mathrm{lm}(x^\alpha f), \mathrm{lm}(x^\beta g)).$$

Soit $\mu \in \mathbb{N}^n$ tel que $x^\delta = x^\mu x^\gamma$. Alors, on vérifie facilement que $S(x^\alpha f, x^\beta g) = x^\mu S(f,g)$ et que la paire critique associée à $(x^\alpha f, x^\beta g)$ correspond à la multiplication par x^μ de celle associée à $S(f,g)$:



On en déduit **i)** et **ii)**.

Pour **iii)**, supposons que



Alors, il existe $u'_1, \ldots, u'_s$ et $u''_1, \ldots, u''_s$ tels que

— $x^\gamma - \frac{x^\gamma}{\mathrm{lt}(f)} f = u'_1 f_1 + \ldots + u'_s f_s + r$,

— $x^\gamma - \frac{x^\gamma}{\mathrm{lt}(g)} g = u''_1 f_1 + \ldots + u''_s f_s + r$,

— pour tout $u'_i \neq 0$, $\mathrm{multideg}(u'_i f_i) \leq \mathrm{multideg}\left(x^\gamma - \frac{x^\gamma}{\mathrm{lt}(f)} f\right) < \gamma$,

— pour tout $u''_i \neq 0$, $\mathrm{multideg}(u''_i f_i) \leq \mathrm{multideg}\left(x^\gamma - \frac{x^\gamma}{\mathrm{lt}(g)} g\right) < \gamma$.

D'où,

$$S(f,g) = (x^\gamma - \frac{x^\gamma}{\mathrm{lt}(g)} g) - (x^\gamma - \frac{x^\gamma}{\mathrm{lt}(f)} f) = (u''_1 - u'_1) f_1 + \ldots + (u''_s - u'_s) f_s$$

avec pour tout $(u''_i - u'_i) \neq 0$,

$$\mathrm{multideg}((u''_i - u'_i) f_i) < \gamma.$$

□

V.3 Théorème (Critère de Buchberger). — Soit $G = \{g_1, \ldots, g_t\}$ une base d'un idéal I de $\mathbb{K}[x_1, \ldots, x_n]$. Les assertions suivantes sont équivalentes :

i) G est une base de Gröbner de I ;

ii) pour tout couple (i, j), avec $i \neq j$,

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

iii) pour tout couple (i, j), avec $i \neq j$, la paire critique associée à (g_i, g_j) est confluente.

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 IV.10, on a $S(g_i, g_j) \xrightarrow{G} 0$. De plus, la relation de réduction $\xrightarrow{G}$ est confluente par la remarque IV.4.1, et donc en particulier les paires critiques le sont.

Supposons réciproquement que l'assertion **ii)** ou l'assertion **iii)** est vérifiée. Soit $G = \{g_1, \ldots, g_t\}$ une base de I. Pour montrer que G est une base de Gröbner de I, il suffit de vérifier que

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle .$$

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

$$f = h_1 g_1 + \ldots + h_t g_t, \tag{V.4}$$

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

$$\delta = \max\{\text{multideg}(h_1 g_1),\ \dots\ ,\text{multideg}(h_t g_t)\}. \tag{V.5}$$

D'après la proposition III.10, on a $\text{multideg}(f) \leq \delta$.

Il existe a priori plusieurs décompositions de f sous la forme (V.4). Pour chaque décomposition, on a un $\delta \in \mathbb{N}^n$, comme défini en (V.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 $i \in [\![1,t]\!]$, tel que $\text{multideg}(f) = \text{multideg}(h_i g_i)$, alors $\text{lt}(f)$ est divisible par $\text{lt}(g_i)$. Par suite,

$$\text{lt}(f) \in \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle .$$

Reste à montrer que $\text{multideg}(f) = \delta$. Pour cela, procédons par l'absurde et 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

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

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

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

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

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

Comme pour tout i tel que $m(i) = \delta$, on a $\text{multideg}(\text{lt}(h_i)\, g_i) = \delta$, la somme $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ satisfait aux hypothèses de la proposition V.1, cette somme se décompose alors en une combinaison linéaire à coefficients dans $\mathbb{K}$ de S-polynômes $S(x^{\alpha(i)} g_i, x^{\alpha(k)} g_k)$:

$$\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k), \tag{V.7}$$

où $c_{jk} \in \mathbb{K}$.

Si $S(g_j, g_k) \xrightarrow{G} 0$ pour tous $j \neq k$, alors on a également $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) \xrightarrow{G} 0$ pour tous $j \neq k$, par la proposition V.2. Comme ces derniers S-polynômes sont de multidegrés strictement inférieurs à δ, ils s'écrivent sous la forme

$$S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) = \sum_{i=1}^{t} u_{ijk} g_i, \tag{V.8}$$

tels que $\text{multideg}(u_{ijk} g_i) < \delta$ pour tout $u_{ijk} \neq 0$. Si toutes les paires critiques associées aux $S(g_j, g_k)$ sont confluentes, alors, par la proposition V.2, il en est de même pour les paires cri-

tiques associées aux $S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$ et ces derniers S-polynômes se décomposent comme en (V.8).

Dans les deux cas, on en déduit en utilisant les équations (V.6) et (V.7) que f admet une décomposition de la forme

$$f = \sum_{i=1}^{t} u_i g_i$$

avec $\text{multideg}(u_i g_i) < \delta$ pour tout $u_i \neq 0$. Ceci contredit l'hypothèse sur la minimalité de δ, par suite, $\text{multideg}(f) = \delta$, ce qui termine la preuve du théorème. □

On déduit de ce critère les caractérisations suivantes des bases de Gröbner.

V.4 Théorème. — Soient I un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ un ensemble fini de polynômes. Alors les assertions suivantes sont équivalentes :

i) G est une base de Gröbner de I ;

ii) pour tout polynôme $f \in I$,

$$f \in I, \text{ si, et seulement si, } f \xrightarrow{G} 0;$$

iii) $I = \langle g_1, \ldots, g_t \rangle$ et la relation de réduction $\xrightarrow{G}$ est confluente.

Preuve. On a déjà vu que **i)** implique **ii)** et **iii)** (proposition IV.10 et remarque IV.4.1). Réciproquement, si on suppose **ii)**, alors tous les polynômes g_i sont dans I et tous les polynômes de I se décomposent selon les g_i, donc $I = \langle g_1, \ldots, g_t \rangle$. De plus, comme tous les S-polynômes sont dans $\langle g_1, \ldots, g_t \rangle = I$, ils se réduisent en 0 modulo G. Ainsi G satisfait le critère de Buchberger (V.3). Si on suppose **iii)**, alors toutes les paires critiques sont confluentes et on conclut de même par le théorème V.3. □

V.2.6. Remarque.— Pour la caractérisation **iii)**, il est nécessaire de supposer que $I = \langle g_1, \ldots, g_t \rangle$, sinon G ne serait qu'une base de Gröbner de $\langle g_1, \ldots, g_t \rangle$ mais pas nécessairement de I.

V.2.7. 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 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 V.3.

Exercice 95. — Montrer que l'ensemble G de l'exemple V.2.7 ne forme pas une base de Gröbner pour l'ordre lexicographique avec l'ordre alphabétique $x < y < z$.

Exercice 96. — 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 97. — L'ensemble $\{x^2 - y, x^3 - z\}$ est-il une base de Gröbner pour un ordre lexicographique ?

FIGURE V.1. – Bruno Buchberger (1942-)

Bruno Buchberger est un mathématicien autrichien 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.

§ 3 L'algorithme de Buchberger

D'après la proposition IV.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.

V.3.1. Exemple.— Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x, y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$. Nous avons vu en V.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

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

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.

V.3.2. 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 V.3.1, 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.

V.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 progressivement 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 IV.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. □

V.3.3. Algorithme de Buchberger.—

ENTRÉE : $F = \{f_1,\dots,f_s\}$ une base de I, avec $f_i \neq 0$, pour $i \in [\![1,s]\!]$.
SORTIE : une base de Gröbner G de I avec $F \subset G$.
INITIALISATION : $G := F$
$\mathscr{G} := \{\ \{f_i,f_j\}\ \mid\ 1 <= i < j <= s\}$
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 $r \neq 0$ **ALORS**
$\mathscr{G} := \mathscr{G} \cup \{\{f,r\}\ \mid$ pour tout $f \in G\}$
$G := G \cup \{r\}$

V.3.4. 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 $x < y$.

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 V.5, l'ensemble $\{f_1, f_2, f_3\}$ forme une base de Gröbner de l'idéal $I = \langle f_1, f_2 \rangle$.

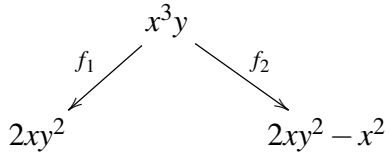
V.3.5. Complétion des paires critiques.— On peut également compléter progressivement les paires critiques associées aux S-polynômes et ainsi satisfaire le second critère. Reprenons la construction de la base de Gröbner dans l'exemple V.3.1. On souhaite construire une base de Gröbner pour l'idéal $I = \langle f_1, f_2 \rangle$ 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.

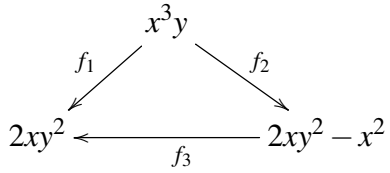
Étape 2. On oriente les relations par rapport à cet ordre

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

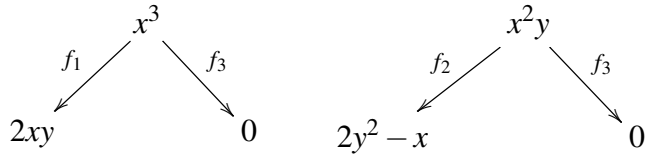
Étape 3. On calcule les paires critiques. Ici, il n'y a qu'une paire critique formée par f_1 et f_2 :



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



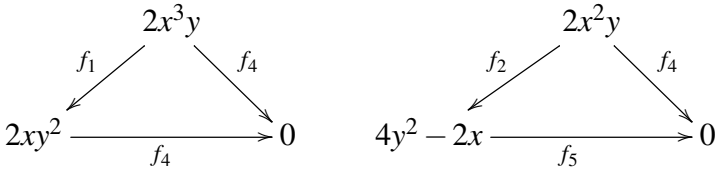
Étape 5. On examine les nouvelles paires critiques :

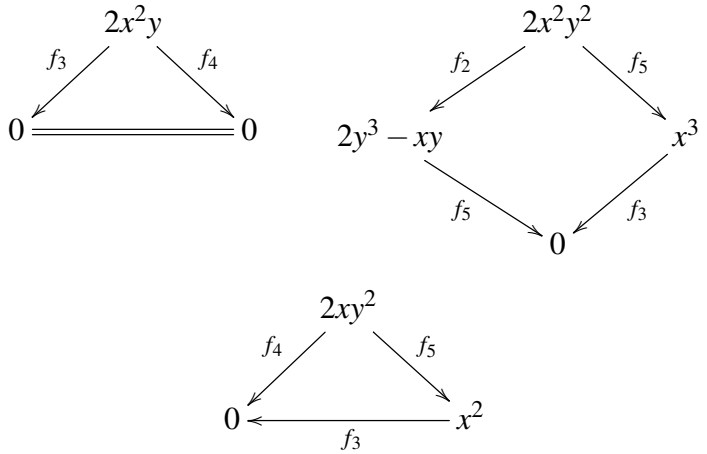


Étape 6. Pour compléter ces diagrammes, on rajoute les règles

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

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 98. — 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. $I = \langle x - z^4, y - z^5 \rangle$.

V.3.6. Remarque.— En pratique, certaines paires critiques sont nécessairement confluentes et, dans certaines situations, quand l'on complète la base par un polynôme, on peut supprimer un polynôme précédent. Ceci permet de diminuer le nombre de calculs. Pour cela, on utilisera les propriétés suivantes :

V.6 Proposition. — Soit $F = \{f_1, \ldots, f_s\}$ un ensemble de polynômes non nuls de $\mathbb{K}[x_1, \ldots, x_n]$ ($s \geq 2$).

i) Si $\text{ppcm}(\text{lm}(f_1), \text{lm}(f_2)) = \text{lm}(f_1)\text{lm}(f_2)$ (c.à.d. si $\text{lm}(f_1)$ et $\text{lm}(f_2)$ sont premiers entre eux), alors la paire critique associée à (f_1, f_2) est confluente modulo $\{f_1, f_2\}$ et

$$S(f_1, f_2) \overset{\{f_1, f_2\}}{\longrightarrow} 0.$$

ii) si $\text{lm}(f_2)$ divise $\text{lm}(f_1)$ et si h est un réduit sous forme normale de $S(f_1, f_2)$ ou une complétion de la paire critique associée modulo F, alors

$$\langle f_1, f_2, \ldots, f_s \rangle = \langle h, f_2, \ldots, f_s \rangle .$$

Exercice 99. — 1. Montrer la proposition V.6.
2. On munit $\mathbb{Q}[x, y, z]$ de l'ordre lexicographique induit par $x > y > z$. Soient $f_1 = xy - y + z$, $f_2 = x^2yz + y^2$ et l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{Q}[x, y, z]$. En utilisant la proposition V.6, déterminer une base de Gröbner de I constituée de trois polynômes.

§ 4 Bases de Gröbner réduites

Une fois calculée une base de Gröbner à l'aide de l'algorithme de Buchberger (ou d'un autre algorithme), on peut réduire cette base :

V.7 Proposition. — Un ordre monomial étant fixé, tout idéal non nul de $\mathbb{K}[x_1,\ldots,x_n]$ possède une unique base de Gröbner G telle que pour tout polynôme $g \in G$ est unitaire et est sous forme normale par rapport à $G \setminus \{g\}$. On appelle cette base, *base de Gröbner réduite*.

La preuve est laissée en exercice ci-dessous :

Exercice 100. — On fixe un ordre monomial et on considère un idéal I non nul de $\mathbb{K}[x_1,\ldots,x_n]$.

1. Montrer que I possède une base de Gröbner G_0 telle que le terme dominant d'aucun polynôme de G_0 ne divise le terme dominant d'un autre polynôme de G_0.
2. Montrer que G_0 est de taille minimale.
3. Montrer qu'il existe une base de Gröbner réduite G_1 de I. (Indication : réduire sous forme normale le polynôme de plus grand multidegré modulo les autres polynômes de la base et itérer.)
4. Décrire un algorithme qui prend en argument une base de Gröbner d'un idéal et retourne une base de Gröbner réduite.
5. On suppose que $G_1 = \{f_1,\ldots,f_n\}$ et $G_2 = \{g_1,\ldots,g_n\}$ sont deux bases de Gröbner réduites de I telles que $\text{multideg}(f_i) = \text{multideg}(g_i) < \text{multideg}(f_{i+1}) = \text{multideg}(g_{i+1})$, pour $0 < i < n$. Montrer par récurrence sur $1 \leq k \leq n$ que $f_k = g_k$.
6. En déduire l'unicité des bases de Gröbner réduites.

Exercice 101. — Réduire les bases de Gröbner obtenues dans l'exercice 98.