

Bases de Gröbner, algorithme de Buchberger et applications

Frédéric Chyzak

Décembre 2004 – Notes de cours

I	Bases de Gröbner et applications	1
1	Introduction	2
2	Idéaux de polynômes	3
3	Quelques problèmes sur les idéaux de polynômes	3
3.1	Finitude de la présentation d'un idéal	3
3.2	Appartenance à un idéal	4
3.3	Résolution de systèmes polynomiaux	4
3.4	Équations implicites d'un lieu géométrique donné par une paramétrisation	5
4	Monômes et ordre monomial	5
4.1	Terminologie sur les polynômes	5
4.2	Monoïde des monômes	6
4.3	Ordres monomiaux et exemples principaux	6
4.4	Coefficients, monômes et termes de tête	7
5	Réduction et division en plusieurs indéterminées	8
5.1	Réduction	8
5.2	Division en plusieurs indéterminées	8
6	Escaliers, définition et existence des bases de Gröbner	9
6.1	Parties stables du monoïde des monômes	10
6.2	Définition des bases de Gröbner	10
6.3	Lemme de Dickson et existence des bases de Gröbner	12
7	Applications de la théorie des bases de Gröbner	13
7.1	Théorème de Hilbert et noethérianité des anneaux de polynômes	13
7.2	Problème d'appartenance à un idéal	13
7.3	Élimination et résolution de systèmes polynomiaux	14
7.4	Élimination et équations implicites	15
II	Algorithme de Buchberger	16
8	Saturation des escaliers et algorithme naïf	16
8.1	S -polynômes et relation avec les bases de Gröbner	17
8.2	Version rudimentaire de l'algorithme de Buchberger	17
9	Réductions à zéro et algorithme classique	18
9.1	Paires triviales et paires inutiles	18
9.2	Forme canonique pour les idéaux de polynômes	19
9.3	Algorithme de Buchberger et ses stratégies classiques	19
10	Cas particulier et extensions de l'algorithme de Buchberger	21
10.1	Cas particulier de l'algorithme d'Euclide	21
10.2	Cas particulier de l'algorithme de Gauss	22
10.3	Bases de Gröbner de modules	22
10.4	Application : base de Gröbner en terme des polynômes initiaux	23
11	Complexité intrinsèque et bases de Gröbner	23
11.1	Problèmes complets	23
11.2	Taille de la sortie	24
III	Calculs en Magma	24

Première partie : Bases de Gröbner et applications

1 Introduction

La division euclidienne et l'algorithme d'Euclide pour le P.G.C.D. sont des outils algorithmiques centraux en algèbre commutative computationnelle¹ et en calcul formel sur les polynômes en une seule indéterminée. Ces outils offrent des moyens algorithmiques pour calculer sur des idéaux (somme par le P.G.C.D., intersection par le P.P.C.M.) ou modulo un idéal de polynômes (forme normale par la division euclidienne, inversion modulo un polynôme par la relation de Bézout), mais aussi, dualement, sur les nombres algébriques, les zéros de polynômes d'une indéterminée.

On s'attend à trouver la même universalité d'applications dans le cas de plusieurs indéterminées, et c'est le cas, avec même plus de richesse. De même que dans le cas d'une seule indéterminée, l'algèbre commutative computationnelle fournit des algorithmes pour la mise sous forme canonique des idéaux de polynômes en plusieurs indéterminées, pour effectuer des divisions avec unicité du reste ou obtenir des formes canoniques modulo un idéal de polynômes. Une opération supplémentaire est celle d'élimination polynomiale. Elle consiste à trouver parmi les combinaisons linéaires d'une famille de polynômes donnés avec des coefficients polynomiaux toutes celles qui ne font plus apparaître telle ou telle indéterminée que l'on s'est fixée.

Du point de vue des applications, on retrouve bien des généralisations au cas de plusieurs indéterminées de celles qui viennent d'être abordées pour le cas d'une indéterminée, mais à chaque fois dans un cadre plus élaboré. La division en plusieurs indéterminées, pour ne prendre que cet exemple, nécessite de savoir diviser par toute une famille de polynômes, et non plus par un seul; dans le cas de reste nul, elle permet d'exprimer un polynôme comme combinaison d'une famille de polynômes donnés avec des coefficients polynomiaux. Avec l'opération d'élimination, on peut de plus aborder des questions comme la recherche d'une équation implicite décrivant un lieu géométrique donné par une paramétrisation ou la résolution de systèmes polynomiaux de plusieurs indéterminées.

La théorie algorithmique bien adaptée pour le cas de plusieurs indéterminées est la théorie des bases de Gröbner, développée initialement pour les idéaux de polynômes de plusieurs indéterminées par B. Buchberger dans les années 1960, qui lui donna le nom de son directeur de thèse. L'algorithme pour les calculer est aujourd'hui appelé algorithme de Buchberger. Sans entrer dans des querelles d'écoles, il nous faut mentionner les travaux antérieurs d'H. Hironaka qui donna une théorie fort similaire pour les idéaux de séries en plusieurs indéterminées. Aujourd'hui, la théorie a été développée dans divers mondes non commutatifs (algèbres de mots, algèbres de groupes, algèbres d'opérateurs linéaires différentiels, de récurrence, etc). Le champ des applications est vaste et varié : géométrie algébrique algorithmique, théorie des invariants, programmation entière, théorie des codes, étude structurelle des ÉDP linéaires et de leur groupes de symétries, étude de systèmes hypergéométriques, manipulation de fonctions spéciales générales, sommation et intégration symboliques, preuve de théorèmes géométriques assistée par ordinateur, ...

Malgré bientôt le demi-siècle d'existence de l'algorithme de Buchberger, sa complexité algorithmique reste encore mal connue. On s'en est longtemps tenu à évoquer sa complexité au pire, doublement exponentielle, que certains invoquent pour refuser d'utiliser les bases de Gröbner. Pourtant, des progrès récents portant sur l'implantation et l'algorithmique permettent de manipuler des systèmes gigantesques. On sait depuis assez longtemps que la complexité au pire tombe à simplement exponentielle dans un certain nombre de cadres d'applications les plus fréquents. Et la recherche en cours semble être sur le point de pouvoir donner des résultats de complexité en moyenne, eux aussi indiquant une complexité simplement exponentielle, et par ailleurs une complexité polynomiale en la taille de la sortie.

Les algorithmes et les applications du cas de plusieurs indéterminées vont être présentés en deux temps. Dans une première partie, nous présenterons la théorie des bases de Gröbner; nous

¹On ne trouve pas ce mot, de l'anglais *computational*, dans le dictionnaire. On dit aussi « effective », mais l'auteur a une préférence pour « computationnel », qui rappelle plus fortement que le calcul peut vraiment se faire sur ordinateur, *computer* en anglais.

nous donnerons l'algorithme de Buchberger comme une boîte noire et verrons comment l'utiliser dans les applications. La partie suivante sera consacrée à détailler l'algorithme de Buchberger.

Dans la section 2, nous rappelons la définition et les premières propriétés algébriques des idéaux. En section 3, nous posons quatre problèmes que nous trouverons une solution algorithmique ou au moins constructive par la théorie des bases de Gröbner. La section 4 introduit les ordres sur les monômes qui vont remplacer les puissances décroissantes du cas d'une indéterminée. La division euclidienne trouve son pendant en plusieurs indéterminées en section 5. Nous sommes alors prêts pour définir les bases de Gröbner en section 6. Nous terminons la première partie en section 7 en explicitant des méthodes algorithmiques qui répondent aux problèmes posés en début de texte.

2 Idéaux de polynômes

De même que l'ensemble de tous les multiples d'un polynôme donné dans le cas univarié, l'objet algébrique à la base de la théorie est ici l'ensemble de toutes les combinaisons linéaires à coefficients polynomiaux d'une famille de polynômes donnés, appelé un « idéal ». Rappelons qu'un idéal I d'un anneau commutatif unitaire A est un sous-groupe de A stable par multiplication par tout élément de A . Étant donnée une famille $(g_u)_{u \in U}$ d'éléments de A , les combinaisons linéaires finies à coefficients dans A forment un idéal noté $\sum_{u \in U} Ag_u$. On montre que tout idéal est de cette forme. Dans cette présentation, les éléments de la famille sont appelés *générateurs* de I . Insistons bien sur le terme « fini » de la définition, les sommes infinies n'étant pas toutes susceptibles de se sommer dans un anneau général.

Dans le cadre qui nous intéresse, celui d'un anneau de polynômes de la forme $\mathbb{C}[X_1, \dots, X_n]$, on peut donc tout d'abord se donner un idéal par des générateurs $g_u \in \mathbb{C}[X_1, \dots, X_n]$. Une des questions qu'il faudra se poser est de savoir si un idéal polynomial peut être engendré par un nombre fini de générateurs. Un autre mode de présentation des idéaux de polynômes fait le lien avec la géométrie : l'ensemble des polynômes de $\mathbb{C}[X_1, \dots, X_n]$ qui s'annulent sur un ensemble donné V de points de \mathbb{C}^n ,

$$I(V) = \{ p \in \mathbb{C}[X_1, \dots, X_n] : \forall x = (x_1, \dots, x_n) \in V, p(x) = 0 \}, \quad (1)$$

est un idéal appelé l'*idéal annulateur* de V .

Rappelons maintenant deux opérations élémentaires sur les idéaux généraux. Étant donnés deux idéaux I et J d'un anneau A , la *somme* $I + J$ est l'idéal engendré par l'union $I \cup J$. Lorsque les idéaux sont donnés par des familles de générateurs, la somme est donnée par l'union de ces familles. L'intersection des idéaux I et J est un idéal. Il n'y a pas de lien explicite immédiat entre une famille de générateurs pour $I \cap J$ et des familles de générateurs pour I et J , mais un algorithme existe dans le cas d'idéaux de polynômes.

3 Quelques problèmes sur les idéaux de polynômes

Dorénavant, sauf mention expresse du contraire, tous les idéaux sont des idéaux d'un anneau de polynômes $\mathbb{C}[X_1, \dots, X_n]$, que l'on notera A_n dans la suite. Nous posons maintenant quatre problèmes que nous trouverons une solution algorithmique par la théorie des bases de Gröbner (ou au moins constructive pour le premier). Nous y reviendrons ultérieurement pour expliciter ces solutions.

3.1 Finitude de la présentation d'un idéal

On l'a dit, un idéal peut toujours être vu comme engendré par une famille ; plus précisément, on a toujours la relation triviale $I = \sum_{p \in I} A_n p$. Une question intéressante est de savoir quand on peut se limiter à une somme finie. Notons d'abord que la question n'est absolument pas évidente pour un idéal donné comme annulateur d'un ensemble algébrique, par la définition (1).

D'autre part, le résultat ne peut être vrai pour un anneau général, même commutatif. Par exemple, il est faux pour l'anneau de polynômes $A_\infty = k[X_0, X_1, \dots]$ en une infinité (dénombrable) d'indéterminées. (Pour se convaincre que cet anneau existe bien, on peut se le représenter comme l'union sur n des A_n .) Chaque élément de A_∞ est une somme finie qui tombe dans un des A_n , donc chaque élément ne fait intervenir qu'un nombre fini d'indéterminées. Montrons que l'idéal $I = \sum_{i \in \mathbb{N}} A_\infty X_i$ n'est pas finiment engendré. Pour ce faire, considérons la chaîne infinie d'inclusions $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ pour les idéaux $I_n = \sum_{i=0}^n A_\infty X_i$ de A_∞ . Cette chaîne est infinie strictement croissante, car chaque X_n est dans $I_n \setminus I_{n-1}$. Sinon, en exprimant X_n comme combinaison de la forme $p_0 X_0 + \dots + p_{n-1} X_{n-1}$ puis en spécialisant chaque X_i pour $i < n$ à 0, nous obtiendrions une contradiction. Si maintenant l'idéal I était engendré par un nombre fini de générateurs, on trouverait un I_n les contenant tous. Donc nous aurions l'inclusion $I \subseteq I_n$, donc l'égalité $I = I_k$ pour $k \geq n$, ce qui serait une contradiction.

Dans le cas d'une indéterminée et de A_1 , les idéaux sont principaux (peuvent être présentés comme engendrés par un unique générateur). Nous verrons que pour les anneaux A_n , un nombre fini de générateurs suffit.

3.2 Appartenance à un idéal

Soient un idéal I de $A_n = \mathbb{C}[X_1, \dots, X_n]$, donné par une famille finie de générateurs, et un polynôme $p \in A$. Comment déterminer algorithmiquement si p est dans I ? Dans l'affirmative, comment calculer algorithmiquement une représentation de p comme combinaison linéaire à coefficients dans A_n des générateurs de I ?

Par exemple, $X^3 - 1$ est-il combinaison linéaire (sur $\mathbb{C}[X, Y, Z]$) de $X + Y + Z$, $XY + YZ + ZX$ et de $XYZ - 1$? La réponse est positive, car

$$X^3 - 1 = (X^2 - XY - XZ - YZ)(X + Y + Z) + (Y + Z)(XY + YZ + ZX) + 1 \times (XYZ - 1).$$

Cependant, on imagine bien qu'une telle décomposition n'est pas unique : il suffit d'ajouter terme à terme l'égalité

$$0 = (XY + YZ + ZX)(X + Y + Z) + (-X - Y - Z)(XY + YZ + ZX) + 0 \times (XYZ - 1)$$

pour obtenir une autre décomposition. Nous verrons comment obtenir de manière générale et algorithmique une décomposition qui sera minimale en un certain sens.

Un lien avec la géométrie se fait par la notion de « variété affine » : pour un ensemble S de polynômes, on définit l'ensemble algébrique (ou variété affine)

$$V(S) = \{x = (x_1, \dots, x_n) \in \mathbb{C}^n : \forall f \in S, f(x) = 0\}.$$

Lorsque S est fini, l'ensemble $V(\sum_{i=1}^s A p_i)$ est noté plus simplement $V(p_1, \dots, p_s)$. Le problème de l'appartenance d'un polynôme p à l'idéal $I \in A_n$ s'interprète alors comme le problème équivalent de l'inclusion $V(I) \subseteq V(p)$. (Remarquons qu'on a pris soin de travailler sur \mathbb{C} et non sur \mathbb{R} pour éviter tout problème créé par une équation polynomiale sans solution réelle, telle $X^2 = 1$.)

3.3 Résolution de systèmes polynomiaux

Un problème qui revient sans cesse dans toutes sortes d'applications est celui de la résolution d'un système polynomial. Il s'agit d'obtenir une description de toutes les solutions dans \mathbb{C}^n d'un système de la forme

$$p_1(x_1, \dots, x_n) = \dots = p_s(x_1, \dots, x_n) = 0.$$

Dans le cas général, un tel système n'a pas un ensemble fini de solutions ; on s'intéressera alors à donner une description paramétrique des solutions.

L'approche par la théorie des bases de Gröbner ne fournit pas la solution la plus efficace, mais certainement l'approche la plus simple pour traiter le cas général et rechercher des expressions exactes pour les solutions, c'est-à-dire en excluant le calcul numérique.

Donnons un exemple : on recherche le lieu et les valeurs des extrema sur la sphère unité $\{(x, y, z) : x^2 + y^2 + z^2 = 1\}$ de l'application polynomiale $(x, y, z) \mapsto x^3 + 2xyz - z^2$. La méthode des multiplicateurs de Lagrange indique que les positions (x, y, z) des extrema vérifient le système polynomial

$$3X^2 + 2YZ = 2\Lambda X, \quad 2XZ = 2\Lambda Y, \quad 2XY - 2Z = 2\Lambda Z, \quad X^2 + Y^2 + Z^2 = 1,$$

pour une nouvelle indéterminée Λ , le multiplicateur de Lagrange.

Nous verrons comment aborder la résolution de tels systèmes par triangularisation.

3.4 Équations implicites d'un lieu géométrique donné par une paramétrisation

Le problème est le suivant : étant donnée une paramétrisation rationnelle

$$x_i = r_i(t_1, \dots, t_m), \quad i = 1, \dots, n,$$

d'un ensemble V de points de \mathbb{C}^n , trouver algorithmiquement un système d'équations polynomiales qui définisse V sans plus faire référence aux t_i (ou du moins le plus petit ensemble algébrique contenant V).

Le prototype de ce problème est celui de la paramétrisation du cercle unité. Partant de la paramétrisation $t \mapsto (x(t), y(t))$ donnée par

$$x = \frac{1-t^2}{1+t^2} \quad \text{et} \quad y = \frac{2t}{1+t^2},$$

il s'agit de calculer la relation implicite $x^2 + y^2 = 1$.

4 Monômes et ordre monomial

Notre premier objectif est de donner une généralisation de la division euclidienne.

Si l'on se souvient du cas d'une indéterminée, on se rappelle qu'il existe en fait deux divisions polynomiales : celle par les puissances décroissantes, qui termine toujours, et une par les puissances croissantes, qui le plus souvent ne termine pas et est en fait mieux adaptée à décrire une division entre séries formelles. Ces deux modes de division sont rattachés à deux ordres sur les exposants entiers des polynômes : respectivement, l'ordre décroissant et l'ordre croissant sur \mathbb{N} . Bien qu'il existe bien d'autres ordres sur \mathbb{N} , ces deux ordres sont les seuls compatibles avec le produit de polynômes, au sens où le « terme de tête », respectivement de plus haut ou de plus petit degré, d'un produit de deux polynômes doit être le produit des termes de têtes de ces deux polynômes.

En plusieurs indéterminées, on rencontre une première différence : toute une variété de ce que l'on va bientôt appeler « ordres monomiaux » est disponible pour définir une division, même en s'imposant de bonnes propriétés de compatibilité avec le produit. Loin d'être une difficulté, on exploitera cette diversité dans les applications.

4.1 Terminologie sur les polynômes

Fixons d'abord notre terminologie sur les polynômes, celle promue par le courant « algébriste », maintenant la plus usitée dans le contexte des bases de Gröbner, et qui a supplanté la terminologie d'abord employée qui avait été introduite par le courant « logicien ».

Un *monôme* m sur des indéterminées X_1, \dots, X_n est un produit (fini) des X_i , éventuellement avec répétitions pour permettre tout exposant entier. Ainsi, m est de la forme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$. Un polynôme p de A_n est donc une combinaison linéaire de monômes à coefficients dans \mathbb{C} . Il s'écrit alternativement sous l'une des formes

$$p = \sum_{\text{finie}} p_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n} \quad \text{et} \quad p = \sum_{j=1}^s c_j m_j$$

pour des monômes m_j et des scalaires $p_{\alpha_1, \dots, \alpha_n}$ et c_j . Plus précisément, $p_{\alpha_1, \dots, \alpha_n}$ est le coefficient de $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ dans p , et c_j celui de m_j dans p . Les termes non nuls de l'une ou l'autre des représentations de p comme somme sont appelés *termes* de p .

4.2 Monoïde des monômes

Il sera commode et fructueux de considérer la structure de l'ensemble des monômes d'un anneau A_n donné. C'est celle d'un « monoïde ».

Un *monoïde* M est un ensemble muni d'une loi interne associative pour laquelle il existe un élément neutre. L'exemple le plus simple est celui de l'ensemble \mathbb{N} des nombres entiers, muni de l'addition usuelle, et avec 0 pour neutre. Une généralisation immédiate est celle de \mathbb{N}^n , avec l'addition terme à terme. La formule d'addition,

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n),$$

reflète l'addition des exposants dans un produit de monômes dans A_n . En fait, les monômes de A_n constituent un monoïde commutatif M , isomorphe au précédent, engendré par les indéterminés X_1, \dots, X_n , ayant pour loi interne le produit usuel de A_n et de neutre $1 = X_1^0 \dots X_n^0$. La loi produit explicite est donnée par

$$(X_1^{a_1} \dots X_n^{a_n}) \times (X_1^{b_1} \dots X_n^{b_n}) = X_1^{a_1+b_1} \dots X_n^{a_n+b_n}.$$

C'est le *monoïde commutatif libre* sur les n générateurs X_1, \dots, X_n , noté $[X_1, \dots, X_n]$.

4.3 Ordres monomiaux et exemples principaux

Définition (Ordre monomial). Un *ordre monomial* sur M est une relation d'ordre strict \prec qui est :

- totale : deux monômes peuvent toujours être comparés ;
- compatible avec le produit : dès lors que $m_1 \prec m_2$, on a $m' m_1 \prec m' m_2$ pour tout m' ;
- un bon ordre : tout ensemble non vide de monômes a un plus petit élément, ou de façon équivalente, toute suite strictement décroissante de monômes termine.

En particulier, pour tout ordre monomial, on a la relation $1 \prec X_i$ pour chaque i . Sinon nous aurions $X_i \prec 1$ pour un certain i , puis de proche en proche $X_i^{k+1} \prec X_i^k$, d'où une suite infinie strictement décroissante. En conséquence, $1 = X_1^0 \dots X_n^0$ est le plus petit élément de M pour tout ordre monomial, car tout monôme m peut être obtenu comme dernier élément d'une chaîne

$$1 \prec X_{i_1} \prec X_{i_1} X_{i_2} \prec \dots \prec X_{i_1} \dots X_{i_r}.$$

Pour la suite, nous adoptons les notations $|\alpha| = \alpha_1 + \dots + \alpha_n$, $X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ et $X^{\alpha+\beta} = X^\alpha X^\beta$ pour tous multi-exposants $\alpha = (\alpha_1, \dots, \alpha_n)$ et $\beta = (\beta_1, \dots, \beta_n)$. On notera \preceq l'ordre large associé à l'ordre strict \prec .

Nous donnons maintenant les exemples principaux de relations d'ordres employées sur des monômes. Pour les besoins de la définition, nous présentons simultanément trois ordres monomiaux et un ordre qui n'est pas un ordre monomial, l'ordre lexicographique renversé.

- *ordre lexicographique* (ordre du dictionnaire) : $X^\alpha \prec_{\text{lex}} X^\beta$ si $\alpha_k < \beta_k$ pour $k = \min\{i : \alpha_i \neq \beta_i\}$, ou autrement dit, si la première valeur non nulle de la suite $\alpha_1 - \beta_1, \alpha_2 - \beta_2, \dots$ est strictement négative.
- *ordre lexicographique gradué* (ordre du degré total raffiné par \prec_{lex}) : $X^\alpha \prec_{\text{grlex}} X^\beta$ si $|\alpha| < |\beta|$ ou $(|\alpha| = |\beta| \text{ et } X^\alpha \prec_{\text{lex}} X^\beta)$.
- *ordre lexicographique renversé* (n'est pas un ordre monomial) : $X^\alpha \prec_{\text{revlex}} X^\beta$ si $\alpha_k > \beta_k$ pour $k = \max\{i : \alpha_i \neq \beta_i\}$, ou autrement dit, si la dernière valeur non nulle de la suite $\alpha_1 - \beta_1, \alpha_2 - \beta_2, \dots$ est strictement positive.
- *ordre lexicographique renversé gradué* (ordre du degré total raffiné par \prec_{revlex}) : $X^\alpha \prec_{\text{grlex}} X^\beta$ si $|\alpha| < |\beta|$ ou $(|\alpha| = |\beta| \text{ et } X^\alpha \prec_{\text{revlex}} X^\beta)$.

Pour tous ces ordres, on vérifie la relation $X_1 \succ X_2 \succ \dots \succ X_n$. Il est aisé de confondre ces différents ordres, aussi donnons-nous explicitement les quelques premiers termes de la suite ordonnée des monômes pour chacun de ces ordres. Il est nécessaire d'avoir au moins trois indéterminées ($n = 3$) et d'aller jusqu'en degré trois pour mettre en évidence les différences entre les ordres.

- *ordre lexicographique* : $1 \prec X_3 \prec X_3^2 \prec X_3^3 \prec \dots \prec X_2 \prec X_2X_3 \prec X_2X_3^2 \prec X_2X_3^3 \prec \dots \prec X_2^2 \prec X_2^2X_3 \prec X_2^2X_3^2 \prec X_2^2X_3^3 \prec \dots \prec X_1 \prec X_1X_3 \prec X_1X_3^2 \prec X_1X_3^3 \prec \dots \prec X_1X_2 \prec X_1X_2X_3 \prec X_1X_2X_3^2 \prec X_1X_2X_3^3 \prec \dots \prec X_1X_2^2 \prec X_1X_2^2X_3 \prec X_1X_2^2X_3^2 \prec X_1X_2^2X_3^3 \prec \dots$
- *ordre lexicographique gradué* : $1 \prec X_3 \prec X_2 \prec X_1 \prec X_3^2 \prec X_2X_3 \prec X_2^2 \prec X_1X_3 \prec X_1X_2 \prec X_1^2 \prec X_3^3 \prec X_2X_3^2 \prec X_2^2X_3 \prec X_2^3 \prec X_1X_3^2 \prec X_1X_2X_3 \prec X_1X_2^2 \prec X_1^2X_3 \prec X_1^2X_2 \prec X_1^3 \prec \dots$
- *ordre lexicographique renversé* : $\dots \prec X_1^3X_2^2X_3 \prec X_1^2X_2^2X_3 \prec X_1X_2^2X_3 \prec X_2^2X_3 \prec \dots \prec X_1^3X_3 \prec X_1^2X_3 \prec X_1X_3 \prec X_3 \prec \dots \prec X_1^3X_2^2 \prec X_1^2X_2^2 \prec X_1X_2^2 \prec X_2^2 \prec \dots \prec X_1^3X_2 \prec X_1^2X_2 \prec X_1X_2 \prec X_2 \prec \dots \prec X_1^3 \prec X_1^2 \prec X_1 \prec 1$.
- *ordre lexicographique renversé gradué* : $1 \prec X_3 \prec X_2 \prec X_1 \prec X_3^2 \prec X_2X_3 \prec X_1X_3 \prec X_2^2 \prec X_1X_2 \prec X_1^2 \prec X_3^3 \prec X_2X_3^2 \prec X_1X_3^2 \prec X_2^2X_3 \prec X_1X_2X_3 \prec X_1^2X_3 \prec X_2^3 \prec X_1X_2^2 \prec X_1^2X_2 \prec X_1^3 \prec \dots$

Encore une fois, l'ordre \prec_{revlex} n'est pas un ordre monomial : il fournit une suite infinie décroissante de monômes. En revanche, les ordres \prec_{lex} , \prec_{grlex} , \prec_{grevlex} sont des ordres monomiaux. Nous laissons la preuve au lecteur. Les ordres monomiaux \prec_{lex} et \prec_{grevlex} seront les plus employés, ainsi que d'autres ordres pondérés et d'élimination de bloc. Pour éviter de renommer les indéterminées, on utilisera la notation $\prec_{\text{lex}(X_{\sigma(1)}, \dots, X_{\sigma(n)})}$, etc. Ainsi par exemple, les ordres $\prec_{\text{lex}(X_1, \dots, X_n)}$ et \prec_{lex} , sont identiques. Par ailleurs, on a pour tous monômes X^α et X^β l'équivalence « $X^\alpha \prec_{\text{revlex}(X_1, \dots, X_n)} X^\beta$ si et seulement si $X^\alpha \succ_{\text{lex}(X_n, \dots, X_1)} X^\beta$ ». Là encore, nous invitons le lecteur à bien se convaincre de ce point technique.

4.4 Coefficients, monômes et termes de tête

Faire choix d'un ordre monomial \prec sur M permet d'associer des monôme, exposant, coefficient et terme distingués à tout polynôme non nul. En raison de la compatibilité d'un ordre monomial avec le produit, ces éléments distingués se comportent bien face au produit.

Plus précisément, le *monôme de tête* (ou *monôme dominant*) d'un polynôme p non nul est le plus grand monôme de coefficient non nul dans p . Il est noté $\text{mt}(p)$. Le *coefficient de tête* (ou *coefficient dominant*) d'un polynôme p non nul est le coefficient noté $\text{ct}(p)$ de son monôme de tête. Le *terme de tête* (ou *terme dominant*) d'un polynôme p non nul est le produit noté $\text{tt}(p)$ de son coefficient de tête par son monôme de tête.

Évidemment, ces notions sont relatives à l'ordre monomial choisi. Donnons l'exemple dans A_3 du polynôme

$$p = -30X_1X_2^2 - 210X_2^2X_3 + 3X_1^2 + 35X_2^2 + 30X_1X_3 - 105X_3^2 + 140X_2X_4 - 21X_5.$$

Son terme de tête est :

- le terme $-30X_1X_2^2$ pour $\text{grevlex}(X_1, \dots, X_5)$ et $\text{grlex}(X_1, \dots, X_5)$,
- le terme $3X_1^2$ pour $\text{lex}(X_1, \dots, X_5)$,
- le terme $-21X_5$ pour $\text{lex}(X_5, \dots, X_1)$.

Faisons maintenant le lien avec le produit. Par définition d'un ordre monomial, le monôme de tête d'un produit de deux polynômes p et q est le produit des monômes de tête $\text{mt}(p)$ et $\text{mt}(q)$. En effet, notons $p = c_0m_0 + \dots + c_r m_r$ et $q = c'_0m'_0 + \dots + c'_s m'_s$ pour deux suites de coefficients non nuls c_i et c'_i et deux suites strictement décroissantes de monômes m_i et m'_i . (En particulier, $c_0 = \text{ct}(p)$, $m_0 = \text{mt}(p)$, et on a les relations analogues pour q .) Ainsi,

$$pq = \sum_{i=0}^r \sum_{j=0}^s c_i m_i c'_j m'_j = \sum_{i=0}^r \sum_{j=0}^s c_i c'_j m_i m'_j.$$

Or, on a $m_i \preceq m_0$ et $m'_j \preceq m'_0$, d'où $m_i m'_j \preceq m_0 m'_j$ et $m_0 m'_j \preceq m_0 m'_0$, et donc $m_i m'_j \preceq m_0 m'_0$. L'égalité ne peut avoir lieu que si $i = j = 0$, ce qui prouve le résultat. Au passage, on a aussi montré que les coefficients de tête se multiplient, de même que les termes de tête.

Cette propriété sur les monômes de tête est à la base de toute la théorie commutative des bases de Gröbner et persiste dans presque tous les cas de généralisations à des cadres non commutatifs. Une variation importante sera celle d'algèbres « tordues » dans lesquelles coefficients et indéterminées ne commutent pas librement, chaque produit $m_i c'_j$ se réécrivant comme un polynôme de monôme de tête m_i , plus forcément réduit à un seul monôme et dont le coefficient de tête ne sera plus forcément c'_j . Dans ces variations, la propriété sur les monômes de tête sera préservée, mais pas celles sur coefficients et termes de tête.

5 Réduction et division en plusieurs indéterminées

La division euclidienne d'un polynôme f en une seule indéterminée X par un polynôme g non nul en la même indéterminée exprime f sous la forme $qg + r$ pour des polynômes q et r tel que r ait degré inférieur à g . Le reste r est l'unique représentant de la classe de f modulo l'idéal $A_1 g$ ayant cette propriété de degré, et l'on peut dire que l'on a divisé f par l'idéal $A_1 g$. Dans le cas d'un anneau de polynômes en plusieurs indéterminées, dans lequel les idéaux ne sont plus nécessairement principaux, il est donc naturel d'autoriser une division par toute une famille de diviseurs g_1, \dots, g_s , l'objectif étant donc d'exprimer f sous la forme $q_1 g_1 + \dots + q_s g_s + r$.

5.1 Réduction

Algorithmiquement, la division euclidienne procède par une succession de « divisions élémentaires », où l'on ne considère que des quotients q qui sont des monômes et donc des restes r qui ne sont pas minimaux au sens du degré. Dans le cas de plusieurs indéterminées, ces étapes sont appelées « réductions ».

On fixe un ordre monomial sur un anneau de polynômes A_n . Un polynôme f non nul de A_n est dit *réductible* par un polynôme g non nul de A_n si $\text{mt}(g)$ divise $\text{mt}(f)$ dans A_n . Un polynôme f non nul de A_n est dit *réductible* par une famille $\{g_i\}_{i \in \{1, \dots, s\}}$ de polynômes non nuls de A_n si f est réductible par l'un des g_i dans A_n .

En une unique indéterminée, f est réductible par g si et seulement si $\deg f \geq \deg g \geq 0$. En plusieurs indéterminées, remarquons que la notion de divisibilité d'un monôme m par un monôme m' n'est pas équivalente à la relation d'ordre $m' \preceq m$.

Lorsqu'un polynôme est réductible, on va pouvoir le « réduire ». *Réduire* un polynôme f non nul de A_n par un polynôme g non nul de A_n , c'est remplacer f par $f' = f - cmg$ pour $m = \text{mt}(f)/\text{mt}(g)$ et $c \in \mathbb{C}$ de façon que $f' = 0$ ou que $\text{mt}(f') \prec \text{mt}(f)$. Autrement dit, c'est remplacer f par $f' = f - tg$ pour $t = \text{tt}(f)/\text{tt}(g)$. *Réduire* un polynôme f non nul de A_n par une famille $\{g_i\}_{i \in \{1, \dots, s\}}$ de polynômes non nuls de A_n , c'est réduire f par un des g_i convenable. Notons dès à présent que rien n'impose le choix de i dans les cas d'ambiguïté ou plusieurs g_i permettent la réduction.

5.2 Division en plusieurs indéterminées

Diviser un polynôme f non nul de A_n par un polynôme g non nul de A_n , respectivement par une famille $\{g_i\}_{i \in \{1, \dots, s\}}$ de polynômes non nuls de A_n , c'est le réduire autant de fois que nécessaire jusqu'à aboutir à un polynôme irréductible par g , respectivement par la famille $\{g_i\}_{i \in \{1, \dots, s\}}$.

On l'a fait observer, divisibilité et ordre ne sont pas des notions équivalentes. Il se peut même qu'un polynôme f ne soit pas réductible par un polynôme g mais qu'un terme de f , autre que le terme de tête, soit lui réductible par g . L'algorithme qui suit propose une division qui renvoie un reste dont tous les termes sont irréductibles.

Algorithme (Division en plusieurs indéterminées).

ENTRÉE : un polynôme f et des polynômes non nuls g_1, \dots, g_s

SORTIE : des polynômes r, q_1, \dots, q_s tels que $f = q_1g_1 + \dots + q_sg_s + r$ et tel qu'aucun monôme de r ne soit réductible par $\{g_i\}_{i \in \{1, \dots, s\}}$

1. $r \leftarrow 0$; pour i de 1 à s , faire $q_i \leftarrow 0$
2. tant que $f \neq 0$, faire
 - si $\text{mt}(g_i)$ divise $\text{mt}(f)$ pour un certain i , choisir un tel i et faire $q_i \leftarrow q_i + \text{tt}(g_i)^{-1} \text{tt}(f)$ et $f \leftarrow f - \text{tt}(g_i)^{-1} \text{tt}(f)g_i$
 - sinon, faire $r \leftarrow r + \text{tt}(f)$ et $f \leftarrow f - \text{tt}(f)$
3. renvoyer r, q_1, \dots, q_s

Correction et terminaison de l'algorithme. La procédure qui précède est correcte, car elle respecte l'invariant $f = q_1g_1 + \dots + q_sg_s + r$ sur les variables du calcul et s'arrête lorsque f est nul et après n'avoir accumulé dans r que des monômes irréductibles. Elle termine pour un ordre monomial car le monôme $\text{mt}(f)$ décroît strictement à chaque passage dans la boucle « tant que » et puisqu'il ne peut y avoir de suite infinie décroissante de monômes pour un ordre monomial. \square

Elle n'est cependant pas déterministe, en conséquence du choix laissé sur i pour chaque réduction. Ce non déterminisme de la division s'observe bien sur l'exemple suivant, où l'on donne deux divisions pour l'ordre monomial $\text{lex}(X, Y)$ de $f = \underline{X^2Y} + XY^2 + Y^2$ par la famille constituée de $g_1 = XY - 1$ et de $g_2 = Y^2 - 1$. (Par commodité, on a souligné les monômes de tête.) En réduisant deux fois successives par g_1 , on a la division

$$\begin{aligned}
 (\underline{X^2Y} + XY^2 + Y^2) + 0 \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
 &= (\underline{XY^2} + X + Y^2) + X \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
 &= (\underline{X} + Y^2 + Y) + (X + Y) \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
 &= (\underline{Y^2} + Y) + (X + Y) \times (XY - 1) + 0 \times (Y^2 - 1) + X \\
 &= (\underline{Y} + 1) + (X + Y) \times (XY - 1) + 1 \times (Y^2 - 1) + X, \\
 &= \underline{1} + (X + Y) \times (XY - 1) + 1 \times (Y^2 - 1) + (X + Y), \\
 &= 0 + (X + Y) \times (XY - 1) + 1 \times (Y^2 - 1) + (X + Y + 1),
 \end{aligned}$$

qui renvoie le résultat

$$q_1 = X + Y, \quad q_2 = 1, \quad r = X + Y + 1.$$

En réduisant d'abord une seule fois par g_1 , puis une autre fois par g_2 , on a la division

$$\begin{aligned}
 (\underline{X^2Y} + XY^2 + Y^2) + 0 \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
 &= (\underline{XY^2} + X + Y^2) + X \times (XY - 1) + 0 \times (Y^2 - 1) + 0 \\
 &= (\underline{2X} + Y^2) + X \times (XY - 1) + X \times (Y^2 - 1) + 0 \\
 &= \underline{Y^2} + X \times (XY - 1) + X \times (Y^2 - 1) + 2X \\
 &= \underline{1} + X \times (XY - 1) + (X + 1) \times (Y^2 - 1) + 2X, \\
 &= 0 + X \times (XY - 1) + (X + 1) \times (Y^2 - 1) + (2X + 1),
 \end{aligned}$$

qui renvoie le résultat

$$q_1 = X, \quad q_2 = X + 1, \quad r = 2X + 1.$$

Ni l'ordre des calculs, ni les quotients, ni les restes finaux ne sont identiques d'un calcul à l'autre.

6 Escaliers, définition et existence des bases de Gröbner

Les bases de Gröbner que nous allons définir sont des systèmes de générateurs d'idéaux de polynômes ayant de bonnes propriétés vis-à-vis de la réduction et de la division. Notamment, un premier point est de comprendre quels monômes peuvent être réduits à l'aide d'un polynôme

donné. Ceci va être fait à l'aide de la notion de « partie stable » du monoïde des monômes, aussi appelés « escalier » en référence à sa représentation picturale. On verra qu'à tout système de générateurs d'un idéal est associé un escalier et qu'une base de Gröbner est essentiellement un système qui colle le mieux à l'escalier intrinsèque de l'idéal.

6.1 Parties stables du monoïde des monômes

Pour tout monoïde commutatif M , une *partie stable* S est un sous-ensemble de M clos par produit par tout élément de M . Cette définition est formellement très proche de celle d'un idéal, si ce n'est que l'ensemble de référence est maintenant un monoïde (muni d'une seule loi interne) et non un anneau (muni de deux lois internes); c'est pourquoi la notion de partie stable est aussi connue sous le vocable de « monoïdéal ».

De façon analogue aux idéaux donnés par générateurs, étant donnée une famille $\{s_i\}_{i \in I}$ d'éléments de M , l'ensemble

$$S = \{ms_i \in M : m \in M, i \in I\} = \bigcup_{i \in I} Ms_i$$

est une partie stable du monoïde M , appelée la partie stable de M engendrée par la famille de générateurs s_i . Toute partie stable peut être vue comme engendrée par une famille de générateurs et encore une fois, la question est de comprendre si une partie stable peut être présentée comme engendrée par un nombre fini de générateurs.

Dans le cas du monoïde $[X, Y]$, on obtient une représentation en escaliers des parties stables de la façon suivante. Chaque monôme $m = X^a Y^b$ est représenté par le point de coordonnées entières (a, b) de \mathbb{N}^2 . Pour un monôme fixé $s = X^{a_0} Y^{b_0}$, la partie stable Ms engendrée par s est ainsi représentée par les points entières (a, b) tels que $a \geq a_0$ et $b \geq b_0$, c'est-à-dire par un quadrant issu de (a_0, b_0) . Une partie stable générale étant une union de parties stables de la forme Ms , elle est représentée par une union de quadrant de \mathbb{N}^2 , dont les coins sont disposés le long d'une forme en escalier.

Rappelons encore une fois l'axiome fondamental à la base de la théorie des bases de Gröbner : le monôme de tête d'un produit, $\text{mt}(fg)$, est le produit des monômes de tête $\text{mt}(f)\text{mt}(g)$. Il s'ensuit que la collection des monômes de tête des éléments non nuls de l'idéal est une partie stable : si un monôme s est dans cette partie, c'est qu'il existe un élément f de l'idéal de monôme de tête s ; pour tout monôme m , le polynôme mf est dans l'idéal et a sm pour monôme de tête. Pour un idéal I , nous noterons $\text{mt}(I)$ la partie stable associée : $\text{mt}(I) = \{\text{mt}(p) : p \in I \setminus \{0\}\}$.

6.2 Définition des bases de Gröbner

Étant donnée une famille finie $\{g_i\}_{i \in \{1, \dots, s\}}$ de polynômes non nuls de A_n , deux parties stables jouent un rôle particulier. Tout d'abord, la partie stable $\text{mt}(I)$ associée à l'idéal $I = \sum_{i=1}^s A_n g_i$, c'est-à-dire l'ensemble des monômes de tête de toutes les combinaisons non nulles $q_1 g_1 + \dots + q_s g_s$ pour des polynômes q_i . D'autre part, la partie stable constituée des monômes de tête de tous les polynômes réductibles par la famille $\{g_i\}_{i \in \{1, \dots, s\}}$, autrement dit, l'ensemble des monômes de tous des produits qg_i pour un polynôme q non nul.

Par construction, la première partie stable, $\text{mt}(I)$, contient toujours la seconde, mais l'égalité n'est pas vérifiée sur tout système de générateurs d'un idéal donné. Considérons l'exemple suivant. On munit $A = \mathbb{C}[X, Y]$ de l'ordre monomial $\text{lex}(Y, X)$. Les deux polynômes $\underline{XY^3} - 1$ et $\underline{X^3Y} + 1$ ne peuvent réduire que la partie stable

$$MXY^3 \cup MX^3Y,$$

alors que la partie stable associée à tout l'idéal I qu'ils engendrent est

$$\text{mt}(I) = MY \cup MX^8.$$

Nous l'affirmons pour le moment sans pouvoir donner de preuve, mais on se convainc au moins de l'inclusion $\text{mt}(I) \supseteq MY \cup MX^8$ quand on observe l'égalité

$$I = A(\underline{Y} + X^5) + A(\underline{X}^8 + 1).$$

Ce phénomène motive la définition suivante.

Théorème-Définition. Soit I un idéal de $A_n = \mathbb{C}[X_1, \dots, X_n]$ et \prec un ordre monomial sur A_n . Un sous-ensemble fini G de $I \setminus \{0\}$ est une *base de Gröbner de I pour l'ordre \prec* si l'une quelconque des propriétés équivalentes est vérifiée :

1. la partie stable de M engendrée par $\text{mt}(G)$ est égale à $\text{mt}(I)$;
2. $\text{mt}(G)$ et $\text{mt}(I)$ engendrent le même idéal ;
3. tout f non nul de I est réductible par G ;
4. pour tout f dans A_n , il existe un unique r dans A_n dont aucun monôme ne soit divisible par un monôme de $\text{mt}(G)$ et tel que $f - r$ soit dans l'idéal I ;
5. pour tout f dans I , le reste de la division de f par G est nul.

Démonstration. Faisons une preuve (presque) circulaire.

1 \Rightarrow 2. Supposons que

$$\bigcup_{g \in G} M \text{mt}(g) = \text{mt}(I).$$

Passons alors aux idéaux. En notant (S) pour signifier l'idéal de A_n engendré par la famille $\{s\}_{s \in S}$, on a les égalités :

$$(\text{mt}(I)) = \sum_{g \in G} (M \text{mt}(g)) = \sum_{g \in G} (\text{mt}(g)) = (\text{mt}(G)).$$

On a prouvé que $\text{mt}(G)$ et $\text{mt}(I)$ engendrent le même idéal.

2 \Rightarrow 3. Supposons $(\text{mt}(G)) = (\text{mt}(I))$. Soit $f \in I \setminus \{0\}$. On a d'abord l'égalité

$$\text{mt}(f) = \sum_{g \in G} q_g \text{mt}(g)$$

pour des polynômes q_g , puis, en scindant en monômes, l'égalité

$$\text{mt}(f) = \sum_j c_j m_j \text{mt}(g_j)$$

pour des c_j de \mathbb{C} , des monômes m_j et des g_j de G . Comme cette somme sur j est en fait une somme de terme, les termes en les monômes autres que $\text{mt}(f)$ doivent s'annuler, et on peut sans perte de généralité supposer que pour chaque j , $m_j \text{mt}(g_j) = \text{mt}(f)$. On a alors, pour j_0 l'un de ces j ,

$$\text{mt}(f) = m_{j_0} \text{mt}(g_{j_0}).$$

Donc f est réductible par G .

3 \Rightarrow 4. Supposons que tout f non nul de I est réductible par G . Soit $f \in A$. On a l'existence énoncée au point (4) en prenant pour r le reste de la division de f par g : alors, $f - r$ est élément de I . Supposons que nous ayons deux écritures $f = h_i + r_i$, pour $i \in \{1, 2\}$, avec $h_i \in I$ et des r_i dont aucun des monômes n'est divisible par un monôme de $\text{mt}(G)$. Alors, l'élément

$$r_1 - r_2 = h_2 - h_1 \in I$$

est soit nul, soit réductible. Supposons cette différence non nulle ; alors $\text{mt}(r_1 - r_2)$ est forcément un monôme parmi ceux de r_1 et r_2 . Ce monôme de tête est à la fois non divisible par un monôme de $\text{mt}(G)$, par définition des r_i , et divisible par l'un d'entre eux, par l'hypothèse faite du point (3). C'est une contradiction, et on a l'unicité de r .

4 \Rightarrow 5. Soit $f \in I$. En application du point (4), on trouve un r , qui par la preuve d'existence et d'unicité précédente ne peut être que le reste de la division de f par G . Comme $r = (r - f) + f$ est élément de I mais n'est pas réductible, c'est que r est nul.

5 \Rightarrow 2. Soit f réductible par G . Alors $\text{mt}(f)$ est dans la partie stable engendrée par $\text{mt}(G)$, donc dans l'idéal engendré par $\text{mt}(G)$. Supposons le point (5). Comme tout élément non nul de I est alors réductible par G , on a obtenu dans ce cas l'inclusion

$$(\text{mt}(I)) \subseteq (\text{mt}(G)) ;$$

l'autre inclusion découle de $G \subseteq I$.

2 \Rightarrow 1. L'inclusion de la partie stable S engendrée par $\text{mt}(G)$ dans $\text{mt}(I)$ découle de ce que $G \subseteq I$. Pour l'autre inclusion, supposons le point (2) et soit $m \in \text{mt}(I) \subseteq (\text{mt}(I)) = (\text{mt}(G))$. Par le même raisonnement que pour l'implication 2 \Rightarrow 3, on écrit m sous la forme $m_{j_0} \text{mt}(g_{j_0})$, qui est un élément de S . La partie stable $\text{mt}(I)$ est donc incluse dans S . \square

Remarquons que le polynôme r du point (4) du théorème précédant n'est autre que le reste de la division de f par G .

Sur un point de terminologie, notons que le terme de « base de Gröbner » est malheureux, puisqu'une base de Gröbner n'est pas une base, mais seulement un système de générateurs d'un idéal : une fois fixée une base de Gröbner $\{g_1, \dots, g_s\}$ d'un idéal I donné, il n'y a en général pas unicité de l'écriture d'un élément de I comme combinaison des g_i , puisqu'il existe en général des combinaisons nulles des g_i .

Enfin, on peut toujours remplacer un élément d'une base de Gröbner par le reste de sa division par les autres éléments. Nous laissons la vérification de ce point au lecteur.

6.3 Lemme de Dickson et existence des bases de Gröbner

À ce stade, rien n'indique que des bases de Gröbner puissent exister pour tout idéal d'un anneau A_n et tout ordre monomial. La contrainte limitante est la finitude imposée par la définition : sans elle, il suffirait de prendre $I \setminus \{0\}$ comme système de générateurs de I . Cette existence repose sur la structure finie des parties stables, donnée par le lemme suivant. Encore une fois, la partie stable $\text{mt}(I)$ est en bon invariant de I , à ordre monomial fixé.

Lemme (de Dickson). Toute partie stable S de $M = [X_1, \dots, X_n]$ est finiment engendrée.

Démonstration. On fait une preuve par récurrence sur n .

Le cas $n = 1$ est immédiat : prendre l'élément de S de degré minimal ; celui-ci engendre S .

Supposons démontré le cas de $[X_1, \dots, X_n]$ et soit S une partie stable de $M = [X_1, \dots, X_n, Y]$. Considérons S' , obtenue en faisant $Y = 1$ dans S . C'est une partie stable de $M' = [X_1, \dots, X_n]$; elle est donc finiment engendrée par des éléments $X^{\alpha_1}, \dots, X^{\alpha_s}$. Il en est de même pour chaque partie stable S'_j de M' donnée par $S'_j = \{m \in M' : mY^j \in S\}$: S'_j est finiment engendrée par des éléments $X^{\alpha_{1,j}}, \dots, X^{\alpha_{s_j,j}}$. Sans perte de généralité, on peut se donner un entier m tel que tous les $X^{\alpha_i} Y^m$ sont dans S . On vérifie aisément que la partie stable (finiment) engendrée par les $X^{\alpha_{i,j}} Y^j$ pour $j < m$ et par les $X^{\alpha_i} Y^m$, tels que définis ci-dessus, n'est autre que S . \square

Nous pouvons maintenant énoncer le théorème d'existence des bases de Gröbner.

Corollaire. Pour tout ordre monomial \prec sur $A_n = \mathbb{C}[X_1, \dots, X_n]$, tout idéal I non nul de A_n admet une base de Gröbner.

Démonstration. Soit I un idéal non nul de A_n . Par le lemme de Dickson, il existe un système fini de générateurs de $\text{mt}(I)$. Considérons un relèvement de ce système en un système d'éléments de I . Par la première définition des bases de Gröbner (par l'égalité des parties stables), celui-ci s'avère être une base de Gröbner de I pour \prec . \square

7 Applications de la théorie des bases de Gröbner

7.1 Théorème de Hilbert et noethérianité des anneaux de polynômes

L'existence des bases de Gröbner donne la réponse constructive suivante à la question de la finitude de la présentation des idéaux polynomiaux.

Corollaire (Théorème de Hilbert). Tout idéal I de $A_n = \mathbb{C}[X_1, \dots, X_n]$ admet un système fini de générateurs, ou, de façon équivalente, toute chaîne infinie croissante (pour l'inclusion) d'idéaux de A_n stationne.

Démonstration. Toute base de Gröbner est un système fini de générateurs, ce qui prouve le premier point. Pour l'équivalence annoncée, supposons d'abord que toute chaîne infinie croissante d'idéaux de A_n stationne. Étant donné un idéal I qui ne soit pas finiment engendré, nous pouvons trouver une suite infinie d'éléments dont chaque terme n'est pas dans l'idéal engendré par la sous-suite finie des termes précédents. On produit ainsi une suite infinie strictement croissante d'idéaux, ce qui contredit l'hypothèse. Ainsi, tout idéal est finiment engendré. Réciproquement, supposons que tout idéal soit finiment engendré et donnons-nous une chaîne infinie croissante d'idéaux. L'union de tous ces idéaux est un nouvel idéal, qui est donc finiment engendré. Soit un système fini de générateurs de l'union ; il existe un idéal de la chaîne qui contient tous ces générateurs. Cet idéal, de même que tous les suivants dans la chaîne, est égal à l'union. \square

Nous donnons maintenant une autre preuve de ce résultat, laquelle est formellement très analogue à celle du lemme de Dickson.

Autre démonstration directe. On fait une preuve par récurrence sur n .

Le cas $n = 1$ est immédiat : prendre un élément de I de degré minimal ; celui-ci engendre I .

Supposons démontré le cas de A_n et soit I un idéal de $A_n[Y] = \mathbb{C}[X_1, \dots, X_n, Y]$, qui n'est autre que A_{n+1} après avoir posé $Y = X_{n+1}$. Considérons I' , obtenu comme l'ensemble des coefficients de plus haut degré en Y des éléments non nuls de I , auxquels on adjoint 0. C'est un idéal de A_n ; il est donc finiment engendré par des éléments $\alpha_1, \dots, \alpha_s$ qui correspondent respectivement à des éléments $a_i = \alpha_i Y^{d_i} + \dots$ de I . Il en est de même pour chaque idéal I'_j de A_n donné comme l'ensemble des coefficients de plus haut degré en Y des éléments de I de degré j en Y , auxquels on adjoint 0 : I'_j est finiment engendré par des éléments $\alpha_{1,j}, \dots, \alpha_{s_j,j}$ qui correspondent respectivement à des éléments $a_i = \alpha_i Y^j + \dots$ de I . La suite des I'_j est une suite croissante d'idéaux de A_n , comme on le vérifie par une multiplication par Y , donc stationnaire par l'hypothèse de récurrence. De plus, chaque I'_j est inclus dans I' . On vérifie aisément que l'idéal (finiment) engendré par les $a_{i,j}$ pour $j < m$ et par les a_i , tels que définis ci-dessus, n'est autre que I , en vérifiant que ces éléments réduisent tout élément de I à zéro. \square

La famille des $a_{i,j}$ et des a_i produite par la preuve qui précède est une base de Gröbner de I .

Plus généralement, on dit qu'un anneau A est *noethérien* lorsque tout idéal I de A admet un système fini de générateurs, ou, de façon équivalente, lorsque toute chaîne infinie croissante (pour l'inclusion) d'idéaux de A stationne.

7.2 Problème d'appartenance à un idéal

L'algorithme de division précédemment présenté retourne à la fois un reste et des quotients qui expriment un polynôme initial en terme d'une famille de diviseurs donnés. Dans bien des applications, les quotients explicites sont inutiles et seul le reste compte. Pour ce cas — et en fait pour l'algorithme de Buchberger qui sera vu ultérieurement —, on modifie l'algorithme de division en oubliant de traiter les quotients, ce qui aboutit à l'algorithme de réduction suivant. (La réduction est ici dite « totale » par opposition à la notion de réductibilité jusqu'alors présentée, qui ne concerne que le monôme de tête ; une autre terminologie parle de « réduction en tête » pour ce que nous avons appelé « réduction » et réserve « réduction » pour notre « réduction totale ».)

Algorithme (Réduction totale).

ENTRÉE : un polynôme f et des polynômes non nuls g_1, \dots, g_s

SORTIE : un polynôme r dont aucun monôme ne soit réductible par $\{g_i\}_{i \in \{1, \dots, s\}}$ et pour lequel il existe des polynômes q_1, \dots, q_s tels que $f = q_1g_1 + \dots + q_sg_s + r$

1. $r \leftarrow 0$
2. tant que $f \neq 0$, faire
 - si $\text{mt}(g_i)$ divise $\text{mt}(f)$ pour un certain i , choisir un tel i et réduire f par g_i , c'est-à-dire faire $f \leftarrow f - \text{tt}(g_i)^{-1} \text{tt}(f)g_i$
 - sinon, faire $r \leftarrow r + \text{tt}(f)$ et $f \leftarrow f - \text{tt}(f)$
3. renvoyer r

Lorsque G est une base de Gröbner, cette procédure est une procédure de mise sous forme canonique des classes de polynômes modulo $I = \sum_{i=1}^s A_n g_i$, les éléments du quotient A_n/I . En effet, une classe γ , donnée d'abord par un représentant f , se voit associer un nouveau représentant r unique (pour un choix fixé d'ordre monomial) avec la propriété que r est nul si et seulement si f est dans I , c'est-à-dire si et seulement si la classe γ est nulle.

En particulier, on peut donner un test algorithmique d'appartenance d'un polynôme f à un idéal donné présenté par un système fini de générateurs g_1, \dots, g_s : il suffit de tester la nullité du reste de f par réduction, ce qui est résumé comme suit.

Algorithme (Test d'appartenance à un idéal polynomial).

ENTRÉE : un polynôme f et des polynômes non nuls p_1, \dots, p_r engendrant un idéal I

SORTIE : une valeur booléenne indiquant si f est élément de I

1. choisir un ordre monomial \prec sur $M = [X_1, \dots, X_n]$
2. calculer une base de Gröbner $G = \{g_1, \dots, g_s\}$ de I pour cet ordre
3. effectuer la réduction de p par G
4. si le reste est nul, répondre VRAI, sinon répondre FAUX

7.3 Élimination et résolution de systèmes polynomiaux

La richesse de la théorie des bases de Gröbner provient de son lien avec l'« élimination polynomiale », c'est-à-dire, étant donnés des polynômes p_1, \dots, p_r , avec le problème de la recherche d'une combinaison $f = q_1p_1 + \dots + q_rp_r$ des p_i pour des coefficients polynomiaux q_i telle que f ne fasse pas intervenir certaines indéterminées fixées à l'avance.

Ce problème a une reformulation en termes d'idéaux, puisqu'on montre aisément que l'intersection d'un idéal I de $A_n = \mathbb{C}[X_1, \dots, X_n]$ avec le sous-anneau $A_{n,k} = \mathbb{C}[X_{k+1}, \dots, X_n]$ est un idéal de $A_{n,k}$. Une question algorithmique naturelle est donc de rechercher une base de Gröbner de l'intersection à partir des p_i . Le résultat est le suivant.

Théorème. Soit I un idéal de $A_n = \mathbb{C}[X_1, \dots, X_n]$ et G une base de Gröbner de I pour l'ordre lexicographique sur les monômes de A_n . Soit encore k un entier entre 1 et $n-1$ inclus. Notons $A_{n,k}$ le sous-anneau $\mathbb{C}[X_{k+1}, \dots, X_n]$ et $I_{n,k}$ l'idéal $I \cap A_{n,k}$. Alors, l'ensemble des éléments de G qui ne font intervenir aucun des X_i pour $i \leq k$ est une base de Gröbner de $I_{n,k}$ pour l'ordre monomial lexicographique induit sur $A_{n,k}$ par celui de A_n .

Démonstration. Observons qu'appartenir à $A_{n,k}$ sans être nul est équivalent à avoir un monôme de tête en X_{k+1}, \dots, X_n . La preuve découle ensuite de la dernière définition des bases de Gröbner (par la nullité des restes de la division par base de Gröbner). \square

Géométriquement, $V(I \cap A_{n,k})$ est donné par l'image de $V(I)$ par la projection de \mathbb{C}^n sur ses $n-k$ dernières composantes. Précisément, c'est la clôture pour la topologie de Zariski de cette image, c'est-à-dire le plus petit ensemble algébrique contenant cette image.

En vue des applications, intéressons-nous maintenant à la forme d'une base de Gröbner pour l'ordre lexicographique. En triant ses éléments par ordre monomial décroissant des monômes de tête, on obtient un système de forme triangulaire, ou tout au moins de la forme échelonnée

$$\begin{aligned}
 g_1(x_1, x_2, \dots, x_n) &= 0, \\
 &\vdots \\
 g_{s_1}(x_1, x_2, \dots, x_n) &= 0, \\
 g_{s_1+1}(x_2, \dots, x_n) &= 0, \\
 &\vdots \\
 g_{s_2}(x_2, \dots, x_n) &= 0, \\
 &\vdots \\
 g_{s_{n-1}+1}(x_n) &= 0, \\
 &\vdots \\
 g_{s_n}(x_n) &= 0,
 \end{aligned} \tag{2}$$

où $s_k = r_1 + \dots + s_k$ pour des entiers positifs r_ℓ (éventuellement nuls). Encore une fois, ce résultat provient de l'équivalence entre appartenir à $A_{n,k}$ sans être nul et avoir un monôme de tête en X_{k+1}, \dots, X_n .

Étant donné un algorithme pour la résolution d'une équation polynomiale d'une indéterminée en ses solutions complexes. On obtient ainsi l'algorithme suivant pour donner toutes les solutions dans \mathbb{C}^n d'un système d'équations polynomiales lorsque celui-ci n'a que des solutions isolées.

Algorithme (Résolution d'un système polynomial à solutions toutes isolées).

ENTRÉE : un système d'équations polynomiales $p_1(x_1, \dots, x_n) = \dots = p_s(x_1, \dots, x_n) = 0$

SORTIE : la famille des solutions dans \mathbb{C}^n ou l'exception « existence de solutions non-isolées »

1. Calculer une base de Gröbner de l'idéal engendré par les p_i pour l'ordre lexicographique et la mettre sous la forme échelonnée (2)
2. Si r_n est nul, renvoyer « existence de solutions non-isolées »
3. Considérer le P.G.C.D. des polynômes $g_{s_{n-1}+1}, \dots, g_{s_n}$
4. Le résoudre en des racines $\alpha_1, \dots, \alpha_t$
5. Pour i de 1 à n :
 - (a) Évaluer la forme échelonnée en $x_n = \alpha_i$
 - (b) Résoudre récursivement en x_1, \dots, x_{n-1}
 - (c) En cas de solutions non-isolées, renvoyer « existence de solutions non-isolées »
6. Renvoyer la collection des $(\gamma_1, \dots, \gamma_{n-1}, \alpha_i)$ pour chaque solution $(\gamma_1, \dots, \gamma_{n-1})$ obtenue à l'étape (b) lors de la i -ème itération de la boucle 5.

Remarquons que dans le cas où une exception est renvoyée, il serait possible de donner une preuve d'existence de solutions non-isolées.

À chaque spécialisation d'une indéterminée par un zéro d'un polynôme, on est amené à recalculer une base de Gröbner. Cet algorithme n'est donc pas un moyen économique pour résoudre.

7.4 Élimination et équations implicites

Redonnons explicitement le problème de la recherche d'équations implicites définissant un lieu géométrique donné par une paramétrisation. Étant donnée une paramétrisation rationnelle

$$x_i = r_i(t_1, \dots, t_m), \quad i = 1, \dots, n,$$

d'un ensemble de points de \mathbb{C}^n , il s'agit de trouver un système d'équations polynomiales qui définisse le plus petit ensemble algébrique qui le contienne.

La méthode consiste à éliminer les indéterminées T_i de l'écriture polynomiale (sans fractions) des équations tout en évitant les pôles des fractions rationnelles r_i . On notera particulièrement dans l'algorithme qui suit l'introduction d'une nouvelle indéterminée U dont le rôle est d'interdire l'annulation des dénominateurs des r_i .

Algorithme (Mise sous forme implicite d'une paramétrisation).

ENTRÉE : les fractions $r_i = p_i/q_i$, en les T_1, \dots, T_m , pour $1 \leq i \leq n$

SORTIE : système d'équations algébriques implicites décrivant le plus petit ensemble algébrique contenant l'image de la paramétrisation

1. Choisir un ordre monomial \prec sur $M = [X_1, \dots, X_n, T_1, \dots, T_m, U]$ qui élimine U et les T_i (par exemple, $\text{lex}(T, T_1, \dots, T_m, X_1, \dots, X_n)$)
2. Calculer pour cet ordre une base de Gröbner de l'idéal engendré par les polynômes $q_i(T_1, \dots, T_m)X_i - p_i(T_1, \dots, T_m)$ et par $Uq_1(T_1) \dots q_m(T_m) - 1$
3. En retirer les polynômes qui font intervenir U ou l'un des T_i et renvoyer la famille ainsi obtenue

Donnons un exemple montrant la nécessité de la variable ajoutée U et explicitant ainsi mieux son rôle. Considérons la nappe paramétrique donnée par la paramétrisation

$$x = \frac{s^2}{t}, \quad y = \frac{t^2}{s}, \quad z = s.$$

Un calcul sans introduire U et le polynôme $STU - 1$ renvoie le polynôme $Z(X^2Y - Z^3)$, dont le lieu géométrique des zéros est l'union de l'hypersurface \mathcal{S} d'équation $x^2y = z^3$ et de l'hyperplan \mathcal{H} d'équation $z = 0$. Cependant, pour qu'une solution soit sur l'hyperplan \mathcal{H} , il est nécessaire que le paramètre s soit nul, donc ne permette pas de définir une valeur de y . La nappe paramétrique est donc tracée toute entière sur \mathcal{S} et le polynôme obtenu, $Z(X^2Y - Z^3)$, n'est pas minimal. En reprenant le calcul en ajoutant le polynôme $STU - 1$, on obtient le polynôme $X^2Y - Z^3$ qui ne décrit que l'hypersurface \mathcal{S} . Bien que les deux droites données respectivement par $x = 0, z = 0$ et par $y = 0, z = 0$ soient dans cette hypersurface sans être sur la nappe, il n'est pas possible de donner une équation algébrique valide pour toute la nappe mais qui exclue ces deux droites : le polynôme $X^2Y - Z^3$ est irréductible dans $\mathbb{C}[X, Y, Z]$ puisqu'il est de degré 1 en Y .

Deuxième partie : Algorithme de Buchberger

8 Saturation des escaliers et algorithme naïf

On l'a vu, la question des bases de Gröbner revient à faire coïncider deux escaliers : l'un associé à l'idéal, unique une fois un ordre monomial choisi, un autre qui dépend du système de générateurs considéré, qui correspond en général à une partie stable plus petite que celle associée à l'idéal. Le calcul d'une base de Gröbner va reposer sur une technique de saturation visant à accroître la partie stable donnée par les générateurs, quitte à faire un changement de système de générateurs. L'outil qui va permettre cette saturation est appelé « S -polynôme ». Le calcul d'une base de Gröbner par l'algorithme de Buchberger se résumera ensuite essentiellement à une itération tant qu'il sera possible de produire de nouveaux S -polynômes.

8.1 S -polynômes et relation avec les bases de Gröbner

Un exemple simple motive la définition qui va suivre : soit I l'idéal $A_1(X-1) + A_1X$. L'escalier associés aux générateurs $X-1$ et X est réduit à la partie stable des puissances de X à exposant strictement positifs. Pourtant, le polynôme $1 \times (X-1) + (-1) \times X$ vaut 1 et la partie stable associée à l'idéal est ainsi l'ensemble de tous les monômes en X . De manière générale, le phénomène est qu'un polynôme p peut très bien être dans un idéal $I = \sum_{i=1}^r A_n p_i$ sans que son monôme de tête $\text{mt } p$ ne soit dans la partie stable $\bigcup_{i=1}^r M \text{mt } p_i$, ce qui a lieu lorsqu'une combinaison $\sum_{i=1}^r l_i p_i$ produit une annulation des termes de tête des $l_i p_i$.

Définition (S -polynômes). Soient deux polynômes non nuls p_1 et p_2 et posons $m_1 = \text{mt } p_1$, $m_2 = \text{mt } p_2$ et $m = \text{ppcm}(m_1, m_2) = n_1 m_1 = n_2 m_2$. On appelle S -polynôme des deux polynômes p_1 et p_2 toute combinaison linéaire non nulle de la forme $l_1 p_1 + l_2 p_2$ pour tous polynômes non nuls l_1 et l_2 tels que $\text{mt } l_i = n_i$ et $\text{tt } l_1 \text{tt } p_1 + \text{tt } l_2 \text{tt } p_2 = 0$. En pratique, on se restreint à des termes et on pose :

$$\text{Spoly}(p_1, p_2) = l_1 p_1 + l_2 p_2 \quad \text{pour} \quad l_1 = \text{ct}(p_2) n_1, \quad l_2 = -\text{ct}(p_1) n_2.$$

Il convient maintenant de faire le lien entre bases de Gröbner et S -polynômes. Comme les S -polynômes sont éléments de l'idéal considéré, ils se réduisent nécessairement à zéro par toute base de Gröbner de l'idéal. À l'inverse, étant donné un système de générateurs $P = \{p_k\}_{1 \leq k \leq r}$ d'un idéal dont les S -polynômes des générateurs pris deux à deux ne se réduisent pas tous à zéro par P , alors, après adjonction à P des restes non nul des divisions correspondantes, on aboutit à un nouveau système de générateurs du même idéal qui par construction réduit à zéro les S -polynômes initiaux. La section qui suit montre qu'on aboutit à une base de Gröbner en répétant cette opération un nombre fini de fois. Au préalable, nous donnons une nouvelle caractérisation des bases de Gröbner, en termes de S -polynômes.

Théorème (Propriété caractéristique des bases de Gröbner). Soit $P = \{p_k\}_{1 \leq k \leq r}$ un système de générateurs non nuls d'un idéal de polynômes. Tous les S -polynômes $\text{Spoly}(p_i, p_j)$ se réduisent à 0 par P si et seulement si P est une base de Gröbner de l'idéal.

Démonstration. On montre l'implication directe en montrant que tout élément de l'idéal se réduit à zéro par P ; l'implication converse a été montrée précédemment. Soit p irréductible par P et exprimé sous la forme $\sum_{i=1}^r l_i p_i$. Sans perte de généralité, on peut supposer que le monôme $\delta = \max_{1 \leq i \leq r} \{\text{mt } l_i p_i\}$ est minimal parmi les écritures de p en termes des p_i et que pour un entier k bien choisi, on a la relation $\delta = \text{mt } l_i p_i \succ \text{mt } l_j p_j$ dès que $1 \leq i \leq k < j \leq r$. Alors,

$$p = \sum_{i=1}^k \text{tt}(l_i) p_i + \sum_{i=1}^k (l_i - \text{tt}(l_i)) p_i + \sum_{i=k+1}^r l_i p_i = \sum_{i=1}^k \text{tt}(l_i) p_i + \sum_{i=1}^r l'_i p_i,$$

où dans la dernière somme, on a $\text{mt}(l'_i p_i) \prec \delta$ dès lors que le polynôme l'_i est non nul. Sans plus de perte de généralité, on peut encore supposer que k est minimal parmi les écritures de p sous cette forme qui minimisent δ . Notons que k vaut au moins 2, sinon δ serait monôme de tête de p et p serait réductible par p_1 . Observons que δ est divisible par le P.P.C.M. des monômes de tête de p_1 et p_2 . On introduit donc les monômes n_1 et n_2 qui interviennent dans la définition de $\text{Spoly}(p_1, p_2)$, ainsi que des constantes λ_1 et λ_2 de \mathbb{C} et le monôme $m = \delta / \text{ppcm}(\text{mt } p_1, \text{mt } p_2)$, pour obtenir :

$$\text{tt}(l_1) p_1 + \text{tt}(l_2) p_2 = \lambda_1 m \text{ct}(p_2) n_1 p_1 + \lambda_2 m \text{ct}(p_1) n_2 p_2 = \lambda_1 m \text{Spoly}(p_1, p_2) + (\lambda_1 + \lambda_2) \text{ct}(p_1) m n_2 p_2.$$

Par construction, le premier polynôme de cette dernière somme a son monôme de tête strictement plus petit que δ alors que le monôme de tête du second polynôme est exactement δ , à moins qu'il ne soit nul. On obtient ainsi une contradiction à la minimalité de k . \square

8.2 Version rudimentaire de l'algorithme de Buchberger

Nous donnons dans cette section un premier algorithme pour le calcul d'une base de Gröbner d'un idéal donné par des générateurs, algorithme qui découle immédiatement du théorème caractéristique précédent.

Algorithme (Algorithme rudimentaire de calcul d'une base de Gröbner).ENTRÉE : un ensemble fini P de polynômes p_i non nuls, un ordre monomial \preceq OUTPUT : une base de Gröbner G pour le même idéal

1. Initialiser G à P et S à l'ensemble des paires d'éléments de G
2. Tant que S n'est pas vide,
 - (a) Choisir une paire $p = \{g, g'\}$ et la retirer de S
 - (b) Calculer $\text{Spoly}(g, g')$ et le réduire par G
 - (c) Si le reste r est non nul, alors
 - i. Adjoindre à S tous les paires $\{g, r\}$ pour $g \in G$
 - ii. Adjoindre r à G
3. Renvoyer G

Correction et terminaison de l'algorithme. Un invariant de cet algorithme est que l'ensemble G ne contient que les générateurs p_i initiaux et des recombinaisons finies de ceux-ci à coefficients polynomiaux : l'idéal engendré par G est donc constant. De plus, si l'algorithme termine, la sortie G réduit à zéro chacun des S -polynômes de ses éléments pris deux à deux. Le théorème précédent fournit donc la correction de l'algorithme.

Pour la terminaison, on remarque que la partie stable engendrée par les monômes de tête des éléments de G croît strictement à chaque adjonction dans G . En considérant les idéaux engendrés successivement par cette partie stable, on obtient ainsi une suite strictement croissante d'idéaux, puisque l'idéal engendré par une partie stable admet en tant qu'espace vectoriel sur \mathbb{C} la base constituée exactement des monômes de la partie stable. Par noethérianité de A_n , cette suite d'idéaux ne peut être infinie et il ne peut donc y avoir qu'un nombre fini d'adjonctions dans G . \square

9 Réductions à zéro et algorithme classique

On l'observe sur des implantations, une grande partie du temps passé par l'algorithme de la section qui précède (et même sur ses optimisations dont on va parler) est passé dans la réduction des S -polynômes par la base de Gröbner en construction. Par ailleurs, la preuve de terminaison qui vient d'être faite indique que, nécessairement, à partir d'un certain stade de l'exécution, tous les S -polynômes se réduisent à zéro. Il apparaît donc comme important de savoir prédire quelles réductions doivent aller à zéro afin d'éviter autant que possible les calculs correspondants.

9.1 Paires triviales et paires inutiles

Dans l'approche de Buchberger, on identifie deux causes différentes de réduction à zéro, en liaison avec des propriétés différentes des paires de polynômes dont on réduit le S -polynôme.

D'abord, les *paires triviales* sont des paires de polynômes qui réduisent leur propre S -polynôme à zéro indépendamment des autres polynômes de la base de Gröbner en construction. Dit autrement, à eux deux ils forment une base de Gröbner de l'idéal qu'ils engendrent. Il est intéressant de pouvoir identifier une telle paire sans calcul. Une condition suffisante pour qu'une paire soit triviale est que les monômes de tête des deux polynômes soient premiers entre eux, autrement dit, que les indéterminées qui apparaissent dans l'un n'apparaissent pas dans l'autre.

Lemme. Si $\text{ppcm}(\text{mt } p, \text{mt } p') = \text{mt}(p) \text{mt}(p')$, alors $\text{Spoly}(p, p')$ se réduit à zéro par $\{p, p'\}$.

Démonstration. Écrivons $p = t_1 + \dots + t_r$ et $p' = t'_1 + \dots + t'_s$ pour deux suites de termes t_i et t'_i , chacune en des monômes qui décroissent strictement avec i . Le S -polynôme $\text{Spoly}(p, p')$ vaut alors $t'_1 p - t_1 p'$, soit

$$(t_1 \quad t_2 \quad \dots \quad t_r) \begin{pmatrix} 0 & -1 & \dots & -1 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} t'_1 \\ t'_2 \\ \vdots \\ t'_s \end{pmatrix}.$$

On va montrer par récurrence que la réduction du S -polynôme va passer par des polynômes q donnés sous la forme

$$(t_1 \quad \dots \quad t_r) \begin{pmatrix} 0 & -U \\ V & 0 \end{pmatrix} \begin{pmatrix} t'_1 \\ \vdots \\ t'_s \end{pmatrix}$$

pour des matrices rectangulaires U et V dont toutes les entrées valent 1. Le S -polynôme est évidemment de cette forme. Considérons une étape de la réduction. Soit à réduire le polynôme q donné par la forme ci-dessus par p et p' . Tout d'abord, la contribution à q provenant de la matrice U , respectivement V , a pour monôme de tête celui correspondant au coin en haut à gauche dans U , respectivement V , qui s'écrit $t_1 t'_i$ avec $i > 1$, respectivement $t_j t'_1$ avec $j > 1$. Les deux termes correspondant ne peuvent se compenser et s'annuler, car $t_1 t'_i$ ne peut valoir $t_j t'_1$: s'il y avait égalité, puisque $\text{mt } t_1 = \text{mt } p$ et $\text{mt } t'_1 = \text{mt } p'$ sont étrangers, il faudrait $i = j = 1$, ce qui est impossible. Si le monôme de tête de q est donné par $t_1 t'_i$, la réduction consiste à ajouter $p_1 t'_i$, ce qui rétrécit U d'une colonne et élargit V d'une colonne ; s'il est donné par $t_j t'_1$, la réduction consiste à retrancher $t_1 p'$, ce qui élargit U d'une ligne et rétrécit V d'une ligne. Après $r + s$ étapes de réduction, q est réduit à zéro. \square

Une autre forme de paires qui se réduisent à zéro, les *paires inutiles*, correspond à des calculs redondants au sein de l'algorithme de Buchberger : la réduction à zéro envisagée n'a lieu que grâce au contexte des autres paires déjà réduites et incorporées à la base de Gröbner en construction.

Lemme. Si $\text{mt}(g_k)$ divise $\text{ppcm}(\text{mt } g_i, \text{mt } g_j)$ et si les paires $\{g_i, g_k\}$ et $\{g_j, g_k\}$ ont déjà été réduites et les restes correspondants introduits, alors le S -polynôme de $\{g_i, g_j\}$ se réduit à zéro.

9.2 Forme canonique pour les idéaux de polynômes

Quelques propriétés générales des bases de Gröbner vont nous permettre de rendre unique la base de Gröbner associée à un idéal donné pour un ordre monomial choisi.

Tout d'abord, on a déjà indiqué qu'on peut toujours remplacer un élément d'une base de Gröbner par le reste de sa division par les autres éléments.

Par ailleurs, on peut toujours supprimer un élément p d'une base de Gröbner dont le monôme de tête est divisible par celui d'un autre élément q . En effet, la première étape de la réduction du polynôme p par le polynôme q est en fait le calcul du S -polynôme $\text{Spoly}(p, q)$, lequel se réduit à zéro dans une base de Gröbner, mais sans plus pouvoir se réduire par p puisque tous les polynômes du considérés à partir du S -polynôme ont un monôme de tête strictement plus petit que p . En d'autres termes, p se réduit à zéro par division par les autres éléments de la base de Gröbner.

Les propriétés précédentes motivent la définition d'une *base de Gröbner réduite* comme d'une base de Gröbner telle qu'aucun monôme apparaissant dans l'un quelconque de ses éléments ne soit réductible par le reste de la base de Gröbner, et dont les coefficients de tête sont normalisés à 1. En termes de la partie stable de l'idéal, exhiber une base de Gröbner réduite revient à se donner un polynôme par coin de l'escalier saillant vers les monômes de plus petits degrés, à calculer le reste de chaque polynôme par les autres, puis à normaliser les coefficients de tête à 1. Ainsi, à ordre monomial donné, tout idéal admet une unique base de Gröbner réduite. En effet, le polynôme d'une base de Gröbner réduite correspondant à un coin donné de l'escalier de l'idéal ne peut alors qu'être unique, puisque son terme de tête est un monôme et que ses autres termes correspondent à des monômes sous l'escalier : si deux tels polynômes proviennent du même coin, par différence on obtient un polynôme de l'idéal qui n'a que des monômes sous l'escalier et est donc nul.

9.3 Algorithme de Buchberger et ses stratégies classiques

Les critères des deux sections précédentes pour identifier à l'avance une réduction à zéro et pour l'unicité d'une base de Gröbner fournissent l'optimisation qui suit de l'algorithme naïf déjà donné pour le calcul de bases de Gröbner.

Algorithme (Algorithme de Buchberger).

ENTRÉE : un ensemble fini P de polynômes p_i , un ordre monomial \preceq

SORTIE : une base de Gröbner réduite G pour le même idéal

1. Initialiser G à P et S à l'ensemble des paires d'éléments de G
2. Tant que S n'est pas vide,
 - (a) Choisir une paire $p = \{g, g'\}$ et la retirer de S
 - (b) Si p est inutile ou triviale, passer à la paire suivante
 - (c) Calculer $\text{Spoly}(g, g')$ et le réduire par G
 - (d) Si le reste r est non nul, alors
 - i. Adjoindre à S tous les paires $\{g, r\}$ pour $g \in G$
 - ii. Retirer de G les polynômes dont le monôme de tête est divisible par celui de r et y adjoindre r
3. Inter-réduire G et renvoyer le résultat

Correction et terminaison de l'algorithme. La terminaison de l'algorithme se fait comme pour la version naïve de l'algorithme ; la correction s'appuie en plus sur les critères de réduction à zéro et de normalisation des deux sections précédentes. \square

Donnons un exemple de calcul en recherchant une base de Gröbner pour l'ordre lexicographique de l'idéal engendré par $p_1 = \underline{X^2} - Y$ et $p_2 = \underline{X^3} - Z$. Le premier S -polynôme à considérer est $\text{Spoly}(p_1, p_2) = Xp_1 - p_2 = -\underline{XY} + Z$, qui est irréductible par $\{p_1, p_2\}$. Nous posons $p_3 = \underline{XY} - Z$. Puisque X^2 divise le P.P.C.M. X^3Y de X^3 et de XY et que la paire (p_1, p_2) a déjà été traitée, traiter la paire (p_1, p_3) rend la paire (p_2, p_3) inutile. Le S -polynôme $\text{Spoly}(p_1, p_3)$ est $Yp_1 - Xp_3$ et vaut $\underline{XZ} - Y^2$, qui est irréductible et que nous baptisons p_4 . De la même façon, la paire (p_1, p_4) rend la paire (p_2, p_4) inutile. Restent donc à traiter les deux paires (p_1, p_4) et (p_3, p_4) . Le S -polynôme $\text{Spoly}(p_1, p_4)$ vaut $Zp_1 - Xp_4 = \underline{XY^2} - YZ = Yp_3$ et se réduit donc à zéro par p_3 . Le S -polynôme $\text{Spoly}(p_3, p_4)$ vaut $Zp_3 - Yp_4 = \underline{Y^3} - Z^2$, lequel est irréductible par $\{p_1, \dots, p_4\}$ et que nous baptisons p_5 . Maintenant, par le critère sur les paires triviales, nous ne retenons que le S -polynôme $\text{Spoly}(p_3, p_5) = Y^2p_3 - Xp_5 = XZ^2 - Y^2Z = Zp_4$ et se réduit donc à zéro par p_4 . La base de Gröbner calculée est donc $\{p_1, \dots, p_5\}$, et la base de Gröbner réduite est $\{p_1, p_3, p_4, p_5\}$, donnant la partie stable engendrée par X^2, XY, XZ, Y^3 .

Deux sources d'indéterminismes restent présentes dans l'algorithme de Buchberger tel qu'il a été décrit : d'une part, il n'est pas dit comment une paire doit être choisie parmi les paires restant dans S ; d'autre part, la procédure de réduction que nous avons donnée, de même que celle de division, ne précise pas comment choisir le polynôme servant à chaque étape de division dans les cas où il y a ambiguïté. Si des choix quelconques assurent la correction et la terminaison de l'algorithme, il s'avère que ces choix ont un impact très fort sur le temps d'exécution de l'algorithme. On observe que les temps de calcul sont meilleurs pour certaines stratégies de choix, mais en général il y a peu de résultats formellement établis. Par ailleurs, une approche qui semble être le plus souvent meilleure que l'algorithme de Buchberger est celle de l'algorithme F5 de Faugère, bien que celui-ci ne fasse une hypothèse sur son entrée. Il ne nous est pas possible d'exposer cette variation de l'algorithme de Buchberger, et nous retiendrons l'existence des quelques stratégies suivantes.

Stratégie normale. La stratégie dite « normale » est due à Buchberger. Elle réduit en priorité par les polynômes les plus anciennement introduits dans la base de Gröbner en construction, au motif que ceux-ci sont souvent de plus petite taille que les polynômes récemment introduits. De plus, les S -polynômes sont traités dans l'ordre croissant des degrés des P.P.C.M. des monômes de tête des polynômes de la paire correspondante.

Stratégie du sucre. La stratégie dite « du sucre » est due à Giovini, Mora, Niesi, Robbiano et Traverso. Elle vise, dans le cas lexicographique d'ordinaire le plus coûteux, à simuler un calcul sur des polynômes homogènes, pour lequel une optimisation est possible. À cette fin, on décore les polynômes d'un degré fantôme qui est le degré homogène qu'aurait le polynôme si le calcul avait été fait sur les polynômes homogénéisés, et on procède par degrés fantômes croissants. Le degré fantôme n'est autre que le degré total sur les polynômes initiaux du calcul, mais il peut devenir plus grand que lui en cours de calcul.

Stratégie de Gebauer et Möller. Une stratégie due à Gebauer et Möller tente d'exploiter au mieux les critères de rejet des paires triviales et inutiles. En particulier, le critère sur les paires inutiles permet souvent de rejeter l'une parmi deux paires. Plutôt que de choisir au hasard, on s'efforce de ne pas rejeter une paire qui pourrait aussi être rejetée pour une autre raison (par exemple parce qu'elle est reconnue comme triviale), ce qui permet de rejeter deux paires sans calcul au lieu d'une seule. Cette stratégie cherche aussi à maintenir la base en construction aussi petite que possible pendant tout le calcul, c'est-à-dire que la phase d'inter-réduction n'a pas lieu seulement à la fin du calcul, mais tout au long de celui-ci.

Dans les logiciels modernes, on dispose en général d'une implantation de l'algorithme de Buchberger optimisée pour l'ordre grevlex en utilisant notamment la stratégie de Gebauer et Möller raffinée par la stratégie normale. Pour les ordres monomiaux « distants » de l'ordre grevlex, en particulier pour l'ordre lex, on préfère utiliser un algorithme de changement d'ordre, c'est-à-dire un algorithme qui calcule une base de Gröbner pour l'ordre cible par de l'algèbre linéaire à partir de la base de Gröbner pour l'ordre initial. Les algorithmes de changement d'ordre les plus employés sont l'algorithme FGLM et l'algorithme de marche de Gröbner.

10 Cas particulier et extensions de l'algorithme de Buchberger

Pour des calculs en une seule indéterminée, l'algorithme de Buchberger se spécialise en une version sans optimisation de l'algorithme d'Euclide. Pour des entrées linéaires en toutes les indéterminées, il se spécialise en une version de l'algorithme de Gauss à pivot partiel (pivot de colonne), et pour un ordre de traitement des colonnes induit par l'ordre monomial. Dans ce dernier calcul et pour l'ordre lexicographique, certains S -polynômes se réduisent trivialement à zéro, à savoir ceux qui correspondent à des paires de lignes de la matrice dont les termes non nuls les plus à gauche ne sont pas sur la même colonne. Cette remarque est à la base d'une généralisation de l'algorithme de Buchberger aux bases de Gröbner de modules. Quoiqu'un peu plus technique, cette généralisation ouvre la voie à bien de nouvelles applications : l'expression des éléments de la base de Gröbner en terme des polynômes initiaux, thème d'une prochaine section ; le calcul d'inverses modulo un idéal (non principal) par une généralisation du calcul de relations de Bézout ; la saturation d'un idéal par un polynôme (pour un polynôme p donné, on adjoint à un idéal tous les polynômes f tel que pf soit dans l'idéal de départ) ; d'autres calculs en algèbre homologique.

10.1 Cas particulier de l'algorithme d'Euclide

Pour deux polynômes $p_1 = c_1X^{d_1} + \dots$ et $p_2 = c_2X^{d_2} + \dots$ de $\mathbb{C}[X]$, avec $\deg p_1 = d_1 > d_2 = \deg p_2$,

$$\text{Spoly}(p_1, p_2) = c_2p_1 - c_1X^{d_1-d_2}p_2$$

est la première étape élémentaire d'une division euclidienne. Les étapes suivantes de la division reproduisent ensuite les mêmes calculs que la réduction de $\text{Spoly}(p_1, p_2)$ par $\{p_2\}$. Ainsi, la réduction de $\text{Spoly}(p_1, p_2)$ par $\{p_2\}$ fournit le reste p_3 de la division euclidienne de p_1 par p_2 (à multiplication par une constante près).

Suivons de près le calcul de l'algorithme de Buchberger sur une entrée constituée des deux polynômes p_1 et p_2 . Ce calcul détermine d'abord le reste p_3 , puis il crée les paires $\{p_1, p_3\}$ et $\{p_2, p_3\}$. La première devient redondante si on traite la seconde. L'algorithme de Buchberger calcule donc une suite de restes successifs, jusqu'à obtenir un reste nul : il émule donc l'algorithme d'Euclide et renvoie finalement le P.G.C.D. des polynômes initiaux p_1 et p_2 .

Ce calcul se généralise à une d'entrée p_1, \dots, p_n constituée de plus de deux polynômes : l'algorithme de Buchberger calcule encore le P.G.C.D. de ses entrées, mais en effectuant les réductions dans un ordre différent de celui qui serait suivi en calculant le P.G.C.D. g_1 de p_1 et p_2 , puis le P.G.C.D. g_2 de g_1 et p_3 , et ainsi de suite jusqu'au P.G.C.D. g_{n-1} de g_{n-2} et p_n .

10.2 Cas particulier de l'algorithme de Gauss

Considérons le système linéaire

$$a_{i,1}x_1 + \dots + a_{i,n}x_n = 0, \quad 1 \leq i \leq m.$$

La réduction de Gauss de ce système renvoie un système triangulaire équivalent, de la forme

$$\begin{aligned} b_{1,1}x_1 + \dots + b_{1,r}x_r + \dots + b_{1,n}x_n &= 0, \\ &\dots \\ b_{r,r}x_r + \dots + b_{r,n}x_n &= 0 \end{aligned}$$

pour des $b_{i,i}$ non nuls.

Ici, « équivalent » signifie qu'il existe des matrices U et V donnant les relations $A = UB$ et $B = VA$ entre les matrices $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$ et $B = (b_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n}$. Ainsi, les deux systèmes de polynômes $\{a_{i,1}X_1 + \dots + a_{i,n}X_n\}_{1 \leq i \leq m}$ et $\{b_{i,1}X_1 + \dots + b_{i,n}X_n\}_{1 \leq i \leq r}$ engendrent le même espace vectoriel sur \mathbb{C} , donc le même idéal de A_n .

Vue leur structure en monômes, les polynômes $b_{i,i}X_i + \dots + b_{i,n}X_n$ constituent pour l'ordre lexicographique une base de Gröbner de l'idéal engendré par les $a_{i,1}X_1 + \dots + a_{i,n}X_n$. Une base de Gröbner réduite fournit un système linéaire triangulaire réduit : la matrice $(b_{i,j})_{1 \leq i, j \leq r}$ est diagonale.

Comparons les réductions par l'algorithme de Gauss et dans le cas linéaire de l'algorithme de Buchberger. L'algorithme de Gauss n'est amené à ne réduire une ligne $U = u_i x_i + \dots + u_n x_n$ par une autre ligne $V = v_j x_j + \dots + v_n x_n$ que dans le cas où le scalaire v_j est non nul et sert de pivot et si $i \geq j$. Sans perte de généralité, nous pouvons aussi supposer que u_i est non nul, quitte à incrémenter i . Si i est alors strictement plus grand que j , la réduction ne fait en réalité aucun calcul. Dans le cas contraire, la ligne U est remplacée par la ligne $W = U - (u_j/v_j)V$, qui est de la forme $W = w_k x_k + \dots + w_n x_n$ avec $k > j$. Par le calcul analogue par algorithme de Buchberger, le S-polynôme des polynômes U et V est trivial lorsque i et j sont différents, alors que s'ils sont égaux, le calcul de S-polynôme correspond en fait à la réduction de U par V dans l'algorithme de Gauss. Pour un calcul par l'algorithme de Buchberger sur des entrées linéaires, on peut donc adapter les critères de rejet de paires en définissant à zéro les S-polynômes de polynômes d'indéterminées de tête différentes.

10.3 Bases de Gröbner de modules

La théorie des bases de Gröbner se généralise pour donner de bons systèmes de générateurs de modules sur A_n , c'est-à-dire pour faire de l'algèbre linéaire à coefficients dans un anneau de polynômes au lieu d'un corps. Rappelons qu'un *module* M sur un anneau A est un groupe additif stable par action par tout élément de A . Par exemple, tout idéal de A est un A -module, de même que les quotients de la forme A/I pour un idéal I de A sont des modules sur A . Plus généralement, étant donnée une famille $(g_u)_{u \in U}$ d'éléments de A^r , les combinaisons linéaires finies à coefficients dans A forment un module noté $\sum_{u \in U} Ag_u$. Les quotients de la forme $A^r / \sum_{u \in U} Ag_u$ sont des modules sur A .

La généralisation de la théorie repose sur la bonne notion d'ordre pour les modules. Considérons la base canonique $B = (b_i)_{1 \leq i \leq p}$ de A^r , avec b_i le vecteur de A^r constitué de 0 sauf en i -ème colonne où 0 est remplacé par 1. On a $A^r = Ab_1 \oplus \dots \oplus Ab_r$. Deux façons naturelles d'étendre les ordres monomiaux de M à $M \times B$ sont disponibles :

- l'ordre **top**, pour *term over position*, pour lequel les mb_i sont triés sur m , puis sur i ,
- l'ordre **pot**, pour *position over term*, pour lequel les mb_i triés sur i puis sur m .

On obtient ainsi des ordres $\prec_{\text{top,lex}}$, $\prec_{\text{pot,lex}}$, $\prec_{\text{top,grevlex}}$, $\prec_{\text{pot,grevlex}}$, etc.

De même, on introduit des S-polynômes pour les modules — ou devrions-nous dire « S-vecteur » ? — en généralisant la remarque faite dans l'interprétation de l'algorithme de Gauss en termes de l'algorithme de Buchberger. Ici encore, on déclare nul un S-polynôme de deux vecteurs ayant des monômes de tête sur des b_i et b_j différents. Soient deux vecteurs $p_1 = \sum_{i=1}^r p_{1,i} b_i$ et $p_2 = \sum_{i=1}^r p_{2,i} b_i$ deux éléments de M et posons $m_1 b_{i_1} = \text{mt } p_1$, $m_2 b_{i_2} = \text{mt } p_2$ et $m = \text{ppcm}(m_1, m_2) = n_1 m_1 = n_2 m_2$. Lorsque $i_1 = i_2$, on appelle *S-polynôme* de p_1 et p_2 toute combinaison linéaire de la forme $l_1 p_1 + l_2 p_2$ pour tous polynômes l_i tels que $\text{mt } l_i = n_i$ et $\text{tt } l_1 \text{tt } p_{1,i} + \text{tt } l_2 \text{tt } p_{2,i} = 0$. Lorsque $i_1 \neq i_2$, on déclare que le S-polynôme de p_1 et p_2 est nul, ou bien l'on dit qu'ils n'ont pas de S-polynôme. On a ainsi la formule synthétique

$$\text{Spoly}(p_1, p_2) = \begin{cases} \text{ct}(p_2)n_1 p_1 + \text{ct}(p_1)n_2 p_2 & \text{si } i_1 = i_2, \\ 0 & \text{sinon.} \end{cases}$$

10.4 Application : base de Gröbner en terme des polynômes initiaux

Traisons succinctement une application de la théorie des bases de Gröbner aux modules sur un anneau de polynômes : étant donnés des polynômes p_1, \dots, p_r , on cherche à exprimer les éléments d'une base de Gröbner de l'idéal engendré I en terme des p_i .

Dans $A^{r+1} = \bigoplus_{i=0}^r Ab_i$, considérons une base de Gröbner pour un ordre **pot** du sous-module S engendré par les $b_0 - p_i b_i$. Cette modélisation réalise l'invariant que tout vecteur $c_0 b_0 + \dots + c_r b_r$ considéré au court du calcul vérifie la relation $c_0 = \sum_{i=1}^r c_i p_i$. On vérifie ainsi que la base de Gröbner pour S contient :

- des éléments de la forme $g b_0 - \sum_{i=1}^r l_i b_i$, pour lesquels $g = \sum_{i=1}^r l_i p_i$. Les g constituent alors une base de Gröbner de I .
- des éléments de la forme $\sum_{i=1}^r u_i b_i$, pour lesquels $\sum_{i=1}^r u_i p_i = 0$. Ceux-ci engendrent ainsi le module des relations entre les p_i .

11 Complexité intrinsèque et bases de Gröbner

Dans cette section, nous annonçons très brièvement quelques résultats qui montrent la nature exponentielle ou doublement exponentielle de problèmes rattachés à la notion de base de Gröbner ou à leur calcul.

11.1 Problèmes complets

Le problème général de la recherche d'une base de Gröbner réduite et le problème d'appartenance à un idéal générique de polynômes sont des problèmes EXPSPACE-complets (pour des coefficients dans \mathbb{Q}).

Restreints à des idéaux binomiaux (engendrés par des binômes $X^\alpha - X^\beta$), il en est de même pour les deux problèmes.

Restreint à des idéaux homogènes (engendrés par des polynômes dont tous les monômes ont même degré), le problème d'appartenance à un idéal n'est que PSPACE-complet.

11.2 Taille de la sortie

Les degrés des polynômes d'une base de Gröbner réduite d'un idéal $Ap_1 + \dots + Ap_s \subseteq \mathbb{C}[X_1, \dots, X_n]$, pour des p_i de degré au plus d , sont au plus

$$2 \left(\frac{d^2}{2} + d \right)^{2^n - 1}.$$

Il existe des idéaux dont toutes les bases de Gröbner contiennent au moins $2^{2^{cn}}$ éléments et des éléments de degré au moins $2^{2^{c'n}}$, pour des constantes réelles c et c' strictement positives.

Troisième partie : Calculs en Magma

En *Magma*, la création d'un anneau de polynômes nécessite de déclarer d'abord le corps de coefficients sur lequel on travaille, ici le corps \mathbb{Q} des nombres rationnels, puis de déclarer le nombre d'indéterminées transcendantales qui servent à étendre ce corps en un anneau de polynômes. Ce nombre est appelé le « rang » de l'anneau par *Magma*.

```
> Q:=RationalField();
> A:=PolynomialRing(Q,3);
> Rank(A);
3
> [A.i:i in [1..Rank(A)]];
[
  $.1,
  $.2,
  $.3
]
```

Dans l'exemple précédent, les indéterminées de A ne sont pas nommées. On peut y faire référence par A.1, A.2 et A.3. Pour éviter cette notation, il est possible de voir ces objets sous d'autres noms par la notation suivante.

```
> Q:=RationalField();
> A<X,Y,Z>:=PolynomialRing(Q,3);
> [A.i:i in [1..Rank(A)]];
[
  X,
  Y,
  Z
]
```

Cet appel a effectivement affecté la valeur A.1 à la variable X. Attention à la difficulté suivante de *Magma*, après déclaration d'un autre anneau utilisant aussi X, il n'est plus possible d'accéder à A.1 à l'aide de X, bien qu'à l'affichage A.1 soit toujours présenté comme X.

Une fois un anneau créé, on peut introduire un polynôme ou un idéal de celui-ci.

```
> f:=X^3-1;
> I:=ideal<A|X+Y+Z,X*Y+Y*Z+Z*X,X*Y*Z-1>;
> I;
Ideal of Polynomial ring of rank 3 over Rational Field
Lexicographical Order
Variables: X, Y, Z
Basis:
[
```

```

X + Y + Z,
X*Y + X*Z + Y*Z,
X*Y*Z - 1

```

]

Un idéal est donné par un système de générateurs, notion pour laquelle *Magma* utilise le mot anglais *basis*. Un idéal admettant plusieurs systèmes de générateurs, *Magma* change librement le système en cours d'utilisation, selon les calculs envisagés. En particulier, lorsqu'une base de Gröbner est calculée, elle devient le nouveau système de générateurs en cours.

La déclaration de l'anneau *A* ci-dessus est en fait la déclaration d'un anneau muni d'un ordre monomial. Implicitement, c'est l'ordre $\prec_{\text{lex}(X,Y,Z)}$ qui a été choisi. L'exemple qui suit montre l'effet du calcul d'une base pour cet ordre.

```

> Basis(I);
[
  X + Y + Z,
  X*Y + X*Z + Y*Z,
  X*Y*Z - 1
]
> Groebner(I);
> Basis(I);
[
  X + Y + Z,
  Y^2 + Y*Z + Z^2,
  Z^3 - 1
]

```

Une fois une base calculée, la mise sous forme normale modulo l'idéal et le test d'appartenance à l'idéal se font comme ci-dessous. Puisque notre polynôme *f* est dans l'idéal, on peut donner ses coordonnées sur la base de Gröbner qui sert de système de générateurs en cours.

```

> NormalForm(f,I);
0
> f in I;
true
> Coordinates(I,f);
[
  X^2 - X*Y - X*Z + Y^2 + 2*Y*Z + Z^2,
  -Y - 2*Z,
  1
]

```

Mais rechercher les coordonnées d'un polynôme hors de l'idéal provoque une erreur.

```

> NormalForm(f+1,I);
1
> f+1 in I;
false
> Coordinates(I,f+1);

>> Coordinates(I,f+1);
~
Runtime error in 'Coordinates': Argument 2 is not
in argument 1

```

Intéressons-nous maintenant à d'autres ordres monomiaux. Ceux-ci doivent être déclarés dès la création de l'anneau de polynômes. En effet, c'est dès cet instant que se décide la représentation de données qui va servir pour le stockage des polynômes. Ici, nous donnons un ordre d'élimination, ou ordre par blocs, qui place *A.1* et *A.2*, à savoir *T* et *U* lexicographiquement avant les deux autres générateurs de l'anneau, et trie les monômes en *T* et *U* par l'ordre par *grevlex(T,U)*.

```

> Q:=RationalField();
> A<T,U,X,Y>:=PolynomialRing(Q,4,"elim",[1,2]);
> I:=ideal<A|(1+T^2)*X-(1-T^2),(1+T^2)*Y-2*T,(1+T^2)*U-1>;
> Groebner(I);
> Basis(I);
[
  T*X + T - Y,
  T*Y + X - 1,
  U - 1/2*X - 1/2,
  X^2 + Y^2 - 1
]
> [b:b in Basis(I)|Degree(b,T) eq 0 and Degree(b,U) eq 0];
[
  X^2 + Y^2 - 1
]

```

Magma dispose aussi de fonctions pour calculer des bases de Gröbner pour les modules. Avant tout, il convient de déclarer le module libre M dans lequel on va décrire un sous-module S donné par générateurs. Ci-dessous, le module M est le module libre sur P de rang 2, le rang (mathématique) étant appelé *degree* par *Magma*. Les éléments de ce module sont présentés comme des vecteurs lignes de longueur 2.

```

> Q:=RationalField();
> P<X,Y,Z>:=PolynomialRing(Q,3,"grevlex");
> M:=Module(P,2);
> M;
Full Module of degree 2
TOP Order
Coefficient ring:
  Polynomial ring of rank 3 over Rational Field
  Graded Reverse Lexicographical Order
  Variables: X, Y, Z
> S:=sub<M|(X^2-1)*M.1+(X*Y-Z)*M.2,(Y^2+X)*M.1+(3*Z-X)*M.2>;
> S;
Module of degree 2
TOP Order
Coefficient ring:
  Polynomial ring of rank 3 over Rational Field
  Graded Reverse Lexicographical Order
  Variables: X, Y, Z
Basis:
( X^2 - 1 X*Y - Z)
( Y^2 + X -X + 3*Z)
> Groebner(S);
> Basis(S);
[
  (0 X*Y^3 + X^3 + X^2*Y - 3*X^2*Z - Y^2*Z - X*Z - X + 3*Z),
  (X^2 - 1 X*Y - Z),
  ( Y^2 + X -X + 3*Z)
]
>

```