

# Introduction au Calcul formel — Algorithmes et complexité

Frédéric Chyzak

9 novembre 2005



# Chapitre 1

## Présentation du cours

Version préliminaire : Id: CalculFormel.tex chyzak Exp .

### 1.1 Le calcul formel

Le calcul formel — *computer algebra* en anglais — a pour objet d'étude la manipulation symbolique effective d'objets mathématiques. Par ses méthodes, il procède en formalisant et en donnant une nature algorithmique au calcul sur des représentations informatiques finies d'objets mathématiques. Calculer, c'est en fait construire une telle représentation, le plus souvent algébrique, en respectant une mécanique fixée à l'avance et uniforme sur toute une classe d'objets. Par delà les questions de faisabilité, une évolution récente de la discipline est de revisiter des problèmes anciens du point de vue de la complexité.

L'objectif principal de cette introduction au calcul formel sera d'en montrer les algorithmes de base, avec, à chaque fois, des exemples d'applications. Les algorithmes étudiés permettront par exemple de répondre à des questions telles :

- Quelle est l'enveloppe des cordes d'une ellipse vues sous un angle droit depuis un point donné ?  
(*Indication : faire pivoter une paire de droites orthogonales autour du point fixe et obtenir une paramétrisation du point variable.*)
- Comment se poursuit la suite  $(3, 0, 4, 2, 3, 0, \dots)$  d'entiers modulo 5 ?  
(*Indication : calculer un approximant de Padé-Hermite.*)
- Est-il possible de trouver des entiers  $e_1, \dots, e_5$  tels que  $12e_1 + 43e_2 + 189e_3 + 19e_4 + 289e_5 = 220$  ?  
(*Indication : utiliser un algorithme de réduction de réseau.*)
- L'intégrale de  $x^{1/2}(\ln x)^5/(1-x)^5$  de 0 à l'infini est difficilement calculable sous forme explicite ; une évaluation numérique donne la valeur approchée  $V = -16.6994737192290704961872434007\dots$ . On a de bonnes raisons de penser que ce nombre s'exprime aisément comme combinaison linéaire des puissances de  $\pi = 3.14159\dots$  avec des coefficients rationnels. Peut-on trouver s'il y a une telle relation entre  $V$  et  $\pi$  ?  
(*Indication : considérer des approximations rationnelles de  $V$  et des puissances de  $\pi$  et utiliser l'algorithme LLL.*)

- Dans un modèle simplifié de l'interaction d'une mailloche frappant la membrane d'une timbale circulaire, la détermination des modes propres de la vibration amène à calculer l'intégrale entre  $-1$  et  $+1$  de  $f_n(p, x) = \exp(-px)T_n(x)/(1-x^2)^{1/2}$ . Que vaut cette intégrale ?  
(Indication : écrire un système d'équations différentielles et de récurrences vérifiées par la fonction  $f_n(p, x)$  et se débarrasser de  $x$ .)
- Quelles sont les conformations géométriques possibles en trois dimensions du cyclohexane  $C_6H_{12}$  ?  
(Indication : on sait que les angles entre les liaisons carbone-carbone successives ont pour cosinus  $-1/3$  et que les atomes de carbone sont libres de leur rotation autour des liaisons. On pourra effectuer plusieurs éliminations polynomiales.)

Par les techniques utilisées (souvent, de l'algèbre) et les objectifs visés (algorithmiser des questions mathématiques), le cours s'adresse à un public d'informaticiens mathématiquement réceptifs.

## 1.2 Contenu du cours

Le cours abordera les sujets et algorithmes suivants, traitant tantôt de structures de données de bas niveau, tantôt de représentations d'objets mathématiques de haut niveau. (L'ordre qui suit n'est pas significatif.)

1. entiers, polynômes, séries, algorithme d'Euclide, résultants ;  
Les opérations élémentaires, somme, produit et division d'entiers et de polynômes, sont au centre de la plupart des algorithmes de calcul formel. On présentera quelques solutions classiques pour la multiplication rapide, culminant dans les algorithmes de type FFT (Fast Fourier Transform). On verra ensuite un premier algorithme d'élimination, l'algorithme d'Euclide, qui s'applique aussi bien aux entiers qu'aux polynômes. Ses applications sont nombreuses, on verra notamment les approximants de Padé et les calculs de résultants.
2. algèbre linéaire (produit de matrices, algorithme de Gauss et optimisations) ;  
Les questions relatives aux opérations matricielles sont extrêmement variées. D'une part, on montrera comment la multiplication, l'inversion, le calcul du polynôme caractéristique, sont de complexité équivalente, lorsqu'on traite des matrices à coefficients dans un corps. On introduira la notion d'exposant de l'algèbre linéaire, qui vient mesurer cette complexité. On évoquera ensuite l'algorithmique de l'algèbre linéaire creuse, qui permet de traiter des matrices de taille très conséquente, à plusieurs centaines de milliers d'entrées. Enfin, on traitera des questions relatives aux matrices ayant d'autres types de coefficients, notamment des entrées entières, des séries formelles, voire des nombres flottants.
3. bases de Gröbner et algorithme de Buchberger, résolution de systèmes polynomiaux ;  
Les bases de Gröbner fournissent une extension de l'algorithme d'Euclide pour le cas de polynômes en plusieurs variables. L'algorithme de Buchberger pour le calcul de bases de Gröbner fournit une procédure d'élimination pour le cas de plusieurs variables. Cette approche algorithmique importante a de nombreuses applications en géométrie (notamment en géométrie algébrique), par exemple à la démonstration semi-automatique de théorèmes de géométrie et à la recherche d'équations implicites de courbes algébriques paramétrées. Une autre application très importante est l'utilisation des bases de Gröbner pour la résolution de systèmes de polynômes en plusieurs variables. La contrepartie de la large applicabilité de cette théorie est sa complexité élevée, doublement exponentielle, au moins dans le cas le pire.
4. algorithme de réduction de réseaux (LLL) ;  
Étant donnés des vecteurs  $V_1, \dots, V_m$  dans l'espace  $\mathbb{Z}^n$ , on appelle réseau engendré par  $V_1, \dots, V_m$  l'ensemble de leurs combinaisons linéaires à coefficients entiers. Le problème de trouver le plus court vecteur dans un réseau est NP-dur, il est donc peu vraisemblable que l'on dispose prochainement d'un algorithme efficace pour le traiter. Si l'on relâche la contrainte d'optimalité, il devient possible de trouver un vecteur « assez » court en temps polynomial, en utilisant l'algorithme LLL (pour

« Lenstra, Lenstra, Lovasz »). Ses applications sont extrêmement nombreuses et vont de la théorie des nombres aux problèmes de sac à dos, en passant par la factorisation des polynômes.

5. intégration symbolique (des fractions rationnelles à l'algorithme de Risch) ;

À la main, le calcul d'une intégrale définie passe souvent par la recherche d'une primitive. Il en est de même en calcul formel, on l'on recherche de plus une forme explicite. Le cas de base, l'intégration des fractions rationnelles, sera traité en détail, puis l'algorithme de Risch sera abordé dans ses grandes lignes.

6. équations différentielles linéaires (solutions polynomiales, rationnelles, exponentielles, calculs sur leurs solutions).

Le calcul formel s'intéresse aussi à la résolution en formules explicites d'équations différentielles ou à l'inverse, à la manipulation de solutions données implicitement comme solutions d'équations différentielles. On s'intéressera dans ce cours tout particulièrement au cas des équations différentielles linéaires. On verra tout d'abord comment en rechercher les solutions polynomiales, rationnelles et exponentielles, puis des méthodes de manipulation permettant le calcul d'intégrales définies paramétrées.



## Chapitre 2

# Bases de Gröbner et applications

### 2.1 Introduction

La division euclidienne et l'algorithme d'Euclide pour le P.G.C.D. sont des outils algorithmiques centraux en algèbre commutative computationnelle<sup>1</sup> 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 de l'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 EDP linéaires et de leur groupes de symétries,

---

<sup>1</sup>On 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.

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 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 2.2, nous rappelons la définition et les premières propriétés algébriques des idéaux. En section 2.3, nous posons quatre problèmes qui trouveront une solution algorithmique ou au moins constructive par la théorie des bases de Gröbner. La section 2.4 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 2.5. Nous sommes alors prêts pour définir les bases de Gröbner en section 2.6. Nous terminons la première partie en section 2.7 en explicitant des méthodes algorithmiques qui répondent aux problèmes posés en début de texte.

## 2.2 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  $\bar{\mathbb{Q}}[X_1, \dots, X_n]$ , pour une clôture algébrique  $\bar{\mathbb{Q}}$  de  $\mathbb{Q}$ , on peut donc tout d'abord se donner un idéal par des générateurs  $g_u \in \bar{\mathbb{Q}}[X_1, \dots, X_n]$ . 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  $\bar{\mathbb{Q}}[X_1, \dots, X_n]$  qui s'annulent sur un ensemble donné  $V$  de points de  $\bar{\mathbb{Q}}^n$ ,

$$I(V) = \{ p \in \bar{\mathbb{Q}}[X_1, \dots, X_n] : \forall x = (x_1, \dots, x_n) \in V, p(x) = 0 \}, \quad (2.1)$$

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.

## 2.3 Quelques problèmes sur les idéaux de polynômes

Dorénavant, sauf mention expresse du contraire, tous les idéaux sont des idéaux d'un anneau de polynômes  $\mathbb{Q}[X_1, \dots, X_n]$ , que l'on notera  $A_n$  dans la suite. Nous posons maintenant quatre problèmes qui 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.

### 2.3.1 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 (2.1).

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  $A_\infty$  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  $A_\infty$ . 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.

### 2.3.2 Appartenance à un idéal

Soient un idéal  $I$  de  $A_n = \mathbb{Q}[X_1, \dots, X_n]$ , 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  $\mathbb{Q}[X, Y, Z]$ ) 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)

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

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  $\mathbb{Q}$  et non sur  $\mathbb{R}$  pour éviter tout problème créé par une équation polynomiale sans solution réelle, telle  $X^2 = 1$ .)

### 2.3.3 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  $\mathbb{Q}^n$  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  $\Lambda$ , le multiplicateur de Lagrange.

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

### 2.3.4 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  $\mathbb{Q}^n$ , 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  $x^2 + y^2 = 1$ .

## 2.4 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.

### 2.4.1 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  $\mathbb{Q}$ . 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  $p$ .

### 2.4.2 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 indéterminées  $X_1, \dots, X_n$ , 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

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

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

### 2.4.3 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  $\prec_{\text{lex}}$ ) :  $X^\alpha \prec_{\text{grlex}} X^\beta$  si  $|\alpha| < |\beta|$  ou ( $|\alpha| = |\beta|$  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  $\prec_{\text{revlex}}$ ) :  $X^\alpha \prec_{\text{grevlex}} X^\beta$  si  $|\alpha| < |\beta|$  ou ( $|\alpha| = |\beta|$  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*,  $\prec_{\text{lex}} : 1 \prec X_3 \prec X_3^2 \prec X_3^3 \prec \dots \prec X_2 \prec X_2X_3 \prec X_2X_3^2 \prec X_2X_3^3 \prec \dots \prec X_2^2 \prec X_2^2X_3 \prec X_2^2X_3^2 \prec X_2^2X_3^3 \prec \dots \prec X_1 \prec X_1X_3 \prec X_1X_3^2 \prec X_1X_3^3 \prec \dots \prec X_1X_2 \prec X_1X_2X_3 \prec X_1X_2X_3^2 \prec X_1X_2X_3^3 \prec \dots \prec X_1X_2^2 \prec X_1X_2^2X_3 \prec X_1X_2^2X_3^2 \prec X_1X_2^2X_3^3 \prec \dots$ .
- *ordre lexicographique gradué*,  $\prec_{\text{grlex}} : 1 \prec X_3 \prec X_2 \prec X_1 \prec X_3^2 \prec X_2X_3 \prec X_2^2 \prec X_1X_3 \prec X_1X_2 \prec X_1^2 \prec X_3^3 \prec X_2X_3^2 \prec X_2^2X_3 \prec X_2^3 \prec X_1X_3^2 \prec X_1X_2X_3 \prec X_1X_2^2 \prec X_1^2X_3 \prec X_1^2X_2 \prec X_1^3 \prec \dots$ .
- *ordre lexicographique renversé*,  $\prec_{\text{revlex}} : \dots \prec X_1^3X_2^2X_3 \prec X_1^2X_2^2X_3 \prec X_1X_2^2X_3 \prec X_2^2X_3 \prec \dots \prec X_1^3X_3 \prec X_1^2X_3 \prec X_1X_3 \prec X_3 \prec \dots \prec X_1^3X_2^2 \prec X_1^2X_2^2 \prec X_1X_2^2 \prec X_2^2 \prec \dots \prec X_1^3X_2 \prec X_1^2X_2 \prec X_1X_2 \prec X_2 \prec \dots \prec X_1^3 \prec X_1^2 \prec X_1 \prec 1$ .
- *ordre lexicographique renversé gradué*,  $\prec_{\text{grevlex}} : 1 \prec X_3 \prec X_2 \prec X_1 \prec X_3^2 \prec X_2X_3 \prec X_1X_3 \prec X_2^2 \prec X_1X_2 \prec X_1^2 \prec X_3^3 \prec X_2X_3^2 \prec X_1X_3^2 \prec X_2^2X_3 \prec X_1X_2X_3 \prec X_1^2X_3 \prec X_2^3 \prec X_1X_2^2 \prec X_1^2X_2 \prec X_1^3 \prec \dots$ .

Encore une fois, l'ordre  $\prec_{\text{revlex}}$  n'est pas un ordre monomial : il fournit une suite infinie décroissante de monômes. En revanche, les ordres  $\prec_{\text{lex}}$ ,  $\prec_{\text{grlex}}$ ,  $\prec_{\text{grevlex}}$  sont des ordres monomiaux. Nous laissons la preuve au lecteur. Les ordres monomiaux  $\prec_{\text{lex}}$  et  $\prec_{\text{grevlex}}$  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  $\prec_{\text{lex}}$ , sont identiques. Par ailleurs, on a pour tous monômes  $X^\alpha$  et  $X^\beta$  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.

#### 2.4.4 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 récrivant 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.

## 2.5 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  $A_1g$  ayant cette propriété de degré, et l'on peut dire que l'on a divisé  $f$  par l'idéal  $A_1g$ . 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 ainsi d'exprimer  $f$  sous la forme  $q_1g_1 + \dots + q_s g_s + r$ .

### 2.5.1 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  $c \in \mathbb{Q}$  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.

### 2.5.2 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  $r, q_1, \dots, q_s$

*Preuve 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  $g_2 = Y^2 - 1$ . (Pour facilité la lecture, 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.

## 2.6 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.

### 2.6.1 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 :  $\text{mt}(I) = \{\text{mt}(p) : p \in I \setminus \{0\}\}$ .

### 2.6.2 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  $q g_i$  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  $A = \mathbb{Q}[X, Y]$  de l'ordre monomial  $\text{lex}(Y, X)$ . Les deux polynômes  $\underline{XY}^3 - 1$  et  $\underline{X}^3 Y + 1$  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  $A_n = \mathbb{Q}[X_1, \dots, X_n]$  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 polynôme non nul  $f$  de  $I$  est réductible par  $G$  ;
4. pour tout  $f$  dans  $A_n$ , il existe un unique polynôme  $r$  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  $\bar{\mathbb{Q}}$ , 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  $S$ .

□

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.

### 2.6.3 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 un 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  $X^{\alpha_{1,j}}, \dots, X^{\alpha_{s,j}}$ . 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  $X^{\alpha_i}Y^j$  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  $A_n = \bar{\mathbb{Q}}[X_1, \dots, X_n]$ , 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  $\prec$ .  $\square$

## 2.7 Applications de la théorie des bases de Gröbner

### 2.7.1 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  $A_n = \bar{\mathbb{Q}}[X_1, \dots, X_n]$  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 générateur 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  $A_n[Y] = \bar{\mathbb{Q}}[X_1, \dots, X_n, Y]$ , 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  $\alpha_{1,j}, \dots, \alpha_{s,j}$  qui correspondent respectivement à des éléments  $a_{i,j} = \alpha_{i,j} Y^j + \dots$  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.

### 2.7.2 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  $f = q_1g_1 + \dots + q_s g_s + r$

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  $\gamma$ , 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  $\gamma$  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

### 2.7.3 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  $f = q_1 p_1 + \dots + q_r p_r$  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  $A_n = \mathbb{Q}[X_1, \dots, X_n]$  avec le sous-anneau  $A_{n,k} = \mathbb{Q}[X_{k+1}, \dots, X_n]$  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  $A_n = \mathbb{Q}[X_1, \dots, X_n]$  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  $\mathbb{Q}[X_{k+1}, \dots, X_n]$  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  $\mathbb{Q}^n$  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

$$\begin{aligned}
 g_1(x_1, x_2, \dots, x_n) &= 0, \\
 &\vdots \\
 g_{s_1}(x_1, x_2, \dots, x_n) &= 0, \\
 g_{s_1+1}(x_2, \dots, x_n) &= 0, \\
 &\vdots \\
 g_{s_2}(x_2, \dots, x_n) &= 0, \\
 &\vdots \\
 g_{s_{n-1}+1}(x_n) &= 0, \\
 &\vdots \\
 g_{s_n}(x_n) &= 0,
 \end{aligned} \tag{2.2}$$

où  $s_k = r_1 + \dots + r_k$  pour des entiers positifs  $r_\ell$  (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  $\mathbb{Q}^n$  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  $\mathbb{Q}^n$  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)

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.

### 2.7.4 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  $\bar{\mathbb{Q}}^n$ , 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,  $\text{lex}(U, T_1, \dots, T_m, X_1, \dots, X_n)$ )
2. Introduire le P.P.C.M.  $\tilde{q}$  des  $q_i$
3. 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  $U\tilde{q}(T_1, \dots, T_m) - 1$
4. 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 seul facteur  $X^2Y - Z^3$  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  $\overline{\mathbb{Q}}[X, Y, Z]$  puisqu'il est de degré 1 en  $Y$ .

# Chapitre 3

## Algorithme de Buchberger

### 3.1 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, accroissement qui correspond 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.

#### 3.1.1 $S$ -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 associé 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  $l_1 \text{ tt } p_1 + l_2 \text{ tt } p_2 = 0$ . 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  $\delta$ . Notons que  $k$  vaut au moins 2, sinon  $\delta$  serait monôme de tête de  $p$  et  $p$  serait réductible par  $p_1$ . Observons que  $\delta$  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  $\lambda_1$  et  $\lambda_2$  de  $\bar{\mathbb{Q}}$  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  $\delta$  alors que le monôme de tête du second polynôme est exactement  $\delta$ , à moins qu'il ne soit nul. Par hypothèse, le  $S$ -polynôme de  $p_1$  et de  $p_2$  se réduit à zéro par  $P$ ; le premier terme  $\lambda_1 m \text{Spoly}(p_1, p_2)$  se réécrit donc comme une somme  $\lambda_1 m \sum_i l''_i p_i = \sum_i \lambda_1 m l''_i p_i$  dans laquelle chaque terme a son monôme de tête strictement plus petit que  $\delta$ . On obtient ainsi une contradiction à la minimalité de  $k$ , d'où la conclusion que tout élément  $\sum_{i=1}^r l_i p_i$  de l'idéal est réductible par  $P$ . Cette famille est donc une base de Gröbner de l'idéal.  $\square$

### 3.1.2 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  $S$  toutes les paires  $\{g, r\}$  pour  $g \in G$
    - ii. Adjoindre  $r$  à  $G$
3. Renvoyer  $G$

*Preuve 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  $\bar{\mathbb{Q}}$  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  $G$ .  $\square$

## 3.2 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.

### 3.2.1 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  $t'_1 p - t_1 p' = p t'_1 - t_1 p'$ , 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  $V$ . Cette contribution 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.  $\square$

On notera l'importance dans cette preuve de la relation  $t'_1 p - t_1 p' = p t'_1 - t_1 p'$ , qui fait que le résultat ne se transpose pas à des théories de bases de Gröbner dans des contextes non commutatifs.

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.

### 3.2.2 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 appaissant 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.

### 3.2.3 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

*Preuve 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  $p_1 = X^2 - Y$  et  $p_2 = X^3 - Z$ . Le premier  $S$ -polynôme à considérer est  $\text{Spoly}(p_1, p_2) = Xp_1 - p_2 = -XY + Z$ , qui est irréductible par  $\{p_1, p_2\}$ . Nous posons  $p_3 = XY - Z$ . 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 dans ce cours introductif 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.

### 3.3 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 (pas nécessairement 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.

#### 3.3.1 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  $\bar{\mathbb{Q}}[X]$ , 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 simule ainsi 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  $p_n$ .

#### 3.3.2 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  $\{b_{i,i}X_i + \dots + b_{i,n}X_n\}_{1 \leq i \leq r}$  engendrent le même espace vectoriel sur  $\bar{\mathbb{Q}}$ , donc le même idéal de  $A_n$ .

Vu 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.

### 3.3.3 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 multiplication 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 d'étendre les ordres monomiaux de  $M$  à  $M \times B$  sont toute naturelles :

- 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  $l_1 \text{tt } p_{1,i} + l_2 \text{tt } p_{2,i} = 0$ . Lorsque  $i_1 \neq i_2$ , on déclare que le S-polynôme de  $p_1$  et  $p_2$  est nul, ou bien on dit qu'ils n'ont pas de S-polynôme. En se restreignant à des  $l_i$  monomiaux, on a ainsi la formule synthétique

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

### 3.3.4 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  $gb_0 - \sum_{i=1}^r l_i b_i$ , 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  $p_i$ .

### 3.4 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.

#### 3.4.1 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.

#### 3.4.2 Taille de la sortie

Les degrés des polynômes d'une base de Gröbner réduite d'un idéal  $Ap_1 + \dots + Ap_s \subseteq \bar{\mathbb{Q}}[X_1, \dots, X_n]$ , 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.

## Chapitre 4

# 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  $\text{grevlex}(T,U)$ .

```

> 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)
]
>

```



## Chapitre 5

# Intégration symbolique des fractions rationnelles

### 5.1 Le problème de l'intégration symbolique et le cas des fractions rationnelles

L'intégration symbolique en « forme close » est un succès des débuts du calcul formel. Avec l'algorithme d'intégration de Risch, on peut déterminer si une expression rationnelle complexe en des fonctions obtenues par compositions de logarithmes et exponentielles admet une primitive de même nature, et dans ce cas la calculer. Par exemple, on calcule qu'une primitive de

$$f = \frac{x \left( \left( x^2 e^{2x^2} - \ln^2(x+1) \right)^2 + 2x e^{3x^2} (x - (2x^2 + 1)(x+1) \ln(x+1)) \right)}{(x+1) \left( \ln^2(x+1) - x^2 e^{2x^2} \right)^2}$$

est

$$F = x - \ln(x+1) + \frac{x e^{x^2} \ln(x+1)}{x^2 e^{2x^2} - \ln(x+1)^2} + 1/2 \ln \left( \ln(x+1) + x e^{x^2} \right) - 1/2 \ln \left( \ln(x+1) - x e^{x^2} \right).$$

On démontre à l'inverse que  $e^{x^2}$  n'admet aucune écriture rationnelle en des fonctions obtenues par compositions de logarithmes et exponentielles. Notons que vérifier le résultat  $\int f dx = F$  est d'une grande simplicité puisqu'il suffit de dériver et de normaliser les expressions. La difficulté est de déterminer  $F$  à partir de  $f$ , sans autre indication a priori sur les exponentielles et les logarithmes qui interviennent dans le résultat.

Un cadre simplifié auquel se ramène ultimement l'algorithme de Risch est celui de l'intégration des fractions rationnelles. De plus, il présente déjà un certain nombre des idées de l'algorithme de Risch général et une étude de sa complexité reste abordable à ce stade du cours. C'est pourquoi nous choisissons de le présenter bien que nous n'aborderons pas l'algorithme général dans ce cours.

Du point de vue algébrique, une fraction algébrique, disons, à coefficients dans un corps  $k$ , est un élément  $f/g$  de  $k(X)$  où  $f$  et  $g$  sont des polynômes de  $k[X]$  que l'on prendra premiers entre eux. D'un point de vue analytique, en faisant  $k = \mathbb{C}$ , une fraction rationnelle représente une fonction de  $\mathbb{C} \cup \{\infty\}$  dans lui-même qui a la propriété de n'avoir qu'un nombre fini de points singuliers (où elle n'est pas développable en série entière) et de n'avoir que des singularités de type polaires. Les deux points de vue se rejoignent avec la conséquence que toute fractions rationnelle de  $\mathbb{C}(X)$  peut se récrire de façon unique sous la forme

$$\frac{f}{g} = c_{r_\infty}^{(\infty)} X^{r_\infty} + \dots + c_1^{(\infty)} X + \sum_{i=1}^s \left( \frac{c_{r_i}^{(i)}}{(X - \alpha_i)^{r_i}} + \dots + \frac{c_1^{(i)}}{X - \alpha_i} \right) + c_0$$

pour des complexes uniquement déterminés  $\alpha_i$ ,  $c_0$  et  $c_j^{(i)}$ .

De manière générale, le problème de l'intégration formelle, de même que sa généralisation à la résolution d'équation différentielles linéaires en solutions rationnelles, repose sur la compréhension de l'action de la dérivation sur les singularités des fonctions. Dans le cas qui nous occupe, la « difficulté » mathématique de l'intégration formelle repose sur le fait que l'intégration des pôles finis d'ordre 1 engendre des logarithmes.

En calcul formel, une difficulté supplémentaire est de pouvoir travailler avec des expressions rationnelles sur une extension algébrique finie  $k$  de  $\mathbb{Q}$  telle que les polynômes de  $k[X]$  ne se factorisent pas nécessairement en facteurs linéaires. En particulier, on s'intéresse aussi à fournir des primitives exprimées lorsque cela est possible avec des coefficients de  $\mathbb{Q}$  et d'éviter l'introduction de nombres complexes.

Dans ce qui suit,  $M(n)$  représente la complexité arithmétique de la multiplication de deux polynômes de degrés au plus  $n$  et  $\omega$  est l'exposant de la complexité arithmétique de l'algèbre linéaire pour des matrices de taille  $n \times n$ . Par exemple,  $M(n) = O(n \ln n \ln \ln n)$  pour la multiplication par FFT ; par ailleurs,  $2 \leq \omega \leq 3$ , la borne supérieure correspondant au produit matriciel naïf. L'objectif est ici de décrire un algorithme pour l'intégration d'une fraction rationnelle  $f/g$  pour des polynômes  $f$  et  $g$  de degrés bornés par  $n$  en complexité arithmétique  $O(M(n)^2 \ln n)$ , modulo le coût de factorisation d'un résultant de degré au plus  $n$  (mais potentiellement assez petit).

## 5.2 Intégration de la partie polynomiale

En considérant la décomposition en éléments simples présentée plus haut, une partie de la fraction rationnelle  $f/g$  à intégrer à un comportement simple, à savoir la « partie polynomiale » provenant du « pôle » à l'infini.

**Algorithme** (Intégration de la partie polynomiale).

ENTRÉE : une primitive  $\int f/g$  à calculer pour des polynômes  $f$  et  $g$  de degrés au plus  $n$  donnés par leur développements

SORTIE : des polynômes  $Q$  et  $h$ , le premier de degré moindre que  $n$ , le second de degré strictement moindre que  $n$ , tels que  $\int f/g = Q + \int h/g$

COMPLEXITÉ ARITHMÉTIQUE :  $O(M(n))$

1. calculer le quotient  $q$  et le reste  $h$  de la division euclidienne de  $f$  par  $g$
2. calculer  $Q = q_d X^{d+1}/(d+1) + \dots + q_0 X$  à partir de  $q = q_d X^d + \dots + q_0$
3. renvoyer l'expression  $Q + \int h/g$

*Preuve de l'algorithme.* La complexité de l'intégration de  $q$  étant linéaire en  $d$ , la complexité dominante est celui de la division euclidienne, en  $O(M(n))$ .  $\square$

Pour la suite, l'intégration de  $h/g$  va reposer sur la détermination de deux fractions rationnelles  $c/d$  et  $a/b$  telles que  $\int h/g = c/d + \int a/b$ . La première fraction  $c/d$  est la « partie rationnelle » de l'intégrale  $\int f/g$  initiale et l'intégrale  $\int a/b$  qu'il restera à déterminer est sa « partie logarithmique », que nous allons réexprimer comme combinaison linéaire de logarithmes.

## 5.3 Partie sans carré et factorisation sans carré

Il est bien connu que tout polynôme unitaire  $f$  de  $k[X]$  se factorise de façon unique (à permutation près des facteurs) sous la forme

$$f = f_1^{e_1} \dots f_r^{e_r}$$

pour des polynômes irréductibles unitaires  $f_i$  deux à deux premiers entre eux et des entiers strictement positifs  $e_i$ . En regroupant les facteurs de même exposant, on obtient une autre factorisation en termes de polynômes unitaires  $g_i$  deux à deux premiers entre eux, de la forme

$$f = g_1 g_2^2 \dots g_m^m.$$

Dans cette écriture, chacun des  $g_i$  est sans carré, au sens où aucun polynôme non constant a son carré qui divise  $g_i$ . Il en est de même du produit  $g_1 \dots g_m$ , ce qui motive la définition suivante.

**Définition.** En termes de la notation ci-dessus, le polynôme  $f_1 \dots f_r = g_1 \dots g_m$  est appelé *partie sans carré* du polynôme unitaire  $f$  et l'expression  $g_1 g_2^2 \dots g_m^m$  est appelée *factorisation sans carré* de  $f$ .

Si pour un polynôme  $g$ , une puissance  $g^i$  divise  $f$ , on trouve un polynôme  $h$  tel que  $f = g^i h$ . Par dérivation, on a l'égalité  $f' = g^{i-1}(ig'h + gh')$ , donc que  $g^{i-1}$  divise  $f'$ . Ainsi,  $g^{i-1}$  divise le P.G.C.D.  $f \wedge f'$  et il en est de même pour le produit  $g_2 g_3^2 \dots g_m^{m-1}$ .

Inversement, comme  $f = g_i^i h$  pour un certain polynôme  $h$  premier avec  $g_i$ ,  $f' = g_i^{i-1}(ig_i' h + g_i h')$  est divisible par  $g_i^i$  si et seulement si  $g_i$  divise  $ig_i'$ , d'où, par comparaison des degrés, si et seulement si  $ig_i'$  est nul. Pour exclure ce cas, on fera dorénavant l'hypothèse que le corps  $k$  est de caractéristique nulle. Donc, chaque  $g_i^{i-1}$ , mais aucun des  $g_i^i$ , divise  $f \wedge f'$  et finalement  $g_2 g_3^2 \dots g_m^{m-1}$  divise  $f \wedge f'$ .

Ainsi, puisque  $g_2 g_3^2 \dots g_m^{m-1}$  et  $f \wedge f'$  sont unitaires, ils sont égaux et égaux à  $f_1^{e_1-1} \dots f_r^{e_r-1}$ . Cette égalité donne l'idée de l'algorithme qui suit.

**Algorithme** (Partie sans carré d'un polynôme).

ENTRÉE : un polynôme unitaire  $f$  de degré  $n$

SORTIE : la partie sans carré de  $f$

COMPLEXITÉ ARITHMÉTIQUE :  $O(M(n) \ln n)$

1. calculer le P.G.C.D.  $u = f \wedge f'$  par l'algorithme d'Euclide
2. calculer le quotient de la division  $f/u$  et le renvoyer

*Preuve de l'algorithme.* La complexité de l'algorithme d'Euclide est de  $O(M(n) \ln n)$  et domine celle de la division,  $O(M(n))$ .  $\square$

Avec les mêmes notations que ci-dessus, la première étape de l'algorithme calcule  $g_2 g_3^2 \dots g_m^{m-1}$ . En répétant le calcul sur ce résultat intermédiaire, on obtient  $g_3 g_4^2 \dots g_m^{m-2}$ , et ainsi de suite jusqu'à obtenir  $g_m$ . Ceci donne un algorithme de complexité presque optimale pour le calcul d'une factorisation sans carré.

**Algorithme** (Factorisation sans carré d'un polynôme).

ENTRÉE : un polynôme unitaire  $f$  de degré  $n$

SORTIE : la factorisation sans carré de  $f$ ,  $f = g_1 g_2^2 \dots g_m^m$

COMPLEXITÉ ARITHMÉTIQUE :  $O(mM(n) \ln n)$

1. poser  $u_0 = f$
2. en partant de  $i = 1$ , calculer  $u_i = u_{i-1} \wedge u_{i-1}'$  par l'algorithme d'Euclide et les quotients  $v_i = u_{i-1}/u_i$ , ce jusqu'à trouver  $u_i = 1$
3. appeler  $m$  la dernière valeur de  $i$  pour laquelle  $u_i$  est autre que 1
4. pour  $i$  de 1 à  $m - 1$ , calculer  $h_i = v_i/v_{i+1}$  et poser  $h_m = v_m$
5. renvoyer la factorisation  $h_1 h_2^2 \dots h_m^m$

*Preuve de l'algorithme.* On a immédiatement les relations  $u_i = g_{i+1} g_{i+2}^2 \dots g_m^{m-i}$ ,  $v_i = g_i \dots g_m$  et  $h_i = g_i$ . La complexité reste encore dominée par celle de l'algorithme d'Euclide. Le nombre d'étapes de la boucle est  $m$ , d'où la complexité annoncée.  $\square$

Un autre algorithme (non présenté en cours), l'algorithme de Yun, effectue cette factorisation en complexité arithmétique  $O(M(n) \ln n)$ , donc sans le facteur arithmétique  $m$ .

## 5.4 Décomposition en fractions partielles relativement à une factorisation sans carré

La détermination des parties rationnelle et logarithmique d'une intégrale  $\int h/f$  où le polynôme  $h$  est de degré strictement moindre que celui du polynôme unitaire  $f$  s'obtient après avoir décomposé la fraction  $h/f$  en « fractions partielles » relativement à la factorisation sans carré de  $f$ . L'idée de la décomposition en fractions partielles, *partial fractions* en anglais, est une généralisation de la décomposition en éléments simples qui ne sépare pas les facteurs irréductibles du dénominateur lorsqu'ils peuvent être traités en parallèle.

En repartant de la notation  $f = f_1^{e_1} \dots f_r^{e_r} = g_1 g_2^2 \dots g_m^m$ , on cherche d'abord à écrire la fraction  $h/f$  sous la forme

$$\frac{h}{f} = \frac{p_1}{g_1} + \frac{p_2}{g_2^2} + \dots + \frac{p_m}{g_m^m}$$

où chaque polynôme  $p_i$  a degré strictement inférieur à celui de  $g_i^i$ , avant de scinder chaque  $p_i/g_i^i$  sous la forme

$$\frac{p_i}{g_i^i} = \frac{p_{i,i}}{g_i^i} + \dots + \frac{p_{i,1}}{g_i}$$

pour des polynômes  $p_{i,j}$  de degré strictement inférieur à celui de  $g_i$ . Notons encore que les  $g_i$  ne sont pas nécessairement irréductibles.

Après multiplication par  $f$ , la première relation cherchée devient

$$h = p_1 \widehat{g_1} g_2^2 \dots g_m^m + \dots + p_i g_1 \dots \widehat{g_i^i} \dots g_m^m + \dots p_m g_1 \dots g_{m-1}^{m-1} \widehat{g_m^m},$$

où le chapeau représente un facteur omis. Pour chaque  $i$ , le facteur  $g_i^i$  intervient en facteur de tous les termes de la somme sauf un, d'où les relations de congruence

$$h \equiv p_i g_1 \dots \widehat{g_i^i} \dots g_m^m \pmod{g_i^i}.$$

Les polynômes unitaires  $g_j^j$  étant deux à deux premiers entre eux, chaque  $g_j^j$  pour  $j \neq i$  est inversible modulo  $g_i^i$  et on a la nouvelle congruence

$$p_i \equiv h g_1^{-1} \dots \widehat{g_i^{-i}} \dots g_m^{-m} \pmod{g_i^i}.$$

Les polynômes  $p_i$  sont donc uniquement déterminés par la contrainte de degré annoncée plus haut.

Quant au passage de  $p_i$  aux  $p_{i,j}$ , une approche possible consiste à poser  $q_i = p_i$ , puis à calculer les divisions euclidiennes  $q_j = q_{j-1} g_i + p_{i,j}$  pour  $j$  de  $i$  à 2. On a alors  $p_i = p_{i,1} g_i^{i-1} + \dots + p_{i,i}$ , d'où l'expression désirée pour  $p_i/g_i^i$ .

On a ainsi l'algorithme suivant.

**Algorithme** (Décomposition en fractions partielles relativement à une factorisation sans carré).

ENTRÉE : une fraction rationnelle  $h/f$  pour un polynôme  $f$  de degré  $n$  et un polynôme  $h$  de degré strictement inférieur à  $n$ , ainsi que la factorisation sans carré  $f = g_1 g_2^2 \dots g_m^m$

SORTIE : des polynômes  $p_{i,j}$  pour  $1 \leq j \leq i \leq m$  avec chaque  $p_{i,j}$  de degré strictement moindre que  $g_i$ , et tels que  $h/f = \sum_{i=1}^m \sum_{j=1}^i p_{i,j}/g_i^j$

COMPLEXITÉ ARITHMÉTIQUE :  $O(mM(n) \ln n)$

1. pour  $i$  de 1 à  $m$

(a) calculer  $u_i = f/g_i^i$

(b) calculer une relation de Bézout  $a_i u_i + b_i g_i^i = 1$  par l'algorithme d'Euclide étendu

(c) calculer le reste  $p_i$  du produit  $h a_i$  modulo  $g_i^i$

(d) poser  $q_i = p_i$ , puis effectuer les divisions  $q_j = q_{j-1} g_i + p_{i,j}$  pour  $j$  de  $i$  à 2

2. renvoyer les  $p_{i,j}$  pour  $1 \leq j \leq i \leq m$

*Preuve de l'algorithme.* Connaissant  $h$ ,  $f$ , et les  $g_i^i$ , la détermination de chaque  $p_i$  par le calcul qui vient d'être esquissé fait une division exacte de polynômes de degrés au plus  $n$ , celle de  $f$  par  $g_i^i$ , une inversion de polynômes de degré au plus  $n$  (par l'algorithme d'Euclide étendu), une multiplication en degrés au plus  $n$  et calcul de reste de division de polynômes de degré au plus  $2n$  par des polynômes de degré au plus  $n$ . D'où une complexité totale pour le calcul des  $p_i$  en  $O(mM(2n) \ln(2n))$ , qui est aussi  $O(mM(n) \ln n)$ . Reste à extraire les  $p_{i,j}$  à partir des  $p_i$ . Pour chaque  $i$ , la complexité arithmétique est en  $O(iM(\deg g_i)) + O((i-1)M(\deg g_i)) + \dots + O(M(\deg g_i))$ , soit en  $O(i^2M(\deg g_i))$ . En sommant sur  $i$ , on obtient, par sous-additivité de  $M$ , la complexité

$$\sum_{i=1}^m O(i^2M(\deg g_i)) \leq O\left(mM\left(\sum_{i=1}^m i \deg g_i\right)\right) \leq O(mM(n)),$$

complexité qui reste dominée par celle du reste de l'algorithme.  $\square$

Indiquons une autre approche, récursive, pour le calcul des  $p_{i,j}$  à partir des  $p_i$ , qui donnera une complexité en  $O(M(n) \ln n)$ . Par simplicité, donnons l'idée pour  $f$  de la forme  $g_m^m$  avec  $m = 2^k$  une puissance de 2, et notons  $d = \deg g$ , si bien que  $n = 2^k d$ . On effectue d'abord une division euclidienne en taille  $n/2$ , celle de  $p_m$  par  $g^{m/2}$ , puis deux en taille  $n/4$ , celles du quotient et du reste par  $g^{m/4}$ , puis quatre en taille  $n/8$ , celles des deux quotients et des deux restes obtenus, et ainsi de suite. La complexité obtenue est alors  $O(M(n/2)) + 2O(M(n/4)) + \dots + 2^{k-1}O(M(n/2^k))$ , qui par sous-additivité de  $M$  est majorée par  $O(M(n/2) \ln n)$ . Par ailleurs, le calcul de  $g, g^2, g^4, \dots, g^m$  coûte  $O(M(n))$  opérations arithmétiques, encore une fois par sous-additivité de  $M$ , d'où la complexité globale annoncée.

## 5.5 Intégration de la partie rationnelle

À ce stade, on a ramené, en complexité essentiellement linéaire, le problème de l'intégration d'une fraction rationnelle sous forme normale à celui de l'intégration d'une expression de la forme

$$\sum_{i=1}^m \sum_{j=1}^i \frac{p_{i,j}}{g_i^j}$$

pour des polynômes  $p_{i,j}$  de degré strictement moindre que  $g_i$ .

Considérons un instant un terme de la somme,  $p_{i,j}/g_i^j$ . Chaque  $g_i$  étant sans carré, on a une relation de Bézout,

$$s_i g_i' + t_i g_i = 1$$

pour des polynômes  $s_i$  et  $t_i$ . En multipliant cette relation par  $p_{i,j}$ , on déduit la relation

$$\int \frac{p_{i,j}}{g_i^j} = \int \frac{-s_i p_{i,j}}{j-1} \cdot \frac{-(j-1)g_i'}{g_i^j} + \int \frac{t_i p_{i,j}}{g_i^{j-1}} = \frac{-s_i p_{i,j}}{(j-1)g_i^{j-1}} + \int \frac{t_i p_{i,j} + (s_i p_{i,j})' / (j-1)}{g_i^{j-1}}$$

par intégration par parties. On a ainsi ramené l'intégration d'un pôle d'ordre  $j$  à celle d'un pôle d'ordre  $j-1$ . Ceci suggère une méthode itérative pour l'intégration de la partie rationnelle, en commençant par les ordres maximaux; c'est le procédé de réduction de Hermite.

**Algorithme** (Intégration de la partie rationnelle par réduction de Hermite).

ENTRÉE : une fraction rationnelle  $h/f$  avec  $f$  de degré  $n$  et  $h$  de degré strictement inférieur à  $n$ , ainsi que la décomposition  $\sum_{i=1}^m \sum_{j=1}^i \frac{p_{i,j}}{g_i^j}$  en fractions partielles relativement à la factorisation sans carré  $f = g_1 g_2^2 \dots g_m^m$

SORTIE : des polynômes  $a_\ell, b_\ell, c_\ell$  et  $d_\ell$  vérifiant la relation  $\int h/f = \sum_\ell c_\ell/d_\ell + \int \sum_\ell a_\ell/b_\ell$  et tels que les  $b_\ell$  divisent la partie sans carré  $g_1 \dots g_m$  et les  $d_\ell$  divisent  $g_2 \dots g_m^{m-1}$

COMPLEXITÉ ARITHMÉTIQUE :  $O(M(n) \ln n)$

1. faire  $u = 0$
2. pour  $i$  de 1 à  $m$ 
  - (a) par l'algorithme d'Euclide étendu, calculer une relation de Bézout  $s_i g'_i + t_i g_i = 1$  pour des polynômes  $s_i$  et  $t_i$  de degré strictement inférieur à celui de  $g_i$
  - (b) pour  $j$  de  $i$  à 2
    - i. effectuer la division euclidienne de  $s_i p_{i,j}$  par  $g_i$  pour trouver  $s_i p_{i,j} = q g_i + \bar{s}$  avec un reste  $\bar{s}$  de degré strictement inférieur à  $g_i$
    - ii. poser  $\bar{t} = t_i p_{i,j} + q g'_i$
    - iii. ajouter  $\bar{t} + \bar{s}'/(j-1)$  à  $p_{i,j-1}$  et normaliser
    - iv. retrancher  $\bar{s}/(j-1)/g_i^{j-1}$  de  $u$  sans normalisation
3. exprimer  $\sum_{i=1}^m p_{i,1}/g_i$  sous la forme  $\sum_{\ell} a_{\ell}/b_{\ell}$  et  $u$  sous la forme  $\sum_{\ell} c_{\ell}/d_{\ell}$
4. renvoyer les  $a_{\ell}$ ,  $b_{\ell}$ ,  $c_{\ell}$  et  $d_{\ell}$

*Preuve de l'algorithme.* Appelons  $d_i$  le degré de  $g_i$ . Pour chaque  $i$ , le calcul de  $s_i$  et  $t_i$  a lieu en  $O(M(d_i) \ln d_i)$  opérations arithmétiques. Pour chaque étape de la réduction de Hermite, le calcul de  $\bar{s}$  et  $\bar{t}$  se fait en complexité  $M(d_i)$ , la mise à jour de  $p_{i,j-1}$  en  $O(d_i)$ . En effet,  $\bar{s}$  est par construction de degré inférieur à  $d_i$  et puisqu'on a la relation  $\bar{s} g'_i + \bar{t} g = p_{i,j}$ , par comparaison des degrés on obtient que  $\bar{t}$  est aussi de degré inférieur à  $d_i$ . La complexité totale est donc, par sous-additivité de  $M$ ,

$$\sum_{i=1}^m O(M(d_i) \ln d_i) + \sum_{i=1}^m O(iM(d_i)) \leq O\left(M\left(\sum_{i=1}^m d_i\right)\right) \ln n + O\left(M\left(\sum_{i=1}^m i d_i\right)\right) \leq O(M(n) \ln n).$$

Par ailleurs, les  $d_{\ell}$  sont par construction de la forme  $g_i^{j-1}$  et divisent donc  $g_i^{i-1}$ ; quant aux  $b_{\ell}$ , ce sont en fait des  $g_i$ .  $\square$

Notons que l'algorithme tel qu'il est donné ci-dessus ne renvoie pas un résultat sous la forme  $c/d + \int a/b$ , pour deux fractions rationnelles  $a/b$  et  $c/d$  sous forme normalisée, mais donne plutôt ces deux fractions rationnelles sous forme de sommes d'expressions rationnelles. Dans les systèmes de calcul formel, cette mise sous forme normale est laissée à l'initiative de l'utilisateur.

Prenons l'exemple du calcul de

$$\int \frac{1}{(2X^2 + 1)^2}.$$

Ici, nous avons simplement  $h = 1/4$  et  $f = g_2^2$  pour  $g_2 = X^2 + 1/2$ . Comme  $g'_2 = 2X$ , nous trouvons la relation de Bézout  $-X g'_2 + 2g_2 = 1$ , d'où la réduction

$$\int \frac{1}{(2X^2 + 1)^2} = \int \frac{X}{4} \frac{-2X}{(X^2 + 1/2)^2} + \int \frac{1/2}{X^2 + 1/2} = \frac{X}{2(2X^2 + 1)} + \int \frac{1}{2(2X^2 + 1)}.$$

La structure des  $b_{\ell}$  et celle des  $d_{\ell}$  suggèrent de rechercher une primitive de la partie rationnelle directement sous la forme  $c/d + \int a/b$ . En suivant le calcul des  $a_{\ell}$  et des  $c_{\ell}$  au cours de l'algorithme précédent, il apparaît que les polynômes  $a$  et  $c$  ont des degrés strictement inférieurs à  $d_1 + \dots + d_m$  et  $d_2 + 2d_3 + \dots + (m-1)d_m$ , respectivement, d'où l'algorithme suivant, par coefficients indéterminés, dû à Horowitz en 1971. Cette méthode est de moins bonne complexité que la méthode de Hermite, mais est bien pratique pour des fractions de petite taille si l'on ne dispose pas du temps pour bien programmer la méthode de Hermite.

**Algorithme** (Intégration de la partie rationnelle par l'algorithme de Horowitz).

ENTRÉE : une fraction rationnelle  $h/f$  avec  $f$  de degré  $n$  et  $h$  de degré strictement inférieur à  $n$ , ainsi que la factorisation sans carré  $f = g_1 g_2^2 \dots g_m^m$

SORTIE : des polynômes  $a$  et  $c$  vérifiant la relation  $\int h/f = c/(g_2 \dots g_m^{m-1}) + \int a/(g_1 \dots g_m)$

COMPLEXITÉ ARITHMÉTIQUE :  $O(n^\omega)$

1. poser  $\delta = d_1 + \dots + d_m$  et écrire  $a = a_0 + \dots + a_{\delta-1}X^{\delta-1}$  et  $c = c_0 + \dots + c_{n-\delta-1}X^{n-\delta-1}$  pour des coefficients indéterminés
2. écrire  $h = c'g_1 \dots g_m - c \sum_{i=2}^m (i-1)g_1 \dots g'_i \dots g_m + ag_2 \dots g_m^{m-1}$  et égaliser les coefficients en  $X$  à zéro
3. résoudre le système linéaire obtenu
4. substituer dans  $a$  et  $c$  pour renvoyer le résultat

*Preuve de l'algorithme.* La relation polynomiale servant à déterminer le système linéaire s'obtient en dérivant  $\int h/f = c/(g_2 \dots g_m^{m-1}) + \int a/(g_1 \dots g_m)$  et en chassant les dénominateurs. Le coût des multiplications de polynômes est dominé par celui de l'algèbre linéaire sur le système qui est de dimension  $n \times (n-2)$ .  $\square$

Reprenons l'exemple de l'intégration de  $1/(2X^2 + 1)^2$ , avec toujours  $h = 1/4$ ,  $f = g_2^2$  pour  $g_2 = X^2 + 1/2$  et  $g'_2 = 2X$ . La mise en équation par la méthode d'Horowitz donne

$$1/4 = c'(X^2 + 1/2) - c(2X) + a(X^2 + 1/2)$$

avec  $a = a_0 + a_1X$  et  $c = c_0 + c_1X$  vu que  $\delta = 2$ . Le système linéaire se résout par  $a_0 = 1/2$ ,  $a_1 = 0$ ,  $c_0 = 0$ ,  $c_1 = 1/4$ , ce qui redonne la primitive déjà calculée par la méthode de Hermite.

## 5.6 Algèbre différentielle pour l'intégration rationnelle

Que ce soit par la méthode de Hermite ou par celle d'Horowitz, on a ramené l'intégration d'une fraction rationnelle générale à celle d'une expression rationnelle de la forme  $a/b$  pour  $b$  sans carré et  $a$  de degré strictement inférieur à  $b$ . L'exemple le plus simple est maintenant celui de l'intégration de la fraction  $1/x$  et chacun s'attend dès lors à ce que l'intégration rationnelle introduise des logarithmes. Comme on l'a déjà annoncé, on se dote d'un cadre algébrique pour évacuer les questions de déterminations multiples des logarithmes. Cette section introduit la terminologie d'algèbre différentielle utile pour notre problème.

Les définitions qui suivent soulignent le fait qu'il est possible de considérer l'opération de dérivation sans plus nécessiter de référence à aucune variable.

**Définition.** Une *dérivation* d'un anneau  $A$  est une application  $a \mapsto a'$  de  $A$  dans lui-même qui est additive, au sens où  $(a+b)' = a' + b'$  pour tous éléments  $a$  et  $b$  de  $A$ , et qui vérifie la règle de Leibniz  $(ab)' = a'b + ab'$ . L'anneau  $A$  est alors appelé un *anneau différentiel*. Si l'anneau  $A$  est un corps, il est dit *corps différentiel*. S'il est une algèbre sur un corps commutatif  $k$  et si la dérivation est l'application nulle sur  $k$ , l'anneau  $A$  est dit une  *$k$ -algèbre différentielle*.

Étant donné un corps commutatif  $k$ , nous allons donner plusieurs exemples de structures de  $k$ -algèbres différentielles sur l'anneau des polynômes  $A = k[X]$ . Notons d'abord la relation  $f(X)' = D(f)(X)X'$  pour tout polynôme  $f$  de dérivée formelle usuelle  $D(f)$ , que l'on montre aisément d'abord sur les monômes  $X^i$  par récurrence sur le degré  $i$ . Pour  $X' = 1$ , on obtient la  $k$ -algèbre différentielle avec pour dérivation la dérivation formelle usuelle des polynômes. Pour  $X' = 0$ , on obtient la dérivation triviale, nulle. Pour  $X' = X$ , on obtient une dérivation sur  $A = k[X]$  qui donne une structure différentielle isomorphe à celle de la  $k$ -algèbre  $k[e^\theta]$  avec dérivation par rapport à la variable  $\theta$ , par l'isomorphisme d'algèbre donné par  $X \mapsto e^\theta$ .

Notons encore qu'il existe une unique extension d'une structure d'anneau différentiel sur  $k[X]$  en une structure de corps différentiel sur  $k(X)$ . En effet, on a nécessairement, pour tout  $a$  de  $A$ ,  $0 = 1' = (aa^{-1})' = a'a^{-1} + a(a^{-1})'$ , d'où  $(a^{-1})' = -a^{-2}a'$ .

Les définitions qui suivent donnent un cadre pour étendre le corps des fractions rationnelles par des objets algébriques qui se comportent comme des logarithmes.



*Démonstration.* Pour montrer l'implication directe, supposons  $\int a/b = \sum_{i=1}^{\ell} c_i \ln v_i$ , qui par dérivation conduit à  $a/b = \sum_{i=1}^{\ell} c_i v'_i/v_i$ , puis, après avoir multiplié par le produit convenable, à  $av_1 \dots v_{\ell} = b \sum_{i=1}^{\ell} c_i v_1 \dots v'_i \dots v_{\ell}$ . Comme les  $v_i$  sont sans carré et deux à deux premiers entre eux, par réduction modulo  $v_i$  on trouve que chaque  $v_i$  divise  $b$ , donc que le produit  $v_1 \dots v_{\ell}$  divise  $b$ . Comme par ailleurs  $a$  et  $b$  sont premiers entre eux,  $b$  divise le produit  $v_1 \dots v_{\ell}$ . Ces deux polynômes étant unitaires, ils sont égaux. On a donc les égalités  $a = \sum_{i=1}^{\ell} c_i v_1 \dots v'_i \dots v_{\ell} = (\sum_{i=1}^{\ell} c_i v'_i/v_i)b$ , d'où il vient  $a - b'Y = \sum_{i=1}^{\ell} (c_i - Y)v_1 \dots v'_i \dots v_{\ell}$ . Ainsi, le P.G.C.D.  $b \wedge (a - b'Y)$  est non-trivial si et seulement si  $Y = c_i$  pour l'un des  $i$  et il vaut  $v_i$  pour le même  $i$  dans ce cas, et le résultant  $R$  est non-nul sous les mêmes conditions équivalentes. On a donc une factorisation de  $R$  en facteurs linéaires de la forme  $Y - c_i$ .

Pour l'implication converse, considérons une clôture algébrique  $\bar{K}$  de  $K$  et notons d'abord que pour tout  $c$  de  $\bar{K}$ , le résultant  $R$  s'annule en  $c$  si et seulement s'il existe un zéro  $\mu$  de  $b$  dans  $\bar{K}$  annulant simultanément  $a(\mu) - b'(\mu)c$ . Dans ce cas, puisque  $b$  est sans carré,  $b'(\mu)$  ne peut être nul et on a  $c = a(\mu)/b'(\mu)$ . Introduisons l'application  $\phi$  de  $b^{-1}(0)$  dans  $R^{-1}(0)$  qui à un zéro  $\mu$  de  $b$  associe  $a(\mu)/b'(\mu)$ , un zéro de  $R$ . Par l'équivalence qui vient d'être donnée, cette application  $\phi$  est bien définie et surjective. Notons  $c_1, \dots, c_{\ell}$  les zéros distincts de  $R$ . On a alors

$$\prod_{\mu \in \phi^{-1}(c_i)} (X - \mu) = b \wedge (a - b'c_i) = v_i,$$

puis par produit sur  $i$ ,

$$b = \prod_{\mu \in b^{-1}(0)} (X - \mu) = v_1 \dots v_{\ell}.$$

On a donc pour tout  $i$  et tout  $\mu$  dans  $\phi^{-1}(c_i) = v_i^{-1}(0)$  les égalités

$$\left( \left( \sum_{j=1}^{\ell} c_j \frac{v'_j}{v_j} \right) b \right) (\mu) = c_i v_1(\mu) \dots v'_i(\mu) \dots v_{\ell}(\mu) = c_i b'(\mu) = a(\mu).$$

Les polynômes  $(\sum_{i=1}^{\ell} c_i v'_i/v_i)b$  et  $a$  sont de degré strictement inférieur à  $n$  et coïncident sur les  $n$  racines distinctes de  $b$ ; ils sont donc égaux. On a ainsi qu'une primitive de  $a/b$  est la combinaison linéaire de logarithmes  $\sum_{i=1}^{\ell} c_i \ln v_i$ .  $\square$

**Algorithme** (Algorithme de Rothstein–Trager).

ENTRÉE : une fraction rationnelle  $a/b$  de  $k(X)$  sous forme réduite, avec  $b$  unitaire, sans carré, de degré  $n$  et  $a$  de degré strictement inférieur à  $n$

SORTIE : une extension algébrique finie  $K$  de  $k$ , des constantes  $c_i$  de  $K$  et des polynômes  $v_i$  de  $K[X]$  tels que  $\int a/b = c_1 \ln v_1 + \dots + c_{\ell} \ln v_{\ell}$

COMPLEXITÉ ARITHMÉTIQUE :  $O(M(n)^2 \ln n)$  plus le coût de la factorisation du résultant  $R$  ci-dessous, de degré au plus  $n$

1. calculer  $R(Y) = \text{res}_X(b, a - b'Y)$
2. factoriser  $R$  en facteurs linéaires en introduisant une extension algébrique adéquate  $K$  de  $k$
3. appeler  $c_1, \dots, c_{\ell}$  les zéros deux à deux distincts de  $R$  dans  $K$
4. pour chaque  $i$ , calculer  $v_i = b \wedge (a - c_i b')$
5. renvoyer une description de  $K$ , les  $c_i$  et les  $v_i$

*Preuve de l'algorithme.* La correction de l'algorithme provient immédiatement du théorème de structure précédent. Pour une complexité optimale, le résultant calculé à l'étape 1 doit être obtenu par l'algorithme d'Euclide. Les polynômes  $b$  et  $a - b'Y$  sont de degré  $O(n)$  en  $X$ , d'où une complexité arithmétique en  $O(M(n) \ln n)$  opérations dans  $k[Y]$ . Les coefficients polynomiaux de  $k[Y]$  ayant des degrés pouvant atteindre  $n$ , la complexité du calcul de ce résultant est donc de  $O(M(n)^2 \ln n)$  opérations dans  $k$ . De la même façon, la complexité arithmétique sur  $k$  du calcul des  $v_i$  doit tenir compte du degré de l'extension algébrique  $K$ , potentiellement aussi grand que  $n$ , donnant encore une fois  $O(M(n)^2 \ln n)$  opérations dans  $k$ .  $\square$

Considérons l'exemple de l'intégration de  $1/(X^3 + X)$ . On a d'abord le calcul naïf suivant, qui passe par les complexes et la décomposition en éléments simples classique :

$$\int \frac{1}{X^3 + X} = \int \left( \frac{1}{X} - \frac{1/2}{X-i} - \frac{1/2}{X+i} \right) = \ln X - \frac{1}{2} \ln(X-i) - \frac{1}{2} \ln(X+i) = \ln X - \frac{1}{2} \ln(X^2 + 1).$$

En suivant la méthode de Rothstein–Trager, on calcule d'abord le résultant

$$R(Y) = \operatorname{res}_X(X^3 + X, 1 - (3X^2 + 1)Y) = \begin{vmatrix} 1 & 0 & -3Y & 0 & 0 \\ 0 & 1 & 0 & -3Y & 0 \\ 1 & 0 & 1-Y & 0 & -3Y \\ 0 & 1 & 0 & 1-Y & 0 \\ 0 & 0 & 0 & 0 & 1-Y \end{vmatrix} = (2Y + 1)^2(1 - Y),$$

qui admet une factorisation en facteurs linéaires sur  $\mathbb{Q}$  sans recours à aucune extension algébrique. On pose donc  $c_1 = 1$  et  $c_2 = -1/2$  et on calcule les P.G.C.D.

$$v_1 = (X^3 + X) \wedge (-3X^2) = X, \quad v_2 = (X^3 + X) \wedge \left( \frac{3}{2} + \frac{3X^2}{2} \right) = X^2 + 1,$$

qui donnent la représentation finale suivante pour une primitive :

$$\int \frac{1}{X^3 + X} = \ln X - \frac{1}{2} \ln(X^2 + 1).$$

Remarquons que la propriété pour une primitive de pouvoir être représentée sans extension algébrique est liée à toute la structure de la fraction rationnelle et non pas seulement aux coefficients avec lesquels des racines complexes conjuguées apparaissent. À titre de comparaison, l'intégration de la fraction  $1/(X^2 + 1)$  par la méthode de Rothstein–Trager donne le résultant

$$R(Y) = \operatorname{res}_X(X^2 + 1, 1 - 2XY) = \begin{vmatrix} 1 & -2Y & 0 \\ 0 & 1 & -2Y \\ 1 & 0 & 1 \end{vmatrix} = 4Y^2 + 1,$$

qui cette fois-ci n'a de factorisation en facteurs linéaires qu'après passage à  $K = \mathbb{Q}[i]$ . On trouve  $c_1 = i/2$ ,  $c_2 = -i/2$ ,  $v_1 = (X^2 + 1) \wedge (1 - iX) = X + i$ ,  $v_2 = (X^2 + 1) \wedge (1 + iX) = X - i$ , d'où

$$\int \frac{1}{X^2 + 1} = \frac{i}{2} \ln(X - i) - \frac{i}{2} \ln(X + i).$$

Par la même méthode, on obtient qu'aucune primitive de  $1/(2X^2 + 1)$  ne s'exprime sans passage aux complexes et que

$$\int \frac{1}{2X^2 + 1} = \frac{i}{2\sqrt{2}} \left( \ln(X + i/\sqrt{2}) - \ln(X - i/\sqrt{2}) \right).$$

On peut donc conclure l'exemple pris pour la méthode de Hermite en donnant l'intégrale

$$\int \frac{1}{(2X^2 + 1)^2} = \frac{X}{2(2X^2 + 1)} + \frac{i}{4\sqrt{2}} \left( \ln(X + i/\sqrt{2}) - \ln(X - i/\sqrt{2}) \right).$$

## 5.8 Complexité globale de l'intégration rationnelle

Pour finir, disons quelques mots sur la complexité globale de l'intégration rationnelle. La méthode de Hermite pour l'intégration de la partie rationnelle a complexité  $O(M(n) \ln n)$ , où  $n$  borne les degrés des numérateurs et dénominateurs en entrée, alors que la méthode de Rothstein–Trager pour l'intégration de la partie logarithmique a complexité  $O(M(n')^2 \ln n')$ , où  $n'$  borne les degrés des numérateurs et dénominateurs des ses entrées. Il semble donc que la complexité globale

soit dominée par celle de l'intégration de la partie logarithmique, mais il faut en réalité préciser le lien entre  $n$  et  $n'$ . Ce dernier nombre étant le degré du dénominateur de la fraction  $a/b$  en sortie de la méthode de Hermite, deux cas extrêmes sont possibles : soit l'intégration d'une fraction  $h/f$  aboutit à une partie polynomiale  $a/b$  donnant  $n'$  de l'ordre de  $n$ , et c'est alors la factorisation du résultant dans l'intégration de la partie logarithmique qui prédomine, avec une complexité arithmétique polynomiale en  $n$ , soit l'intégration aboutit à une partie polynomiale donnant un  $n'$  significativement plus petit que  $n$ , ce qui est le cas quand la factorisation sans carré de  $f$  fait intervenir un  $g_m^m$  pour un  $m$  grand, et la complexité globale reste dominée par le coût de la méthode de Hermite.

## Bibliographie

- [1] BRONSTEIN, M. *Symbolic integration. I*, vol. 1 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1997. Transcendental functions, With a foreword by B. F. Caviness.
- [2] GEDDES, K. O., CZAPOR, S. R., AND LABAHN, G. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992.
- [3] VON ZUR GATHEN, J., AND GERHARD, J. *Modern computer algebra*. Cambridge University Press, New York, 1999.

Ce cours s'appuie en particulier sur les sections 5.11 et 14.6 et le chapitre 22 de [3]. Le même sujet est traité au chapitre 11 de [2], en n'abordant cependant absolument pas les questions de complexité ; le prolongement de ces méthodes au cadre des fonctions liouvilienues par l'algorithme de Risch y est fait au chapitre 12 de [2]. Le livre [1] est à l'heure actuelle la référence la plus aboutie sur le sujet.



## Chapitre 6

# Sommation et intégration symboliques des fonctions spéciales

### 6.1 Expression de la création télescopique en termes d'algèbres de Ore rationnelles

On a déjà exposé dans ce cours la méthode de la création télescopique, en l'appliquant à la sommation hypergéométrique définie par une combinaison de l'algorithme de Gosper et d'une idée due à Zeilberger. Cette approche se généralise en des algorithmes de sommation et intégration pour les suites et fonctions  $\partial$ -finies.

Rappelons le principe de la méthode. Soit à évaluer une somme paramétrée

$$F_n = \sum_{k=a}^b f_{n,k}.$$

En toute généralité, le principe de la création télescopique est de déterminer une suite auxiliaire  $g = (g_{n,k})$  ainsi que des coefficients  $\eta_0, \dots, \eta_r$ , fonctions de la variable  $n$ , tels que se trouve vérifiée la relation

$$\eta_r(n)f_{n+r,k} + \dots + \eta_0(n)f_{n,k} = g_{n,k+1} - g_{n,k}.$$

Ici, nous ne faisons pas plus d'hypothèses sur les  $\eta_i$  et  $g$  que celle de pouvoir évaluer la relation ci-dessus pour tout  $n$  quand  $k$  décrit les entiers de  $a$  à  $b$ . Dans ce cas, une sommation sur  $k$  fournit l'égalité

$$\eta_r(n)F_{n+r} + \dots + \eta_0(n)F_n = g_{n,b+1} - g_{n,a}.$$

Ensuite, soit le membre de droite est naturellement nul, soit on recherche un opérateur annulateur de ce second membre; par composition, on obtient une récurrence homogène sur  $F$ .

Des algorithmes d'efficacité différentes ont été donnés selon le domaine de recherche des  $\eta_i$  et de  $g$ , et selon le compromis choisi entre efficacité et richesse de la classe de suites  $f$  en entrée. En particulier, l'algorithme de Zeilberger, optimisé pour une suite  $f$  hypergéométrique, revient à rechercher des  $\eta_i$  polynomiaux et une suite  $g$  similaire à  $f$ , c'est-à-dire un multiple  $\phi f$  pour une fraction rationnelle  $\phi$  en  $n$  et  $k$ . La suite  $g = \phi f$  devant être une somme indéfinie, la recherche de  $\phi$  et des  $\eta_i$  se fait par une variante paramétrée de l'algorithme de Gosper. Notons que le domaine de recherche de  $g$  est l'espace vectoriel  $\mathbb{C}(n, k)f$ , qui n'est autre, dans le cas hypergéométrique, que le module engendré par  $f$  sur l'algèbre de Ore  $A = \mathbb{C}(n, k)\langle S_n, S_k; \sigma_n, \sigma_k, 0, 0 \rangle$ , pour des opérateurs de décalages  $\sigma_n$  et  $\sigma_k$  relatifs à  $n$  et  $k$ . Nous considérons ici la généralisation au cas où  $f$  est une fonction  $\partial$ -finie et où le module  $A \cdot f$  est un espace vectoriel de dimension finie sur  $\mathbb{C}(n, k)$ . Soit

$v_1, \dots, v_d$  les éléments d'une base vectorielle de  $A \cdot f$ , l'algorithme de Zeilberger étendu recherche  $g$  sous la forme indéterminée  $\phi_1 v_1 + \dots + \phi_d v_d$ , pour des fractions rationnelles  $\phi_i$  en  $n$  et  $k$ . Cette recherche se fait par une extension  $\partial$ -finie de la variante paramétrée de l'algorithme de Gosper.

Tout ce qui a été dit s'étend au monde différentiel pour l'évaluation d'une intégrale paramétrée

$$F(x) = \int_a^b f(x, y) dy.$$

On cherche alors une relation

$$\eta_r(x) \frac{\partial^r f}{dx^r}(x, y) + \dots + \eta_0(n) f(x, y) = \frac{\partial g}{dy}(x, y),$$

qui après intégration fournit l'égalité

$$\eta_r(n) F^{(r)}(x) + \dots + \eta_0(n) F(x) = \int_a^b g(x, y) dy.$$

La même méthode permet aussi de traiter des sommes paramétrées continûment,

$$F(x) = \sum_{k=a}^b f_k(x),$$

et des suites d'intégrales de la forme

$$F_n = \int_a^b f_n(y) dy.$$

**Exercice.** Formuler la relation entre  $f$  et  $g$  à rechercher dans ces deux derniers cas.

## 6.2 L'algorithme sur l'exemple $\frac{1}{2} J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \dots = \frac{1}{2}$

Nous allons montrer que la famille paramétrée des fonctions de Bessel de première espèce,  $J_\nu$ , où chaque  $J_\nu$  est une solution que nous allons préciser de l'équation de Bessel

$$x^2 y''(x) + xy'(x) + (x^2 - \nu^2)y(x) = 0,$$

a une somme  $\frac{1}{2} J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \dots$  qui s'évalue à  $\frac{1}{2}$ .

L'équation de Bessel et les fonctions de Bessel peuvent être considérées pour des valeurs complexes du paramètre  $\nu$ , mais vu la nature de la somme à étudier, nous nous limiterons dorénavant à des valeurs entières  $\nu \in \mathbb{N}$ . En étudiant l'équation indicelle de l'équation de Bessel, on s'aperçoit qu'il existe pour chaque  $\nu$  des solutions dans les séries formelles  $\mathbb{C}[[x]]$  et que ces solutions constituent un espace vectoriel de dimension 1 sur  $\mathbb{C}$  de séries. Une base de ces solutions formelles est donnée par la série de Bessel

$$J_\nu(x) = (z/2)^\nu \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{n! (n + \nu)!},$$

de valuation  $\nu$ , qui vu la décroissance de ses coefficients est pour chaque entier  $\nu$  une série entière.

**Exercice.** Vérifier ces résultats.

On vérifie par simple substitution et évaluation que ces fonctions  $J_\nu$  satisfont aussi aux relations

$$xJ'_\nu(x) + xJ_{\nu+1}(x) - \nu J_\nu(x) = 0 \quad \text{et} \quad xJ_{\nu+2}(x) - 2(\nu + 1)J_{\nu+1}(x) + xJ_\nu(x) = 0.$$

En introduisant l'algèbre de Ore  $A = \mathbb{C}(\nu, x)\langle S, D; \sigma, \text{id}, 0, \delta \rangle$  où  $\sigma$  est le décalage avant sur  $\nu$  et  $\delta$  est la dérivation par rapport à  $x$ , on a donc un système d'annulateurs pour  $J$ ,

$$\begin{aligned} p_1 &= x^2 D^2 + xD + (x^2 - \nu^2), \\ p_2 &= xD + xS - \nu, \\ p_3 &= xS^2 - 2(\nu + 1)S + x. \end{aligned}$$

Les deux premiers forment une base de Gröbner de l'idéal engendré pour l'ordre  $\text{lex}(S, D)$ ; les deux derniers pour l'ordre  $\text{lex}(D, S)$ .

Bien évidemment,  $J$  est une fonction  $\partial$ -finie. Le module  $A \cdot J$  est donné, par exemple, comme l'espace vectoriel sur  $\mathbb{C}(\nu, x)$  de base  $(J, S \cdot J)$ . Pour représenter le carré de  $J$  en vue d'une sommation, on peut observer que, en tant qu'espace vectoriel, le module  $A \cdot J^2$  admet la base  $(J^2, J \times (S \cdot J), (S \cdot J)^2)$  et utiliser l'algorithme de clôture par produit pour obtenir une base de Gröbner. En fait, le calcul qui suit n'a même pas besoin d'une représentation aussi explicite de  $J^2$  : pour calculer la somme  $h(x) = \frac{1}{2}J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \dots$  comme fonction de  $x$ , on recherche une fonction  $\eta$  de  $x$ , indépendante de  $\nu$ , telle que  $h' + \eta h$  soit la différence finie en  $\nu$  d'un élément  $g$  de  $A \cdot J^2$ . Pour la suite du calcul, nous fixons cet élément sous la forme indéterminée donnée par

$$g(\nu) = \phi_0(\nu)J_\nu^2 + \phi_1(\nu)J_{\nu+1}^2 + \phi_2(\nu)J_\nu J_{\nu+1},$$

où nous avons omis de faire référence à la variable  $x$  dans les évaluations de  $g$ , des  $\phi_i$  et de  $J$ , car cette variable ne va intervenir que comme paramètre dans le calcul des fractions rationnelles  $\phi_i$ . (On peut penser qu'on travaille temporairement dans l'algèbre de Ore  $A' = \mathbb{C}(\nu, x)\langle S; \sigma, 0 \rangle$ .)

Par construction, on a alors la relation  $h' + \eta h = (S - 1) \cdot g$ , puis, après réduction de chaque occurrence des dérivées et décalées de  $J$  par la base de Gröbner  $\{p_2, p_3\}$ ,

$$\begin{aligned} 2J_\nu J'_\nu + \eta J_\nu^2 &= (S - 1) \cdot (\phi_0(\nu)J_\nu^2 + \phi_1(\nu)J_{\nu+1}^2 + \phi_2(\nu)J_\nu J_{\nu+1}) \\ &= \phi_0(\nu + 1)J_{\nu+1}^2 - \phi_0(\nu)J_\nu^2 + \phi_1(\nu + 1)x^{-2}(2(\nu + 1)J_{\nu+1} - xJ_\nu)^2 - \phi_1(\nu)J_{\nu+1}^2 \\ &\quad + \phi_2(\nu + 1)x^{-1}J_{\nu+1}(2(\nu + 1)J_{\nu+1} - xJ_\nu) - \phi_2(\nu)J_\nu J_{\nu+1}, \end{aligned}$$

laquelle se récrit

$$\begin{aligned} (2\nu x^{-1} + \eta)J_\nu^2 - 2J_\nu J_{\nu+1} \\ &= (\phi_1(\nu + 1) - \phi_0(\nu))J_\nu^2 - (4(\nu + 1)x^{-1}\phi_1(\nu + 1) + \phi_2(\nu + 1) + \phi_2(\nu))J_\nu J_{\nu+1} \\ &\quad + (\phi_0(\nu + 1) + 4(\nu + 1)^2 x^{-2}\phi_1(\nu + 1) - \phi_1(\nu) + 2(\nu + 1)x^{-1}\phi_2(\nu + 1))J_{\nu+1}^2. \end{aligned}$$

Comme les fonctions  $J_\nu^2$ ,  $J_{\nu+1}^2$  et  $J_\nu J_{\nu+1}$  sont linéairement indépendantes sur  $\mathbb{C}(\nu, x)$ , on déduit les relations nécessaires

$$\begin{aligned} -\phi_0(\nu) + \phi_1(\nu + 1) &= (2\nu x^{-1} + \eta), \\ 4(\nu + 1)x^{-1}\phi_1(\nu + 1) + \phi_2(\nu) + \phi_2(\nu + 1) &= 2, \\ \phi_0(\nu + 1) - \phi_1(\nu) + 4(\nu + 1)^2 x^{-2}\phi_1(\nu + 1) + 2(\nu + 1)x^{-1}\phi_2(\nu + 1) &= 0. \end{aligned}$$

En résolvant les deux premières respectivement en  $\phi_0$  et en  $\phi_1$ , puis en substituant dans la dernière, on trouve la récurrence

$$\begin{aligned} x^2(\nu + 1)\phi_2(\nu + 3) - (\nu + 1)(4\nu^2 + 20\nu + 24 - x^2)\phi_2(\nu + 2) \\ + (\nu + 3)(4\nu^2 + 12\nu + 8 - x^2)\phi_2(\nu + 1) - x^2(\nu + 3)\phi_2(\nu) = -4x(\eta\nu^2 + 4\eta\nu + 3\eta + x). \end{aligned}$$

Nous résolvons maintenant celle-ci en ses solutions rationnelles par l'algorithme d'Abramov, dans sa variante paramétrée qui résout en  $\phi_2 \in \mathbb{C}(n, \nu)$  et simultanément en  $\eta \in \mathbb{C}$ . Les coefficients extrêmes de la partie homogène indiquent que toute solution rationnelle doit être polynomiale,

puisque le P. G. C. D.  $((\nu - 3) + 1) \wedge (x + 3)$  vaut 1. La mise sous forme de différences finies de la partie homogène indique que l'opérateur associé accroît de 2 le degré d'un polynôme. Le degré de la partie inhomogène étant 2, toute solution rationnelle ne peut être qu'une constante. On trouve  $\phi_2 = 1$  et  $\eta = 0$ , d'où après report  $\phi_1 = 0$  et  $\phi_0 = -2\nu/x$ . Autrement dit, on a

$$D \cdot J_\nu^2 = (S - 1) \cdot (J_\nu J_{\nu+1} - 2\nu x^{-1} J_\nu^2),$$

qui par sommation fournit

$$D \cdot \sum_{\nu=0}^N J_\nu^2 = J_{N+1} (J_{N+2} - 2(N+1)x^{-1} J_{N+1}) - J_0 J_1.$$

Comme la série  $J_N \in \mathbb{C}[[x]]$  a valuation  $N$ , le membre droit tend vers  $-J_0 J_1 = \frac{1}{2} D \cdot J_0^2$  quand  $N$  tend vers  $\infty$  pour la topologie usuelle donnée par la métrique  $|s| = 2^{-v}$  pour toute série non-nulle  $s$  de valuation  $v$ . On a donc

$$D \cdot \left( \frac{1}{2} J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \dots \right) = 0$$

qui caractérise la somme par une condition initiale. Une simple évaluation en 0 montre que la somme vaut  $\frac{1}{2}$ , ce qui achève la preuve de l'identité annoncée.

### 6.3 Bases de Gröbner de modules et découplage de systèmes

Dans l'exemple qui précède, on a pour le moment effectué le découpler « à la main », mais un procédé systématique et automatique est disponible, par le biais des bases de Gröbner de modules, qui généralise la notion de base de Gröbner pour les idéaux. Cette notion existe tant dans le domaine des polynômes commutatifs que dans le cadre non-commutatif des algèbres de Ore; nous la présentons directement dans ce second cas.

Dans le cas d'un idéal  $I$  d'une algèbre de Ore  $A$ , les éléments de  $I$  s'interprètent comme autant d'équations vérifiées par une fonction inconnue  $\phi$ . Dans une perspective algorithmique, chaque idéal est engendré par un nombre fini de générateurs. Une question naturelle est celle de systèmes linéaires sur un vecteur de fonctions inconnues  $(\phi_1, \dots, \phi_d)$ , à coefficients dans  $A$ . On considère des systèmes d'un nombre fini d'équations de la forme  $g_i = g_{i,1} \cdot \phi_1 + \dots + g_{i,d} \cdot \phi_d$  pour des opérateurs  $g_{i,j}$  de  $A$ . Un tel système se représente de façon compacte un par une matrice  $(g_{i,j})$  à entrées dans  $A$ . Les questions qui sont alors naturelles sont celle de l'algèbre linéaire pour ces matrices, dont en particulier celle de donner un algorithme du pivot de Gauss pour des coefficients dans  $A$ , c'est-à-dire non plus dans un corps, mais dans un anneau, et non-commutatif de surcroît.

Pour ce faire, au lieu de considérer simplement l'algèbre de Ore  $A = k(x)\langle \partial; \sigma, \delta \rangle$  munie d'un ordre monomial sur les  $\partial^a$ , pour lequel tout idéal à gauche admet une base de Gröbner, on s'intéresse plus généralement à un module libre de rang fini sur  $A$ , donné par une base sous la forme  $A^d = Ae_1 + \dots + Ae_d$  et muni d'un ordre sur les  $\partial^a e_i$ , dans lequel on va étendre la notion de base de Gröbner pour des sous-modules à gauche de  $A^d$ . La notion d'ordre monomial conserve formellement la même définition, si ce n'est que les  $e_i$  ne peuvent apparaître que linéairement dans les monômes  $\partial^a e_i$  et qu'ils ne peuvent servir pour des multiplications à gauche. La notion de S-polynôme s'étend aussi mot pour mot, à ceci près que deux polynômes de monômes de tête  $\partial^a e_i$  et  $\partial^b e_j$  ont un S-polynôme nul dès lors que  $i$  et  $j$  sont différents. Les définitions et caractérisations équivalentes des bases de Gröbner d'idéaux restent alors valables pour les sous-modules du module libre  $A^d$ . L'algorithme de Buchberger, modifié pour suivre ces nouvelles définitions, termine sur tout sous-module en fournissant une base de Gröbner. Pour certains ordres, ce calcul correspond à l'algorithme de Gauss.

Un point de vue presque équivalent, mais qui donne une variante des calculs avec un peu plus de réductions, est que le calcul est celui d'une base de Gröbner dans l'anneau  $A[e_1, \dots, e_d]$  des polynômes en les indéterminées commutatives  $e_i$  à coefficients dans l'anneau  $A$  pour l'idéal à gauche engendré par les  $g_i$  initiaux et tous les produits  $e_i e_j = 0$ .

Reprenons l'exemple du découplage des relations entre les coordonnées  $\phi_i$  donnant  $g$  dans la section précédente sur la somme des carrés fonctions de Bessel. Ces relations se recodent par les éléments

$$\begin{aligned} g_1 &:= -e_0 + Se_1 - (2\nu x^{-1} + \eta)e_3, \\ g_2 &:= 4(\nu + 1)x^{-1}Se_1 + (S + 1)e_2 - 2e_3, \\ g_3 &:= Se_0 + (4(\nu + 1)^2x^{-2}S - 1)e_1 + 2(\nu + 1)x^{-1}Se_2, \\ g_4 &:= (S - 1)e_3, \end{aligned}$$

du module libre  $A^4$  pour l'algèbre de Ore  $A = \mathbb{C}(n, k)\langle S_n, S_k; \sigma_n, \sigma_k, 0, 0 \rangle$ . Ici, chaque  $e_i$  représente la fonction rationnelle inconnue  $\phi_i$ , et l'on a astucieusement représenté les second membres de équations inhomogènes d'origine comme multiple d'une nouvelle inconnue représentée par  $e_3$  et contrainte par  $g_4$  à être constante.

Le découplage effectué dans la section précédente revient au calcul d'une base de Gröbner pour l'ordre  $\text{lex}(e_0, e_1, e_2, e_3, S)$ . Les monômes de tête respectifs des  $g_i$  sont  $e_0, Se_1, Se_0$  et  $Se_3$ , si bien que le seul S-polynôme non nul est  $\text{Spoly}(g_1, g_3)$ . Il est donné par

$$\text{Spoly}(g_1, g_3) = Sg_1 + g_3 = (S^2 + 4(\nu + 1)^2x^{-2}S - 1)e_1 + 2(\nu + 1)x^{-1}Se_2 - (2(\nu + 1)x^{-1} + \eta)Se_3.$$

Après réductions par  $g_2$  et  $g_3$ , ce polynôme devient

$$g_5 = -e_1 - \left( \frac{x}{4(\nu + 2)}S^2 + \frac{x^2 - 4\nu^2 - 12\nu - 8}{4x(\nu + 2)}S + \frac{\nu + 1}{x} \right) e_2 + \left( \frac{x}{2(\nu + 2)} - \eta \right) e_3,$$

qui est adjoint à la base de Gröbner en cours de calcul. L'unique nouvel S-polynôme à considérer est celui entre ce  $g_5$  et  $g_2$ , qui est  $\text{Spoly}(g_2, g_4) = g_2 + 4(\nu + 1)x^{-1}Sg_5$  et a pour monôme de tête  $S^3e_2$ . Après réduction par  $e_3$  et renormalisation, le dernier polynôme introduit dans la base de Gröbner est

$$\begin{aligned} ((\nu + 1)x^2S^3 + (\nu + 1)(x^2 - 4\nu^2 - 20\nu - 24)S^2 - (\nu + 3)(x^2 - 4\nu^2 - 12\nu - 8)S - (\nu + 3)x^2)e_2 \\ + 4((\nu^2 + 4\nu + 3)\eta + x)xe_3. \end{aligned}$$

Ce polynôme n'est autre qu'un recodage de l'équation inhomogène du troisième ordre qui a permis de déterminer  $\phi_2$  dans la section précédente.



# Table des matières

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Présentation du cours</b>   | <b>3</b>  |
| 1.1      | Le calcul formel . . . . .   | 3         |
| 1.2      | Contenu du cours . . . . .   | 4         |
| <b>2</b> | <b>Bases de Gröbner et applications</b>  | <b>7</b>  |
| 2.1      | Introduction . . . . .   | 7         |
| 2.2      | Idéaux de polynômes . . . . .  | 8         |
| 2.3      | Quelques problèmes sur les idéaux de polynômes . . . . .                           | 9         |
| 2.3.1    | Finitude de la présentation d'un idéal . . . . .                                   | 9         |
| 2.3.2    | Appartenance à un idéal . . . . .  | 9         |
| 2.3.3    | Résolution de systèmes polynomiaux . . . . .                                       | 10        |
| 2.3.4    | Équations implicites d'un lieu géométrique donné par une paramétrisation . . . . . | 10        |
| 2.4      | Monômes et ordre monomial . . . . .  | 10        |
| 2.4.1    | Terminologie sur les polynômes . . . . .   | 11        |
| 2.4.2    | Monoïde des monômes . . . . .  | 11        |
| 2.4.3    | Ordres monomiaux et exemples principaux . . . . .                                  | 11        |
| 2.4.4    | Coefficients, monômes et termes de tête . . . . .                                  | 12        |
| 2.5      | Réduction et division en plusieurs indéterminées . . . . .                         | 13        |
| 2.5.1    | Réduction . . . . .  | 13        |
| 2.5.2    | Division en plusieurs indéterminées . . . . .                                      | 14        |
| 2.6      | Escaliers, définition et existence des bases de Gröbner . . . . .                  | 15        |
| 2.6.1    | Parties stables du monoïde des monômes . . . . .                                   | 15        |
| 2.6.2    | Définition des bases de Gröbner . . . . .  | 16        |
| 2.6.3    | Lemme de Dickson et existence des bases de Gröbner . . . . .                       | 17        |
| 2.7      | Applications de la théorie des bases de Gröbner . . . . .                          | 18        |
| 2.7.1    | Théorème de Hilbert et noethérianité des anneaux de polynômes . . . . .            | 18        |
| 2.7.2    | Problème d'appartenance à un idéal . . . . .                                       | 19        |
| 2.7.3    | Élimination et résolution de systèmes polynomiaux . . . . .                        | 20        |
| 2.7.4    | Élimination et équations implicites . . . . .                                      | 21        |
| <b>3</b> | <b>Algorithme de Buchberger</b>  | <b>23</b> |
| 3.1      | Saturation des escaliers et algorithme naïf . . . . .                              | 23        |
| 3.1.1    | $S$ -polynômes et relation avec les bases de Gröbner . . . . .                     | 23        |
| 3.1.2    | Version rudimentaire de l'algorithme de Buchberger . . . . .                       | 24        |
| 3.2      | Réductions à zéro et algorithme classique . . . . .                                | 25        |
| 3.2.1    | Paires triviales et paires inutiles . . . . .                                      | 25        |
| 3.2.2    | Forme canonique pour les idéaux de polynômes . . . . .                             | 26        |
| 3.2.3    | Algorithme de Buchberger et ses stratégies classiques . . . . .                    | 26        |
| 3.3      | Cas particulier et extensions de l'algorithme de Buchberger . . . . .              | 28        |
| 3.3.1    | Cas particulier de l'algorithme d'Euclide . . . . .                                | 28        |
| 3.3.2    | Cas particulier de l'algorithme de Gauss . . . . .                                 | 28        |
| 3.3.3    | Bases de Gröbner de modules . . . . .  | 29        |

|          |  |           |
|----------|--|-----------|
| 3.3.4    | Application : base de Gröbner en terme des polynômes initiaux . . . . .                                | 29        |
| 3.4      | Complexité intrinsèque et bases de Gröbner . . . . .   | 30        |
| 3.4.1    | Problèmes complets . . . . .   | 30        |
| 3.4.2    | Taille de la sortie . . . . .  | 30        |
| <b>4</b> | <b>Calculs en Magma</b>  | <b>31</b> |
| <b>5</b> | <b>Intégration symbolique des fractions rationnelles</b>   | <b>35</b> |
| 5.1      | Le problème de l'intégration symbolique et le cas des fractions rationnelles . . . . .                 | 35        |
| 5.2      | Intégration de la partie polynomiale . . . . .   | 36        |
| 5.3      | Partie sans carré et factorisation sans carré . . . . .  | 36        |
| 5.4      | Décomposition en fractions partielles relativement à une factorisation sans carré . . . . .            | 38        |
| 5.5      | Intégration de la partie rationnelle . . . . .   | 39        |
| 5.6      | Algèbre différentielle pour l'intégration rationnelle . . . . .  | 41        |
| 5.7      | Intégration de la partie logarithmique . . . . .   | 42        |
| 5.8      | Complexité globale de l'intégration rationnelle . . . . .  | 44        |
|          | Bibliographie . . . . .  | 45        |
| <b>6</b> | <b>Sommation et intégration symboliques des fonctions spéciales</b>                                    | <b>47</b> |
| 6.1      | Expression de la création télescopique en termes d'algèbres de Ore rationnelles . . . . .              | 47        |
| 6.2      | L'algorithme sur l'exemple $\frac{1}{2}J_0(x)^2 + J_1(x)^2 + J_2(x)^2 + \dots = \frac{1}{2}$ . . . . . | 48        |
| 6.3      | Bases de Gröbner de modules et découplage de systèmes . . . . .  | 50        |