Lecture dirigée : Bases de Gröbner

Jad Abou-Yassin, Alexi Delmas, Antoine Galet
Encadrant : Harold Favereau

Avril 2020

Ce travail s'appuie majoritairement sur l'étude du chapitre 2 du livre *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra* de D.A.Cox, J.Little et D.O'Shea [1]

Table des matières

1 Introduction

1.1 Motivation

Étant donné un corps K, l'anneau des polynômes à une variable sur K, $K[x]$, a une arithmétique bien connue et facile à étudier : c'est un anneau euclidien, donc principal, et ses idéaux se manipulent facilement au travers des polynômes générateurs. On aimerait généraliser ces propriétés pratiques à des anneaux de polynômes à plusieurs variables. Malheureusement, ces anneaux ne sont pas principaux : on le constate par exemple avec l'idéal $\langle x, y\rangle$ de $K[x, y]$ engendré par les deux polynômes x et y, qui est évidemment non principal. Des opérations fondamentales en arithmétique, comme tester l'appartenance à un idéal par un algorithme de division, même avec la donnée d'une famille génératrice, s'en retrouvent sensiblement plus difficiles, et des questions théoriques importantes, comme celle l'existence de familles génératrices finies pour un idéal, sont bien moins simples à aborder.

L'objectif de ce texte est de présenter des outils algébriques qui ont été développés pour contourner l'absence de division euclidienne dans le contexte multivarié, leurs propriétés, et leurs champs d'application.

1.2 Une tentative de division généralisée dans $K[x, y]$

Une première stratégie consisterait à généraliser la division euclidienne de $K[x]$ dans un anneau de polynômes à plusieurs variables, comme $K[x, y]$. Cet anneau n'étant pas euclidien, il nous faudrait étendre la notion de division entre polynômes à une sorte de division d'un polynôme par un idéal. Cependant, en pratique il est bien sûr plus simple pour les calculs d'utiliser une famille génératrice de l'idéal que l'idéal lui-même, et on s'intéressera plutôt à la division d'un polynôme par une famille finie de polynômes.

Dans $K[x]$, l'algorithme d'Euclide consiste à éliminer successivement le terme de plus haut degré du dividende, jusqu'à obtenir un reste de plus petit degré que le diviseur. Autrement dit, il séquence le processus de division en n'effectuant que des comparaisons entre monômes - et plus précisément entre *termes dominants* - pour lesquelles la divisibilité est facile à tester. Par analogie, la généralisation de cette division à $K[x, y]$ reposera sur l'élimination successive des monômes du dividende, au moyen de comparaisons entre les *termes dominants* du dividende et des diviseurs.

La notion de terme dominant, encore heuristique à ce stade, fera l'objet de la section 2.

Illustrons par un exemple les propos précédents. Considérons ici les trois polynômes :

$$\begin{cases} f = x^2y + 2xy - y^2 + x + 1 \\ d_1 = xy + y \\ d_2 = y + 1 \end{cases}$$

On veut procéder à la division généralisée de f par d_1 et d_2. Commençons par annuler le terme de degré le plus élevé, x^2y. On peut le faire en soustrayant soit xd_1, soit x^2d_2. Choisissons, dans une telle situation, de toujours prendre le premier diviseur éligible de la famille, ici d_1. On obtient :

$$f = xd_1 + xy - y^2 + x + 1$$

À ce stade, on voit déjà qu'il faut préciser ce qu'on entend par "terme dominant", puisqu'ici le degré seul ne permet pas de discriminer xy et $-y^2$. Cette formalisation sera l'objet de la section suivante. On choisit (de façon ici arbitraire) d'éliminer xy en premier, comme précédemment en utilisant d_1 :

$$f = (x + 2)d_1 - y^2 + x + 1$$

Puis on annule le terme restant de plus haut degré, $-y^2$ au moyen de d_2 (d_1 ne permettant plus de le faire sans ajouter de termes "plus gros") :

$$f = (x + 2)d_1 + (-y)d_2 + x - y + 1$$

Enfin on annule le terme $-y$ avec d_2 :

$$f = (x + 2)d_1 + (-y - 1)d_2 + x + 2$$

Puisqu'il n'est plus possible de simplifier de termes dans $x + 2$ avec les polynômes d_1 et d_2 sans générer de terme "plus gros", on aimerait dire que l'algorithme est terminé, et que le "reste" de la division généralisée de f par le couple (d_1, d_2) est $r = x + 2$.

L'exemple précédent soulève plusieurs des difficultés de la division généralisée, bien que cette dernière n'ait pas encore été formellement définie. Premièrement, le résultat dépend *a priori* de

l'ordre dans lequel la famille est choisie. On peut en effet vérifier que, si on avait effectué la division en priorisant d_2 à d_1, on aurait obtenu la décomposition suivante, très différente de la première :

$$f = 0d_1 + (x^2 + 2x - y + 1)d_2 - x^2 - 2x + 2$$

Deuxièmement, là où en une seule variable la division euclidienne permet de détecter la divisibilité par un reste nul, dans $K[x, y]$ cette propriété est perdue : le reste peut être non nul bien que le dividende appartienne à l'idéal engendré par les diviseurs. En effet, l'identité suivante :

$$f = xd_1 + (x - y + 1)d_2$$

indique que f est en réalité dans l'idéal engendré par d_1 et d_2, alors qu'on a obtenu un reste r non nul dans les deux divisions euclidiennes effectuées précedemment.

Un des objectifs de la suite de ce texte sera de démontrer l'existence, pour tout idéal de $K[x_1, \ldots, x_n]$, de familles génératrices particulières, pour lesquelles cette division généralisée possède de bonnes propriétés : notamment l'unicité de la décomposition avec reste dans la famille (en exigeant certaines propriétés de cette décomposition), ce qui impliquera entre autres l'invariance du résultat de la division par permutation des éléments de la famille, et la caractérisation de l'appartenance à l'idéal engendré par un reste nul.

2 Ordres monomiaux

2.1 Définition

Comme nous l'avons vu, si l'on veut construire une division rigoureuse, nous avons besoin d'un ordre nous permettant de distinguer tous les monômes, donc plus précis que le "degré" utilisé précédemment.

Définition 2.1 (Ordre monomial)**.** Un ordre monomial $>$ sur $K[x_1, \ldots, x_n]$ est une relation d'ordre (stricte) sur $\mathbb{N}^n$ vérifiant :

— L'ordre $>$ est total

— L'ordre $>$ est un bon ordre, c'est-à-dire que toute partie non vide de $\mathbb{N}^n$ admet un minimum pour $>$

— L'ordre $>$ est compatible avec l'addition : si $\alpha, \beta, \gamma \in \mathbb{N}^n$ et si $\alpha > \beta$ alors $\alpha + \gamma > \beta + \gamma$

La donnée d'un ordre monomial est équivalente à celle d'un bon ordre sur les monômes de $K[x_1, \ldots, x_n]$, satisfaisant une propriété de multiplicativité : $x^\alpha > x^\beta \Rightarrow x^\alpha x^\gamma > x^\beta x^\gamma$.

2.2 Exemples

Nous allons définir trois exemples fondamentaux d'ordres monomiaux sur $K[x_1, \ldots, x_n]$.

Définition 2.2 (Ordre lexicographique)**.** On définit la relation d'ordre lexicographique $>_{lex}$ telle que pour $\alpha, \beta \in \mathbb{N}^n, \alpha >_{lex} \beta$ si $\alpha \neq \beta$ et si dans $\mathbb{Z}^n$, la composante non nulle la plus à gauche de $\alpha - \beta$ est positive.

L'ordre lexicographique est monomial, cependant, contrairement au degré dans l'anneau à une variable $K[X]$, il ne permet pas d'éliminer les monômes de plus haut degré cumulé (les x^α avec $|\alpha|$ maximal), ce qui posera des problèmes de temps de calcul si on veut concevoir un algorithme de division s'appuyant sur cet ordre. Nous allons donc introduire deux nouveaux ordres monomiaux prenant en compte ce problème.

Définition 2.3 (Ordres gradués)**.** Soient $\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n)$ des éléments de $\mathbb{N}^n$

L'ordre lexicographique gradué est la relation $>_{glex}$ définie par $\alpha >_{glex} \beta$ si $|\alpha| > |\beta|$ ou si $|\alpha| = |\beta|$ et $\alpha >_{lex} \beta$

L'ordre lexicographique gradué renversé est la relation $>_{grevlex}$ définie par $\alpha >_{grevlex} \beta$ si $|\alpha| > |\beta|$ ou si $|\alpha| = |\beta|$ et $(\beta_n, ..., \beta_1) >_{lex} (\alpha_n, ..., \alpha_1)$

Ces deux ordres dont également des ordres monomiaux. Il est notable que l'ordre $>_{grevlex}$ est différent d'un ordre $>_{glex}$ ou on inverserait l'ordre des variables, c'est pourquoi leurs utilisations et leurs efficacités vont différer.

Exemple. Considérons le polynôme f de $\mathbb{C}[x, y, z]$ donné par $f = 3x^2y + 2xyz - 5x + 5z^2 + 4yz^2$, et ordonnons ses monômes selon les trois ordres monomiaux vus précédemment :

- Ordre lexicographique : $f = 3x^2y + 2xyz - 5x + 4yz^2 + 5z^2$

- Ordre lexicographique gradué : $f = 3x^2y + 2xyz + 4yz^2 + 5z^2 - 5x$
- Ordre lexicographique gradué renversé : $f = 4yz^2 + 2xyz + 3x^2y + 5z^2 - 5x$

2.3 Multidegré d'un polynôme

Étant donné un ordre monomial sur $K[x_1, \ldots, x_n]$, on peut définir par analogie au degré pour une variable, le multidegré d'un polynôme, qui dépend donc de l'ordre que l'on se donne.

Définition 2.4 (Multidegré)**.** On fixe un ordre monomial $>$.

Soit $P = \sum_\alpha a_\alpha x^\alpha$ un polynôme non nul. Son multidegré est le n-uplet

$$multideg(P) = \max(\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0)$$

On appelle alors *coefficient dominant* de P le scalaire $CD(P) = a_{multideg(P)}$, *monôme dominant* de P le monôme unitaire $MD(P) = x^{multideg(P)}$, et enfin *terme dominant* de P le monôme coefficienté $TD(P) = CD(P)MD(P)$.

Exemple. Reprenons le polynôme f de l'exemple précédent. Le multidegré de f dépend de l'ordre monomial choisi, par exemple :

- Pour l'ordre lexicographique : $multideg(f) = (2, 1, 0)$
- Pour l'ordre lexicographique gradué : $multideg(f) = (2, 1, 0)$
- Pour l'ordre lexicographique gradué renversé : $multideg(f) = (0, 1, 2)$

Ce multidegré a de bonnes propriétés de calcul analogues à celles du degré.

Lemme 2.5. *Soient P et Q des polynômes non nuls de $K[x_1, \ldots, x_n]$. Alors*

— $multideg(PQ) = multideg(P) + multideg(Q)$

— *Si $P + Q \neq 0$, alors* $multideg(P + Q) \leq \max(multideg(P), multideg(Q))$.

— *Si $multideg(P) \neq multideg(Q)$, alors* $multideg(P + Q) = \max(multideg(P), multideg(Q))$

— *Si $TD(P) + TD(Q) = 0$, alors* $multideg(P + Q) < \max(multideg(P) + multideg(Q))$

3 Algorithme de division dans $K[x_1, \ldots, x_n]$

Comme vu en première partie, nous allons présenter un algorithme de division dans $K[x_1, \ldots, x_n]$ en généralisant l'algorithme d'Euclide dans $K[X]$. Modulo un ordre monomial fixé, nous avons établi précédemment une notion de terme dominant qui jouera un rôle important dans l'algorithme.

Théorème 3.1 (Division dans $K[x_1, \ldots, x_n]$)**.** *Soit $>$ un ordre monomial sur $\mathbb{N}^n$ et $F = (f_1, \ldots, f_s)$ un s-uplet de polynômes de $K[x_1, \ldots, x_n]$. Soit $f \in K[x_1, \ldots, x_n]$.*

Alors il existe $a_1, \ldots, a_s, r \in K[x_1, \ldots, x_n]$ tels que

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

et $r = 0$ ou r est une combinaison K-linéaire de monômes divisibles par aucun des $TD(f_i)$, $1 \leq i \leq s$.

On appelle alors r un reste de la division de f par F dans $K[x_1, \ldots, x_n]$. De plus, si $1 \leq i \leq s$ et $a_i f_i \neq 0$, alors on a

$$multideg(f) \geq multideg(a_i f_i)$$

Remarque. Contrairement à la division dans $K[X]$, il n'y a pas unicité du reste r si on change l'ordre des f_i dans F. Un exemple a été présenté en première partie. En particulier, on divise un polynôme par un s-uplet de polynômes et non pas par un ensemble fini de polynômes.

Preuve. *La preuve se fait grâce à l'algorithme de division suivant :*

Posons initialement $a_1 = \cdots = a_s = 0$, $r = 0$.

Tant que $f \neq 0$, on tente d'éliminer le terme dominant de f en divisant par le premier des f_i convenable :

— *Si $\{1 \leq i \leq s \,|\, TD(f_i)$ divise $TD(f)\}$ est vide, on met à jour :*

$$\begin{cases} r & \leftarrow & r + TD(f) \\ f & \leftarrow & f - TD(f) \end{cases}$$

— *Sinon, notons i le minimum de cet ensemble. On met à jour :*

$$\begin{cases} a_i & \leftarrow & a_i + \dfrac{TD(f)}{TD(f_i)} \\ f & \leftarrow & f - \dfrac{TD(f)}{TD(f_i)} f_i \end{cases}$$

On vérifie aisément la terminaison de l'algorithme, le multidegré de f diminuant strictement à chaque itération. Prouvons la correction. Pour ce faire, nous allons exhiber un invariant de boucle. Si N est le nombre d'itération avant la fin de l'algorithme, notons pour $0 \leq i \leq N$ $f^{(i)}$, $a_k^{(i)}$ et $r^{(i)}$ respectivement les valeurs de f, a_k et r obtenues à la fin de la i-ème étape, pour tout $1 \leq k \leq s$. Pour $i = 0$, ces valeurs représentent les valeurs initiales données en entrée de l'algorithme. On a alors :

$$\forall i \in [\![0, N]\!], \begin{cases} f^{(0)} = f^{(i)} + \sum_{k=1}^{s} a_k^{(i)} f_k + r^{(i)} \\ r \text{ est une combinaison } K\text{-linéaire de monômes divisibles par aucun des } TD(f_i), 1 \leq i \leq s \end{cases}$$

En effet, c'est évidemment vrai si $i = 0$. Supposons vrai ce résultat pour $0 \leq i \leq N - 1$. On a $f^{(i)}$ non nul car l'algorithme n'est pas fini.

— *Si $\{1 \leq i \leq s \,|\, TD(f_i) \text{ divise } TD(f^{(i)})\}$ est vide, alors :*

$$\begin{cases} f^{(i+1)} + r^{(i+1)} = f^{(i)} + r^{(i)} \\ \forall k \in [\![1, s]\!], a_k^{(i+1)} = a_k^{(i)} \end{cases}$$

Dans ce cas, on a aussi $r^{(i+1)} = r^{(i)} + CD(f^{(i)})MD(f^{(i)})$ et $MD(f^{(i)})$ est un monôme qui n'est divisible par aucun des $TD(f_i)$

— *Sinon, notons k_0 le minimum de cet ensemble. On a alors*

$$\begin{cases} f^{(i+1)} + a_{k_0}^{(i+1)} f_{k_0} = f^{(i)} + a_{k_0}^{(i)} f_{k_0} \\ \forall k \in [\![1, s]\!] \setminus \{k_0\}, a_k^{(i+1)} = a_k^{(i)} \\ r^{(i+1)} = r^{(i)} \end{cases}$$

Dans les deux cas, on a alors que

$$\begin{cases} f^{(i+1)} + \sum_{k=1}^{s} a_k^{(i+1)} f_k + r^{(i+1)} = f^{(i)} + \sum_{k=1}^{s} a_k^{(i)} f_k + r^{(i)} \\ r^{(i+1)} = r^{(i)} + \alpha \tilde{r} \text{ où } \alpha \in K \text{ et } \tilde{r} \text{ est un monôme divisible par aucun des } TD(f_i), 1 \leq i \leq s \end{cases}$$

Par hypothèse de récurrence, on obtient le résultat. Ceci prouve la correction de l'algorithme car $f^{(N)} = 0$.

La division exécutée en partie 1 est un exemple de l'algorithme précédent, où l'ordre monomial employé est l'ordre lexicographique de $K[x, y]$ où $x >_{lex} y$.

Un des intérêts majeurs de la division euclidienne dans $K[X]$ est de pouvoir tester efficacement l'appartenance d'un polynôme à un idéal engendré par un nombre fini d'éléments : Si $f \in K[X]$ et $f_1, \ldots, f_s \in K[X]$, alors on a

$$f \in \langle f_1, \ldots f_s \rangle \Leftrightarrow \text{ Le reste de la division de } f \text{ par } f_1, \ldots, f_s \text{ est nul}$$

Si $f, f_1, \ldots, f_s, a_1, \ldots, a_s \in K[x_1, \ldots, x_n]$ sont tels que

$$f = a_1 f_1 + \cdots + a_s f_s$$

alors il est immédiat que $f \in \langle f_1, \ldots, f_s \rangle$. Mais cette condition n'est pas nécessaire comme le montre l'exemple en partie 1. Ainsi, cette généralisation de l'algorithme de division euclidienne n'est pas satisfaisante. Dans la suite de ce texte, nous allons répondre au problème d'appartenance à un idéal en écrivant un tel idéal comme étant l'idéal engendré par un ensemble judicieusement choisi de polynômes : une base de Gröbner de cet idéal.

4 Idéaux monomiaux et lemme de Dickson

Intéressons-nous d'abord au problème d'appartenance à un idéal dans le cas particulier des idéaux monomiaux. Ce cas est simple à traiter, et il sera fondamental dans la démonstration du cas général.

Définition 4.1 (Idéal monomial)**.** On dit qu'un idéal I de $K[x_1, \ldots, x_n]$ est monomial s'il existe

$A \subseteq \mathbb{N}^n$ tel que $I = \langle x^\alpha \mid \alpha \in A \rangle$

Exemple. L'idéal $\langle xy, x^2, x^9y^8 \rangle$ est un idéal monomial. L'idéal $\langle x - y \rangle$ n'est pas un idéal monomial.

Dans le cas de l'appartenance d'un monôme dans un idéal monomial, on a une caractérisation simple.

Lemme 4.2. *Soit $A \subseteq \mathbb{N}^n$ et $I = \langle x^\alpha \mid \alpha \in A \rangle$ un idéal monomial. Si $\beta \in \mathbb{N}^n$, on a l'équivalence*

$$x^\beta \in I \Leftrightarrow \exists \alpha \in A, x^\alpha \mid x^\beta$$

Preuve. *Le sens réciproque est immédiat. Montrons le sens direct : Soit $\beta \in \mathbb{N}$ tel que $x^\beta \in I$. Alors il existe $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ et $\alpha_1, \ldots, \alpha_s \in A$ tels que $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i}$. En développant cette somme, on obtient une combinaison K-linéaire de monômes, chacun étant divisible par l'un des x^{α_i}. Ainsi, x^β est divisible par l'un des x^{α_i}*

Ce lemme permet de montrer une condition nécessaire et suffisante d'appartenance d'un polynôme à un idéal monomial :

Proposition 4.3. *Soit $A \subseteq \mathbb{N}^n$ et $I = \langle x^\alpha \mid \alpha \in A \rangle$ un idéal monomial. Si $f \in K[x_1, \ldots, x_n]$, on équivalence entre*

(i) $f \in I$

(ii) Chaque terme de f appartient à I

(iii) f est une combinaison K-linéaire de monômes de I

Preuve. *Les implications $(iii) \Rightarrow (ii) \Rightarrow (i)$ sont triviales. Montrons $(i) \Rightarrow (iii)$. Soit $f \in I$, on a $s \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_s \in A$ et $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ tels que $f = \sum_{k=1}^{s} h_k x^{\alpha_k}$. En développant le membre de droite, on obtient que f s'écrit comme une combinaison K-linéaire de monômes, chacun d'entre eux étant divisible par un certain x^{α_k} pour un k dans $[\![1, s]\!]$. Par le lemme précédent, chacun de ces monômes est dans I.*

On a ainsi caractérisé d'une manière simple l'appartenance d'un polynôme à un idéal monomial. Une conséquence immédiate est que deux idéaux monomiaux de $K[x_1, \ldots, x_n]$ sont égaux si et seulement si ils contiennent les mêmes monômes.

Exemple. Considérons l'idéal $I = \langle x, y\rangle$ de $K[x, y]$. On sait que cet idéal n'est pas $K[x, y]$ tout entier car les constantes n'y sont pas dedans. Puisque I est un idéal monomial, on sait alors qu'un polynôme f de $K[x, y]$ appartient à I si et seulement si f est une combinaison K-linéaire de monômes appartenant à I. Or, il est immédiat de voir que tout monôme non constant est dans I et que tout monôme constant n'est pas dans I. Ainsi, on obtient que $I = \{f \in K[x, y] \mid f \text{ n'a pas de terme constant}\}$

Le résultat principal de cette partie est le lemme de Dickson, disant que tout idéal monomial est engendré par un nombre fini de monômes. Ce résultat sera fondamental dans la suite.

Théorème 4.4 (Lemme de Dickson)**.** *Soit $A \subseteq \mathbb{N}^n$ et $I = \langle x^\alpha \mid \alpha \in A\rangle$ un idéal monomial. Alors il existe $s \in \mathbb{N}$ et $\alpha_1, \ldots, \alpha_s \in A$ tels que $I = \langle x^{\alpha_1} \ldots, x^{\alpha_s}\rangle$. En particulier, tout idéal monomial est de type fini.*

Preuve. *Démontrons le lemme de Dickson par résurrence sur n, le nombre de variables. Si $n = 1$, le résultat est immédiat car $K[x]$ est un anneau principal, donc tous ses idéaux sont principaux (monomiaux ou non). Soit maintenant $n \in \mathbb{N}^*$ et on suppose vrai le résultat au rang n. Plaçons nous dans $K[x_1, \ldots, x_n, y]$, de sorte à ce que chaque monôme s'écrive de manière unique $x^\alpha y^m$ où $\alpha \in \mathbb{N}^n$ et $m \in \mathbb{N}$.*

Soit I un idéal de $K[x_1, \ldots, x_n, y]$. Considérons l'idéal J engendré par les x^α pour tout α dans $\mathbb{N}^n$ tels qu'il existe m dans $\mathbb{N}$ tel que $x^\alpha y^m$ soit dans I. On appelle J la projection de I sur $K[x_1, \ldots, x_n]$. Par hypothèse de récurrence, comme J est un idéal monomial de $K[x_1, \ldots, x_n]$, alors il existe $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^n$ tels que $J = \langle x^{\alpha_i} \mid 1 \leq i \leq s\rangle$. Or, pour tout i dans $[\![1, s]\!]$, il existe $m_i \in \mathbb{N}$ tel que $x^{\alpha_i} y^{m_i} \in I$. Posons $m = \max_{1\leq i\leq s} m_i$. On note alors $s_m = s$ et pour tout i dans $[\![1, s_m]\!]$, on note $\alpha_{m,i} = \alpha_i$.

Nous allons maintenant considérer pour tout $k \in [\![0, m-1]\!]$, l'idéal J_k de $K[x_1, \ldots, x_n]$ engendré par les monômes x^β pour tout β dans $\mathbb{N}^n$ tel que $x^\beta y^k \in I$. Par hypothèse de récurrence, comme J_k est un idéal monomial de $K[x_1, \ldots, x_n]$, alors il existe $s_k \in \mathbb{N}$ et $\alpha_{k,1}, \ldots, \alpha_{k,s_k} \in \mathbb{N}^n$ tels que $J_k = \langle x^{\alpha_{k,i}} \mid 1 \leq i \leq s_k\rangle$.

Montrons alors que $I = \langle x^{\alpha_{k,i}} y^k \mid 0 \leq k \leq m,\ 1 \leq i \leq s_k\rangle$.

Notons I' cet idéal. Soit $x^\alpha y^p$ un monôme dans I. Montrons qu'il appartient à I'. Si $p \geq m$, alors par construction de J, il existe $i \in [\![1, s_m]\!]$ tel que $x^{\alpha_{m,i}} y^m$ divise $x^\alpha y^p$. Sinon, par construction de J_p, il existe $i \in [\![1, s_p]\!]$ tel que $x^{\alpha_{p,i}} y^p$ divise $x^\alpha y^p$. Ainsi, par critère d'appartenance d'un monôme à un idéal monomial, $x^\alpha y^p \in I'$. Le résultat s'en déduit immédiatement pour un polynôme de

I, combinaison K-linéaire de monômes de I, par le lemme précédent. Ainsi, $I \subseteq I'$. Mais les générateurs de I' sont dans I par construction, donc $I = I'$ qui est donc engendré par un nombre fini d'éléments.

5 Bases de Gröbner

5.1 Théorème de la base de Hilbert

Nous allons maintenant généraliser les résultats d'appartenance à un idéal de $K[x_1, \ldots, x_n]$ pour un idéal quelconque, grâce aux résultats qu'on a établis dans la partie précédente pour les idéaux monomiaux de $K[x_1, \ldots, x_n]$.

Tout d'abord, nous allons définir une notation pratique :

Définition 5.1. Soit I un idéal de $K[x_1, \ldots, x_n]$ non nul. On note $TD(I) = \{TD(f) | f \in I\}$

Ce qui a été fait précédemment montre l'importance des termes dominants dans l'étude des polynômes et idéaux de $K[x_1, \ldots, x_n]$. Si I est un idéal non nul de $K[x_1, \ldots, x_n]$, nous allons nous intéresser à l'idéal $\langle TD(I) \rangle$.

Proposition 5.2. *Soit I un idéal de $K[x_1, \ldots, x_n]$ non nul. Alors*

(i) $\langle TD(I) \rangle$ est un idéal monomial de $K[x_1, \ldots, x_n]$

(ii) Il existe $t \in \mathbb{N}^*$ et $g_1, \ldots, g_t \in I$ tels que $\langle TD(I) \rangle = \langle TD(g_1), \ldots, TD(g_t) \rangle$

Ce résultat simple [1] permet de démontrer le théorème de la base de Hilbert.

Théorème 5.3 (Théorème de la base de Hilbert)**.** *Tout idéal de $K[x_1, \ldots, x_n]$ est de type fini.*

Preuve. *Soit I un idéal de $K[x_1, \ldots, x_n]$. Le résultat est trivial si I est l'idéal nul. On suppose que ce n'est pas le cas. Par la proposition précédente, on a $t \in \mathbb{N}^*$ et $g_1, \ldots, g_t \in I$ tels que $\langle TD(I) \rangle = \langle TD(g_1), \ldots, TD(g_t) \rangle$. Montrons que $I = \langle g_1, \ldots, g_t \rangle$.*

Comme on a déjà $\langle g_1, \ldots, g_t \rangle \subseteq I$, on montre l'inclusion réciproque. Soit $f \in I$ un polynôme. Si f est le polynôme nul, alors $f \in \langle g_1, \ldots, g_t \rangle$. Sinon, effectuons la division euclidienne de f par le n-uplet $(g_1, \ldots, g_t)$. On a $a_1, \ldots, a_t, r \in K[x_1, \ldots, x_n]$ tels que $f = a_1 g_1 + \cdots + a_t g_t + r$ et r est une

combinaison K-linéaire de monômes divisibles par aucun des $TD(g_i)$ pour $1 \leq i \leq t$. Montrons qu'alors, $r = 0$, ceci prouvera que $f \in \langle g_1, \ldots, g_t \rangle$.

On remarque tout d'abord que $r = f - (a_1 g_1 + \cdots + a_t g_t) \in I$. Si r était non nul, on aurait donc $TD(r) \in \langle TD(I) \rangle = \langle TD(g_1), \ldots, TD(g_t) \rangle$. Ainsi, $TD(r)$ est divisible par l'un des $TD(g_i)$ pour $1 \leq i \leq t$, ce qui est absurde. Donc $r = 0$ d'où le résultat.

5.2 Bases de Gröbner

Ce qui précède nous conduit à introduire le concept de base de Gröbner, un choix judicieux de système de générateurs d'un idéal de $K[x_1, \ldots, x_n]$ pour lequel la division euclidienne nous permet de déterminer facilement si un polynôme appartient à cet idéal ou non.

Définition 5.4. Soit I un idéal de $K[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une partie finie de I. On dit que G est une *base de Gröbner* de I si $\langle TD(I) \rangle = \langle TD(g_1), \ldots, TD(g_t) \rangle$

La preuve du théorème de la base de Hilbert nous donne également ce résultat d'existence :

Proposition 5.5. *Tout idéal non nul de $K[x_1, \ldots, x_n]$ admet une base de Gröbner, et toute base de Gröbner d'un idéal non nul de $K[x_1, \ldots, x_n]$ en est une partie génératrice.*

5.3 Propriétés des bases de Gröbner

Un des problèmes majeurs rencontrés lors de notre tentative de généralisation de la division euclidienne est que selon l'ordre dans lequel sont les diviseurs, le résultat (et surtout le reste de la division !) peut être différent. Il se trouve que les bases de Gröbner corrigent ce défaut :

Proposition 5.6. *Soit I in idéal de $K[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une base de Gröbner de I. Si f est un polynôme de $K[x_1, \ldots, x_n]$, alors il existe un unique couple (g, r) d'éléments de $K[x_1, \ldots, x_n]$ tel que*

(i) $g \in I$

(ii) r *est une combinaison K-linéaire de monômes divisibles par aucun des $TD(g_i)$ pour $1 \leq i \leq t$.*

(iii) $f = g + r$

r est appelé reste de la division euclidienne de f par G. Étant unique, il ne dépend pas de l'ordre dans lequel on considère les éléments de G. On notera $f \equiv r$ modulo G, et $\overline{f}^G = r$

Preuve. *L'existence d'un tel couple provient simplement de la division euclidienne de f par les éléments de G, pris dans un ordre quelconque. Nous allons montrer l'unicité d'un tel couple (g, r). Soient (g, r) et (g', r') deux couples de $I \times K[x_1, \ldots, x_n]$ vérifiant (ii) et (iii). Alors $r - r' = g' - g \in I$. Le même argument utilisé dans la preuve du théorème de la base de Hilbert donne alors que $r - r' = 0$, donc $(g, r) = (g', r')$ d'où l'unicité.*

Remarque. Bien qu'un tel couple (g, r) soit unique, il n'en est pas de même pour les a_i, quotients de la division euclidienne, qui peuvent varier selon l'ordre dans lequel les éléments de G sont considérés.

Étant donnée une base de Gröbner d'un idéal, l'appartenance d'un polynôme f à cet idéal peut se vérifier facilement avec l'algorithme de division :

Corollaire 5.7. *Soit I un idéal de $K[x_1, \ldots, x_n]$ et G une base de Gröbner de I. Soit f un élément de $K[x_1, \ldots, x_n]$. Alors on a :*

$$f \in I \Leftrightarrow \overline{f}^G = 0$$

Définition 5.8. Soit f un polynôme et $F = (f_1, ..., f_s)$ un s-uplet ordonné de polynômes. On note $\overline{f}^F$ le reste de la division de f par le s-uplet F.

Remarque. Dans le cas où F est une base de Gröbner de l'idéal engendré par F. La proposition 1 donne que l'ordre des polynômes peut être quelconque.

Le corollaire précédent nous donne alors une condition très simple pour savoir si un polynôme f appartient à un idéal polynomial I, et cette condition se vérifie algorithmiquement. Cependant, il reste à obtenir une base de Gröbner. Le théorème de la base de Hilbert nous dit qu'elle provient du lemme de Dickson, mais ce dernier ne donne pas une preuve constructive des générateurs d'un idéal monomial...

Définition 5.9. Soient $f, g \in K[x_1, \ldots, x_n]$ non nuls. On note $\alpha = multideg(f), \beta = multideg(g)$. On considère le n-uplet γ tel que pour $i \in [1, n]$, $\gamma_i = max(\alpha_i, \beta_i)$. x^γ est le plus petit commun

multiple (ppcm) des termes dominants $TD(f)$ et $TD(g)$.
On définit le S-polynôme de f et g comme

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

Proposition 5.10. *Soit $s \in \mathbb{N}^*$ et $c_1, \ldots, c_s \in K$, $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ et $\delta \in \mathbb{N}^n$ tels que pour tout $1 \leq i \leq s$, $multideg(f_i) = \delta$ et $multideg\left(\sum_{i=0}^{s} c_i f_i\right) < \delta$.*

Alors $\sum_{i=0}^{s} c_i f_i$ est une combinaison K-linéaire des S-polynômes $S(f_i, f_j)$ pour $1 \leq i \neq j \leq s$, qui ont tous un multidegré strictement inférieur à δ.

Les S-polynômes nous donnent le critère suivant, permettant de vérifier si une partie génératrice d'un idéal polynomial en est une base de Gröbner.

Théorème 5.11 (Critère de Buchberger)**.** *Soit I un idéal de $K[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\} \subseteq I$ une partie génératrice de I. On a équivalence entre :*

(i) G est une base de Gröbner de I

(ii) Pour tout $1 \leq i \neq j \leq t$, $\overline{S(g_i, g_j)}^G = 0$

Les preuves de ces deux résultats non triviaux peuvent être trouvées dans le livre *Ideals, Verieties, and Algorithms* [1].

Bien que très pratique, ce critère ne nous permet pas de construire une base de Gröbner connaissant une partie génératrice d'un idéal de $K[x_1, \ldots, x_n]$.

6 Algorithme de Buchberger

L'algorithme de Buchberger permet, à partir d'une partie génératrice d'un idéal polynomial, de construire une base de Gröbner de ce dernier. Informellement, le but de cet algorithme est d'ajouter des éléments dans la partie génératrice pour que le critère de Buchberger soit vérifié, et le choix le plus raisonnable est d'ajouter les S-polynômes qui n'ont pas un reste nul après division par la partie génératrice. L'idée est de continuer ainsi jusqu'à ce que tous les S-polynômes soient

congrus à 0 modulo la partie génératrice, et le critère de Buchberger permet d'affirmer qu'on a bien obtenu une base de Gröbner.

Théorème 6.1 (Algorithme de Buchberger)**.** *Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal non nul de $K[x_1, \ldots, x_n]$. L'algorithme suivant permet de construire G une base de Gröbner de I :*

Entrée : $F = (f_1, \ldots, f_s)$

Traitement :

Poser $G = F$ et $G' = \emptyset$

Tant que $G \neq G'$ faire :

$G' \leftarrow G$

Pour tout $(p, q) \in {G'}^2$ tel que $p \neq q$ faire :

$S = \overline{S(p,q)}^{G'}$

$G \leftarrow G \cup \{S\}$ *si* $S \neq 0$

Sortie : Une base de Gröbner G de I avec $F \subseteq G$

Preuve. *La correction de l'algorithme est immédiate par le critère de Buchberger. Comme on ne fait qu'ajouter des éléments, on a $F \subseteq G$. Il reste juste à montrer que $G \subseteq I$ pour conclure. C'est immédiat car si $a, b \in I$, alors $S(a, b) \in I$ donc $\overline{S(a,b)}^{G} \in I$ comme somme de deux termes dans I.*

Montrons la terminaison de l'algorithme. Si $G = \langle g_1, ..., g_n \rangle$ on note $\langle TD(G) \rangle$ l'idéal $\langle TD(g_1), ..., TD(g_n) \rangle$. Après un passage dans la boucle, on a rajouté à G tous les restes $\overline{S(p,q)}^{G'}$ pour $p, q \in G'$ (G' étant G avant le passage dans la boucle). De plus, si $G' \neq G$, $\langle TD(G') \rangle$ est strictement inclus dans $\langle TD(G) \rangle$. En effet, si r est un reste ajouté pendant le passage dans la boucle, alors $TD(r)$ n'est pas dans $\langle TD(G') \rangle$, sinon on aurait pu le diviser pas un polynôme de G'. Or $TD(r)$ est dans $\langle TD(G) \rangle$, d'où l'inclusion stricte. Ainsi la suite des $\langle TD(G) \rangle$ est une suite croissante d'idéaux, elle est donc constante à partir d'un certain rang par le théorème de la base de Hilbert. Donc, à partir d'un certain rang, on aura $G' = G$.

Lemme 6.2. *Soit G une base de Gröbner d'un idéal I, et p un polynôme de G. Si $TD(p) \in \langle TD(G \setminus \{p\}) \rangle$, alors $G \setminus \{p\}$ est une base de Gröbner de I.*

Ce résultat nous donne un critère pour retirer un polynôme "redondant" à une base de Gröbner, ce qui nous mène à la notion de base de Gröbner minimale.

Définition 6.3. Une base de Gröbner G d'un idéal I est dite minimale si

— Pour tout $p \in G$, $CD(p) = 1$

— Pour tout $p \in G$, $TD(p)$ n'est pas dans $\langle TD(G \setminus \{p\})\rangle$

Il est ainsi aisé d'obtenir une base de Gröbner minimale grâce à l'algorithme de Buchberger puis en retirant tous les générateurs inutiles grâce au lemme. Cependant, pour un idéal polynômial I, il peut exister de multiples bases de Gröbner minimales. Or, il serait souhaitable d'associer à un idéal polynômial une unique base de Gröbner l'engendrant. Ceci est possible grâce à la notion de base de Gröbner réduite.

Définition 6.4. Une base de Gröbner G d'un idéal I est dite réduite si

— Pour tout $p \in G$, $CD(p) = 1$

— Pour tout $p \in G$, aucun terme de p n'est dans $\langle TD(G \setminus \{p\})\rangle$

Proposition 6.5. *Soit I un idéal polynômial non nul. Alors I a une unique base de Gröbner réduite.*

Remarque. On rappelle que tous ces résultats sont vrais pour un ordre monomial fixé : une partie génératrice d'un idéal polynômial en est une base de Gröbner ou non selon l'ordre monomial fixé.

Preuve. *Soit I un idéal de $K[x_1, \ldots, x_n]$*

Existence : Soit G une base de Gröbner minimale de I. Construisons à partir de G une base de Gröbner réduite de I. On dit que $g \in G$ est réduit pour G lorsque tous les termes de G ne sont pas dans $\langle TD(G \setminus \{g\})\rangle$.

Soit $g \in G$. Posons $g' = \overline{g}^{G\setminus\{g\}}$ et $G' = (G \setminus \{g\}) \cup \{g'\}$. Alors G' est encore une base de Gröbner minimale de I. En effet, on a d'abord que $TD(g) = TD(g')$, puisque $TD(g)$ n'est divisible par aucun des termes dominants des éléments de $G \setminus \{g\}$ par définition d'une base de Gröbner minimale. Ainsi, $\langle TD(G)\rangle = \langle TD(G')\rangle$. Ainsi, G' est une base de Gröbner minimale de I. Enfin, g' est réduit pour G' par construction.

Pour obtenir une base de Gröbner réduite de I, il suffit d'appliquer ce qui précède à chaque éléments de G, en remarquant que si un élément $g \in G$ est réduit pour G, alors il est réduit pour toute base de Gröbner minimale qui contient g et qui possède les mêmes termes dominants que G.

Unicité : Soient G et $\widetilde{G}$ deux bases de Gröbner réduite de I. Montrons le résultat suivant :

Lemme 6.6. *Soit I un idéal polynômial et G, $\widetilde{G}$ deux bases de Gröbner minimales de I. Alors $TD(G) = TD(\widetilde{G})$*

Preuve. *Si $TD(G) \neq TD(\widetilde{G})$, quitte à échanger G et $\widetilde{G}$, on peut supposer qu'il existe $g \in G$ tel que $TD(g) \in I = TD(G) \setminus TD(\widetilde{G})$. Comme $g \in \langle \widetilde{G} \rangle$, alors $TD(g) \in \langle TD(\widetilde{G}) \rangle$. Comme $TD(g)$ est un monôme par définition d'une base de Gröbner minimale, et que $\langle TD(\widetilde{G}) \rangle$ est un idéal monomial, alors il existe $\alpha \in \mathbb{N}^n$ tel que $TD(g) = x^\alpha TD(\widetilde{g})$ pour un certain $\widetilde{g} \in \widetilde{G}$. De même (on n'a pas utilisé le fait que $TD(g) \in TD(G) \setminus TD(\widetilde{G})$ encore), on a $\beta \in \mathbb{N}^n$ tel que $TD(\widetilde{g}) = x^\beta TD(g')$ pour un certain $g' \in G$. Mais alors, si $g \neq g'$, $TD(g) = x^{\alpha+\beta} TD(g') \in \langle TD(G) \setminus \{g\} \rangle$ et c'est impossible car G est une base de Gröbner minimale pour I. Ainsi $g = g'$ et alors $\alpha = \beta = (0, \ldots, 0)$. Donc $TD(g) = TD(\widetilde{g})$, ce qui est absurde. Finalement, un tel g n'existe pas, donc $TD(G) = TD(\widetilde{G})$ ce qui conclut la preuve du lemme.*

Comme G et $\widetilde{G}$ sont des bases de Gröbner réduites de I, elle sont en particulier minimales. Le lemme assure donc que $TD(G) = TD(\widetilde{G})$. Soit $g \in G$, il existe donc un unique $\widetilde{g} \in \widetilde{G}$ tel que $TD(g) = TD(\widetilde{g})$. Montrons que $g = \widetilde{g}$. Soit $h = g - \widetilde{g}$. Alors $h \in I$ donc $\overline{h}^G = 0$. Or, tous les termes de h ne sont divisibles par aucun des éléments de $TD(G)$, puisque $TD(g) = TD(\widetilde{g})$ donc ces termes disparaissent dans $h = g - \widetilde{g}$ et parce que G est une base de Gröbner réduite. Donc finalement, $\overline{h}^G = h = 0$. Donc $g = \widetilde{g}$ ce qui conclut.

7 Applications

7.1 Le problème de l'appartenance à un idéal

L'une des motivations principales qui nous a conduit à introduire la notion de bases de Gröbner est celle du problème d'appartenance d'un polynôme de $K[x_1, \ldots, x_n]$ à un idéal de cet anneau.

L'étude précédente montre qu'il est ainsi aisé de répondre à ce problème, grâce au résultat suivant : Si I est un idéal de $K[x_1, \ldots, x_n]$, G une base de Gröbner de I et $f \in K[x_1, \ldots, x_n]$, alors on a :

$$f \in I \Leftrightarrow \overline{f}^G = 0$$

Appliquons ce critère à un exemple :

Exemple. Soient $f_1 = xz - y^2$ et $f_2 = x^3 - z^2$ deux polynômes de $\mathbb{C}[x, y, z]$ et $I = \langle f_1, f_2 \rangle$. Soit $f = -4x^2y^2z^2 + y^6 + 3z^5$ un polynôme de $\mathbb{C}[x, y, z]$. On veut savoir si $f \in I$.

Tout d'abord, fixons un ordre monomial. Nous allons utiliser l'ordre lexicographique gradué.

Ensuite, vérifions si (f_1, f_2) est une base de Gröbner de I. Par le critère de Buchberger, il suffit de vérifier que $\overline{S(f_1, f_2)}^{(f_1, f_2)} = 0$. Le calcul du S-polynôme de f_1 et f_2 donne que $S(f_1, f_2) = -x^2y^2 + z^3$. Or, $xz = TD(f_1)$ et $x^3 = TD(f_2)$ ne divisent ni $-x^2y^2$, ni z^3. ainsi, $\overline{S(f_1, f_2)}^{(f_1, f_2)} = S(f_1, f_2) \neq 0$: (f_1, f_2) n'est pas une base de Gröbner de I.

Appliquons alors l'algorithme de Buchberger afin d'obtenir, à partir de (f_1, f_2), une base de Gröbner de I. Notons $G = (f_1, f_2)$. La première étape consiste à ajouter $S(f_1, f_2)$ à G, qu'on note f_3. On a maintenant $G = (f_1, f_2, f_3)$. Après calcul, on obtient que :

$$\begin{cases} S(f_1, f_3) = -xy^4 + z^4 \\ \overline{S(f_1, f_3)}^G = -xy^4 + z^4 \end{cases} \quad \begin{cases} S(f_2, f_3) = -y^2z^2 + xz^3 \\ \overline{S(f_2, f_3)}^G = 0 \end{cases}$$

On pose alors $f_4 = -xy^4 + z^4$, on l'ajoute à G et on recommence :

$$\begin{cases} S(f_1, f_4) = -y^6 + z^5 \\ \overline{S(f_1, f_4)}^G = -y^6 + z^5 \end{cases} \quad \begin{cases} S(f_2, f_4) = -y^4z^2 + x^2z^4 \\ \overline{S(f_2, f_4)}^G = 0 \end{cases} \quad \begin{cases} S(f_3, f_4) = -y^2z^3 + xz^4 \\ \overline{S(f_3, f_4)}^G = 0 \end{cases}$$

On pose alors $f_5 = -y^6 + z^5$ et on l'ajoute à G. Quatre derniers calculs de S-polynômes et d'algorithme de division euclidienne montre que tous les S-polynômes de G sont congrus à 0 modulo G. L'algorithme de Buchberger termine et dans ce cas :

$$G = (f_1, f_2, f_3, f_4, f_5) = (xz - y^2, x^3 - z^2, -x^2y^2 + z^3, -xy^4 + z^4, -y^6 + z^5)$$

est une base de Gröbner de I.

Il ne reste plus qu'à calculer $\overline{f}^G$ pour conclure : Appliquons l'algorithme de division euclidienne étape par étape. Notons f' le polynôme f qui sera modifié au cours de l'algorithme.

0. Initialement, on a :

$$\begin{cases} f' = -4x^2y^2z^2 + y^6 + 3z^5 \\ r = 0 \end{cases} \quad \text{et} \quad \begin{cases} a_1 = 0 & a_2 = 0 \\ a_3 = 0 & a_4 = 0 \\ a_5 = 0 \end{cases}$$

1. Comme $TD(f') = -4x^2y^2z^2$ est divisible par $TD(f_1) = xz$, on obtient que :

$$\begin{cases} f' = -4xy^4z + y^6 + 3z^5 \\ r = 0 \end{cases} \quad \text{et} \quad \begin{cases} a_1 = -4xy^2z & a_2 = 0 \\ a_3 = 0 & a_4 = 0 \\ a_5 = 0 \end{cases}$$

2. Comme $TD(f') = -4xy^4z$ est divisible par $TD(f_1) = xz$, on obtient que :

$$\begin{cases} f' = -3y^6 + 3z^5 \\ r = 0 \end{cases} \quad \text{et} \quad \begin{cases} a_1 = -4xy^2z - 4y^4 & a_2 = 0 \\ a_3 = 0 & a_4 = 0 \\ a_5 = 0 \end{cases}$$

3. Comme $TD(f') = -3y^6$ est divisible par $TD(f_5) = -y^6$ et pas par aucun des termes dominants de $f_1, \ldots, f_4$, on obtient que :

$$\begin{cases} f' = 0 \\ r = 0 \end{cases} \quad \text{et} \quad \begin{cases} a_1 = -4xy^2z - 4y^4 & a_2 = 0 \\ a_3 = 0 & a_4 = 0 \\ a_5 = 3 \end{cases}$$

On a $f' = 0$, l'algorithme s'arrête. Ainsi, on obtient que :

$$f = (-4xy^2z - 4y^4)(xz - y^2) + 3(-y^6 + z^5)$$

En particulier, $\overline{f}^G = 0$: on en conclut que $f \in I$.

Remarquons qu'il est possible de vérifier de manière plus immédiate si un polynôme appartient

à un idéal ou non dans certains cas : prenons par exemple $g = xy - 5z^2 + x$. En remarquant simplement que $TD(g) = xy \notin \langle TD(G)\rangle = \langle xz, x^3, -x^2y^2, -xy^4, -y^6\rangle$, on en conclut directement que $g \notin I$

7.2 Résolution d'équations polynomiales [2]

Les bases de Gröbner interviennent de manière très utile dans la théorie de l'élimination, qui consiste à résoudre de manière algorithmique des systèmes d'équations polynomiales par élimination de variables. Dans le cas linéaire, on peut citer l'algorithme du pivot de Gauss comme un algorithme d'élimination. Voyons sur un exemple comment appliquer les bases de Gröbner à la résolution d'équation polynomiales.

Considérons le système suivant dans $\mathbb{C}[x, y, z]$:

$$\begin{cases} x^2 + y^2 + z^2 &= 4 \\ x^2 + 2y^2 &= 5 \\ xz &= 1 \end{cases}$$

Ce système définit l'idéal $I = \langle f_1, f_2, f_3\rangle = \langle x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1\rangle$, et on cherche à calculer la variété affine $V(I)$, définie par :

$$V(I) = \{(a_1, a_2, a_3) \in \mathbb{C}^3 \,|\, \forall f \in I, f(a_1, a_2, a_3) = 0\}$$

Une des propriétés des variétés affines d'un idéal est que celle-ci est égale à la variété affine d'une de ses parties génératrices, et ne dépend pas de la famille génératrice considérée (ce qui justifie la notation $V(I)$). Ainsi, on a, pour toute famille génératrice $g_1, \ldots, g_s$ de I :

$$V(I) = \{(a_1, a_2, a_3) \in \mathbb{C}^3 \,|\, \forall i \in [\![1, s]\!], g_i(a_1, a_2, a_3) = 0\}$$

Nous allons voir ce qui se passe si on prend une base de Gröbner pour le calcul de $V(I)$. Nous allons utiliser l'ordre lexicographique comme ordre monomial, nous expliquerons ensuite pourquoi ce choix. Une application de l'algorithme de Buchberger puis une minimisation donnent pour base

de Gröbner de I l'ensemble $G = \{g_1, g_2, g_3\}$ où

$$\begin{cases} g_1 &= x + 2z^3 - 3z \\ g_2 &= y^2 - z^2 - 1 \\ g_3 &= 2z^4 - 3z^2 + 1 \end{cases}$$

On remarque un fait intéressant, g_3 ne dépend que de la variable z ! De plus, une factorisation de g_3 s'obtient assez facilement en remarquant que 1 et -1 sont racines :

$$g_3 = (z-1)(z+1)(z+1/\sqrt{2})(z-1/\sqrt{2})$$

On obtient ainsi quatre valeurs possibles pour z, qui sont $-1, 1, 1/\sqrt{2}$ et $-1/\sqrt{2}$. En les substituant une à une dans l'équation $g_2 = 0$ et $g_1 = 0$, on obtient :

z	y	x
1	$\pm\sqrt{2}$	1
-1	$\pm\sqrt{2}$	-1
$1/\sqrt{2}$	$\pm\sqrt{3/2}$	$\sqrt{2}$
$-1/\sqrt{2}$	$\pm\sqrt{3/2}$	$-\sqrt{2}$

Ce qui donne huit solutions au système. On a ainsi trouvé $V(I)$ grâce aux bases de Gröbner.

Le point remarquable de cet exemple est qu'on a obtenu g_3 ne dépendant que de la variable z, et il était aisé d'en trouver ses quatre racines, ce qui donne quatre nouveaux systèmes polynomiaux d'ordre strictement inférieurs. De manière générale, ce principe s'applique également : il s'agit des théorèmes d'élimination et d'extension.

Le théorème d'élimination permet, à partir d'une base de Gröbner d'un idéal $I = \langle f_1, \ldots, f_s \rangle$ pour l'ordre lexicographique, d'obtenir les bases de Gröbner des idéaux d'élimination de I, c'est-à-dire des idéaux $I \cap K[x_{l+1}, \ldots, x_n]$ pour $0 \leq l \leq n-1$ (éventuellement nuls). Ces idéaux

représentent l'ensemble des combinaisons linéaires à coefficients dans $K[x_1, \ldots, x_n]$ des f_i qui ne font plus intervenir les variables $x_1, \ldots, x_l$.

Le théorème d'extension permet quant à lui, dans le cas où $K = \mathbb{C}$, de trouver à partir d'une solution partielle $(a_{l+1}, \ldots, a_n)$ de $V(I_l)$ des solutions partielles de la forme $(a_l, a_{l+1}, \ldots, a_n)$ de $V(I_{l-1})$ (éventuellement aucune s'il n'y en a pas). En remarquant que $I_0 = I$, ces deux théorèmes offrent un moyen de calculer algorithmiquement $V(I)$ dans de nombreux cas, en calculant par le théorème d'élimination dans un premier temps le premier idéal d'élimination non nul I_l de $K[x_n]$, représentant un système polynomial avec peu d'indéterminées qu'on peut résoudre plus facilement en général, puis dans un second temps en se ramenant à des solutions de I_{l-1} par l'algorithme d'extension. On répète ensuite ceci jusqu'à obtenir les solutions de I_0.

Bibliographie

[1] David A. Cox, John Little et Donal O'Shea. "Gröbner Bases". In : *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Cham : Springer International Publishing, 2015, p. 49-119. ISBN : 978-3-319-16721-3. DOI : 10.1007/978-3-319-16721-3_2. URL : https://doi.org/10.1007/978-3-319-16721-3_2.

[2] David A. Cox, John Little et Donal O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2005. Chap. 2, p. 24-26. ISBN : 9780387207339. URL : https://books.google.fr/books?id=QFFpepgQgT0C.