UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LES ALGORITHMES F4 ET F5 POUR LE CALCUL DES BASES DE GRÖBNER.

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES

PAR
WAHIB LASSOUANI

FÉVRIER 2023

REMERCIEMENTS

Toute ma gratitude à Dieu le tout puissant qui m'a permis de réaliser mon rêve de faire des études de cycle supérieur en mathématiques, surtout avec l'équipe pédagogique exceptionnelle que j'ai eu le privilège de croiser le long de mon cheminement à l'UQÁM.

Mes remerciements particuliers à mon directeur, Franco Valentino Saliola, pour sa disponibilité, sa patience, ses encouragements, sa façon passionnante d'expliquer les choses et sa bonne humeur motivante.

Mes remerciements aux organisateurs et intervenants de la petite école du LACIM de l'été 2021, merci à Hugh Thomas, François Bergeron, Christophe Reutenauer et encore une fois à Franco Valentino Saliola qui m'a séduit par son exposé sur les bases de Gröbner.

Merci à toute ma famille et mon entourage qui m'ont soutenu surtout dans le contexte particulier de la pandémie.

TABLE DES MATIÈRES

RÉSUMÉ

Dans ce mémoire, nous allons explorer les versions originales des deux algorithmes de Faugère F4 et F5, décrits respectivement dans les articles (Faugére, 1999) et (Faugère, 2002) pour le calcul d'une base de Gröbner d'un idéal généré par une liste finie de polynômes à plusieurs variables.

Pour cela, nous allons commencer par introduire dans le chapitre I quelques définitions et notions de base liées aux calculs dans un anneau de polynômes. Ensuite on enchaine dans le chapitre II par la présentation de l'algorithme de base de Buchberger pour le calcul d'une base de Gröbner. Les algorithmes F4 et F5 font respectivement l'objet des chapitres III et IV avec un exemple traité pas à pas pour chacun des deux algorithmes. Enfin pour terminer, le chapitre V met en œuvre quelques applications célèbres des bases de Gröbner pour la résolution de problèmes dans différents domaines.

Mots-clés : Base de Gröbner, idéal polynomial, algorithme de Buchberger, algorithme F4, algorithme F5.

INTRODUCTION

En 1965 Bruno Buchberger (mathématicien autrichien né en 1942) fonda la théorie des bases de Gröbner qui doit son nom à Wolfgang Gröbner (1899-1980), son directeur de thèse. Cette découverte devient aujourd'hui un outil à la fois puissant et indispensable en théorie et applications de l'algèbre computationnelle.

L'algorithme de base décrit par Buchberger dans sa thèse de doctorat, intitulée "*Un algorithme pour trouver une base vectorielle de l'anneau quotient par un idéal polynomial de dimension zéro*", permet de calculer une base de Gröbner $G \subset K[x_1, \cdots, x_n]$ pour un idéal I engendré par un ensemble de polynômes $F \subset K[x_1, \cdots, x_n]$. Ce type de base particulière pour l'idéal I se distingue parmi d'autres bases pour le même idéal par des propriétés fortes qui permettent de résoudre de nombreux problèmes difficiles liés à l'idéal polynomial I et qui deviennent aussitôt faciles en choisissant certains générateurs de I comme les éléments de la base de Gröbner G.

Le premier problème, qualifié de fondamental, résolu par simple calcul d'une base de Gröbner, est celui connu sous le nom de "*Ideal Membership Problem" (IMP)* qui consiste à répondre à la question d'appartenance d'un polynôme arbitraire $f \in K[x_1, \cdots, x_n]$ à un idéal polynomial I engendré par un ensemble de polynômes. Un autre problème aussi résoluble par le calcul des bases de Gröbner est la résolution des systèmes d'équations polynomiales qui joue un rôle crucial dans le domaine de la cryptographie. La programmation entière, la robotique, la théorie des graphes et les démonstrateurs automatiques des théorèmes de la géométrie sont aussi des domaines pour lesquels les bases de Gröbner apportent des solutions efficaces

en terme du degré de complexité pour certaines classes de problèmes grâce aux différentes implémentations des algorithmes de recherche des bases de Gröbner sur les systèmes de calcul formel tels que *SageMath* et *Magma*.

Dans ce mémoire, nous allons explorer les versions des deux algorithmes de Faugère F4 et F5, décrits respectivement dans les articles (Faugére, 1999) et (Faugère, 2002). Ces nouveaux algorithmes pour le calcul d'une base de Gröbner d'un idéal polynomial sont les résultats des améliorations apportées à l'algorithme de base de Buchberger en faisant appel aux concepts de l'algèbre linéaire pour ajouter de nouveaux critères qui permettent d'optimiser les calculs dans certains contextes particuliers des systèmes de polynômes donnés en entrée de l'algorithme.

CHAPITRE I

DÉFINITIONS ET CONCEPTS DE BASE

1.1 Généralités sur les polynômes

Dans cette section du mémoire, nous allons faire un petit rappel des éléments de base sur les polynômes et fixer les notations utilisées pour les différentes notions. Parmi toutes celles utilisées dans la littérature, nous avons opté pour la notation qui apparait dans le livre (Cox *et al.*, 1997).

Définition 1.1.1. Un *monôme* en $x_1, x_2, ..., x_n$ est un produit fini de la forme ${x_1}^{\alpha_1} {x_2}^{\alpha_2} \cdots {x_n}^{\alpha_n}$ où tous les exposants α_i sont des entiers positifs ou nuls.

(i) Le degré de ce *monôme* est l'entier $d = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

(ii) Pour $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ on pose $x^\alpha = {x_1}^{\alpha_1} {x_2}^{\alpha_2} \cdots {x_n}^{\alpha_n}$ et son *degré* $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

Définition 1.1.2. Un *polynôme* f en $x_1, x_2, ..., x_n$, à coefficients dans un *corps* K, est une combinaison linéaire finie à coefficients dans K de monômes en $x_1, x_2, \cdots, x_n$:

$$f = \sum_{\alpha} a_\alpha x^\alpha \quad , \quad a_\alpha \in K$$

où $a_\alpha \neq 0$ pour un nombre fini de *n-uplets* α.

L'ensemble de tous les *polynômes* en $x_1, x_2, \cdots, x_n$ à coefficients dans le corps K est noté $K[x_1, \cdots, x_n]$.

Définition 1.1.3. Soit $f = \sum_\alpha a_\alpha x^\alpha$ un polynôme dans $K[x_1, \cdots, x_n]$.

(i) On dit de a_α que c'est le *coefficient* du monôme x^α.

(ii) Si $a_\alpha \neq 0$, on dit que $a_\alpha x^\alpha$ est un *terme* de f.

(iii) Si $f \neq 0$, on note $\deg(f)$ le *degré* du polynôme f qui correspond au maximum des degrés de tous les monômes de f dont le coefficient est non nul.

(iv) Le *polynôme nul* est le polynôme dont tous les coefficients sont nuls.

(v) Si tous les monômes, à coefficients non nuls, qui apparaissent dans un polynôme f sont du même degré d, on dit que f est un polynôme *homogène* de degré d.

L'ensemble des polynômes $K[x_1, \cdots, x_n]$ muni des opérations d'addition et de multiplication, possède la structure d'un *anneau commutatif*. On parle alors de *l'anneau des polynômes* $K[x_1, \cdots, x_n]$.

Définition 1.1.4. On dit qu'un polynôme non nul $g \in K[x_1, \cdots, x_n]$ *divise* le polynôme $f \in K[x_1, \cdots, x_n]$ et on note $g|f$, s'il existe un polynôme $h \in K[x_1, \cdots, x_n]$ tel que $f = gh$.

1.2 Les idéaux

Dans toute la suite du document, on note par $K[x_1, \cdots, x_n]$ l'anneau des polynômes en $x_1, \cdots, x_n$ à coefficients dans le corps K.

Définition 1.2.1. Un sous ensemble $I \subseteq K[x_1, \cdots, x_n]$ est un *idéal* de $K[x_1, \cdots, x_n]$ s'il satisfait aux conditions suivantes :

(i) $0 \in I$ (le polynôme nul).

(ii) Si $f, g \in I$ alors $f + g \in I$ (fermeture pour l'addition).

(iii) Si $f \in I$ et $h \in K[x_1, \cdots, x_n]$, alors $hf \in I$ (fermeture pour la multiplication par un polynômes dans $K[x_1, \cdots, x_n]$).

Définition 1.2.2. Soient $f_1, \cdots, f_s \in K[x_1, \cdots, x_n]$. On note

$$\langle f_1, \cdots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \quad | \quad h_1, \cdots, h_s \in K[x_1, \cdots, x_n] \right\}$$

Lemme 1.2.3. Si $f_1, \cdots, f_s \in K[x_1, \cdots, x_n]$, alors $\langle f_1, \cdots, f_s \rangle$ est un *idéal* de $K[x_1, \cdots, x_n]$.

Démonstration. (i) $0 \in \langle f_1, \cdots, f_s \rangle$ car $0 = \sum_{i=1}^{s} 0.f_i$.

Soit $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} q_i f_i$ et $h \in K[x_1, \cdots, x_n]$. On a alors :

(ii) $f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i + q_i) f_i \in I$.

(iii) $fh = h \sum_{i=1}^{s} p_i f_i = \sum_{i=1}^{s} (hp_i) f_i \in I$ □

On dit que $\langle f_1, \cdots, f_s \rangle$ est l'idéal *engendré* par $f_1, \cdots, f_s$ et que $f_1, \cdots, f_s$ forment une *base* pour l'idéal I.

Remarque 1.2.4. Un idéal peut avoir plusieurs bases différentes, ce qui peut rendre le choix d'une base particulière plus intéressant qu'une autre pour effectuer certains calculs. Nous allons voir justement, qu'une base dite de *Gröbner* permet de résoudre un grand nombre de problèmes et d'apporter des réponses directes à des questions liées aux idéaux.

Définition 1.2.5. (*Séquence régulière de polynômes*) Une séquence (suite) de polynômes homogènes $f_1, \cdots, f_m \in K[x_1, \cdots, x_n]$ est dite *régulière* si :

(i) $\langle f_1, \cdots, f_m \rangle \neq K[x_1, \cdots, x_n]$.

(ii) $\forall\, 1 < i \leq m$, $\forall g \in K[x_1, \cdots, x_n]$, $gf_i \in \langle f_1, \cdots, f_{i-1} \rangle \implies g \in \langle f_1, \cdots, f_{i-1} \rangle$.

Autrement dit, il n'existe aucune relation de la forme $\sum_{i=1}^{m} g_i f_i = 0$ hormis les relations induites par les relations triviales $f_i f_j - f_j f_i = 0$. Cette définition sera utilisée dans le chapitre IV comme condition sur le système d'entrée de l'algorithme F5.

1.3 L'ordre monomial

Le principe de l'algorithme de division dans l'anneau des polynômes à une seule variable et celui de l'élimination de Gauss dans les systèmes d'équations linéaires à plusieurs variables, sont basés sur le choix d'*ordre* défini sur les monômes, qui possède certaines propriétés, comme :

$$x^n > x^{n-1} > \cdots > x > 1$$

Notons qu'il existe une bijection entre l'ensemble des *n-uplets* $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ et l'ensemble des monômes dans $K[x_1, \cdots, x_n]$. En outre, tout ordre $>$ défini sur l'espace $\mathbb{N}^n$ induit un ordre sur les monômes dans $K[x_1, \cdots, x_n]$ en posant :

$$\alpha > \beta \Rightarrow x^\alpha > x^\beta$$

Rappelons la définition d'une *relation d'ordre* sur un ensemble :

Définition 1.3.1. Une relation binaire notée $\leq$ sur un ensemble E est un *ordre total* si et seulement si $\forall x, y, z \in E$ on a :

(i) $x \geq x$ (*réflexivité*).

(ii) $x \leq y$ et $y \leq z \Rightarrow x \leq z$ (*transitivité*).

(iii) $x \leq y$ ou $y \leq x$ (*totalité*).

Exemple 1. L'ensemble des lettres de l'alphabet est totalement ordonné (*ordre alphabétique*).

Définition 1.3.2. Un *ordre* sur les monômes de $K[x_1, \cdots, x_n]$ est dit *monomial* s'il est induit par une relation binaire $>$ dans $\mathbb{N}^n$ qui satisfait les conditions suivantes :

(i) $>$ est un ordre total sur $\mathbb{N}^n$.

(ii) $\forall \alpha, \beta, \gamma \in \mathbb{N}^n : \alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$.

(iii) $>$ est un *bon ordre* sur $\mathbb{N}^n$ (tout sous ensemble non vide de $\mathbb{N}^n$ admet un *plus petit* élément sous $>$). Autrement dit, si $\emptyset \neq A \subseteq \mathbb{N}^n$ alors, il existe $\alpha \in A$ tel que $\beta > \alpha$ pour tout $\beta \neq \alpha$ dans A.

Lemme 1.3.3. Une relation d'ordre $>$ sur $\mathbb{N}^n$ est un bon ordre si et seulement si toute chaine strictement décroissante $\alpha_1 > \alpha_2 > \alpha_3 > \cdots$ se termine.

Démonstration. Si $>$ n'est pas un bon ordre, alors il existe un sous ensemble non vide $S \subseteq \mathbb{N}^n$ qui n'admet pas de plus petit élément. Soit $\alpha_1 \in S$. Comme α_1 n'est pas le plus petit élément de S alors on peut trouver $\alpha_2 \in S$ tel que $\alpha_1 > \alpha_2 \neq \alpha_1$. Comme α_2 n'est pas le plus petit élément de S alors on peut trouver $\alpha_3 \in S$ tel que $\alpha_2 > \alpha_3 \neq \alpha_2$. En continuant de cette façon, on obtient une chaine infinie décroissante $\alpha_1 > \alpha_2 > \alpha_3 > \cdots$. Inversement, étant donnée une chaine décroissante infinie $\alpha_1 > \alpha_2 > \alpha_3 > \cdots$ dans $\mathbb{N}^n$, alors $\{\alpha_1, \alpha_2, \alpha_3, \cdots\}$ est un sous ensemble non vide de $\mathbb{N}^n$ qui n'admet pas de plus petit élément. D'où, $>$ n'est pas un bon ordre. □

Ce lemme sera utilisé pour montrer qu'un algorithme se termine parce que certains termes évoluent en décroissant (selon un ordre monomial fixé) au cours de l'exécution de l'algorithme.

Parmi les ordres monômiaux usuels, on peut citer les trois suivants :

Définition 1.3.4. (L'ordre *lexicographique*) Soit $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ et $\beta =$

$(\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$. On dit que $\alpha >_{\text{lex}} \beta$, si la composante non nulle la plus à gauche du vecteur $\alpha - \beta \in \mathbb{Z}^n$ est positive. On écrit alors $x^\alpha >_{lex} x^\beta$ si $\alpha >_{lex} \beta$.

Exemple 2. (i) $(2,3,0) >_{lex} (1,4,5)$ car dans le vecteur $(2,3,0) - (1,4,5) = (1,-1,-4)$, la composante non nulle la plus à gauche est positive. D'où

$$x_1^2 x_2^3 >_{lex} x_1 x_2^4 x_3^5$$

(ii) $(2,1,3) >_{lex} (2,1,0)$ car dans le vecteur $(2,1,3) - (2,1,0) = (0,0,3)$, la composante non nulle la plus à gauche est positive. D'où

$$x_1^2 x_2 x_3^3 >_{lex} x_1^2 x_2$$

Remarque 1.3.5. Dans $\mathbb{N}^n$ on a : $(1,\ldots,0) >_{lex} (0,1,\cdots) >_{lex} \cdots >_{lex} (0,\ldots,1)$ d'où :

$$x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$$

Définition 1.3.6. (L'ordre *lexicographique gradué*) Soit $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ et $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$. On dit que $\alpha >_{grlex} \beta$, si l'une des conditions suivantes est satisfaite :

(i) $|\alpha| > |\beta|$

(ii) $|\alpha| = |\beta|$ et $\alpha >_{lex} \beta$ avec $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$

Exemple 3. (i) $(2,2,2) >_{grlex} (3,1,0)$ car la première condition de la définition est satisfaite. En effet, $2+2+2 > 3+1+0$. D'où

$$x_1^2 x_2^2 x_3^2 >_{grlex} x_1^3 x_2$$

(ii) $(1,2,4) >_{grlex} (1,1,5)$ car la deuxième condition de la définition est satis-

faite. En effet, $1+2+4 = 1+1+5$ et $(1,2,4) >_{lex} (1,1,5)$. D'où :

$$x_1x_2^2x_3^4 >_{grlex} x_1x_2x_3^5$$

(iii) $x_1 >_{grlex} x_2 >_{grlex} \cdots >_{grlex} x_n$

Définition 1.3.7. (L'ordre *lexicographique gradué inverse*) Soit $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$ et $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$. On dit que $\alpha >_{grevlex} \beta$, si l'une des conditions suivantes est satisfaite :

(i) $|\alpha| > |\beta|$

(ii) $|\alpha| = |\beta|$ et la composante non nulle la plus à droite du vecteur $\alpha - \beta$ est négative.

Exemple 4. $(3,6,0) >_{grevlex} (3,4,2)$ car la deuxième condition de la définition est satisfaite. En effet, on a : $3+6+0 = 3+4+2$ et la composante non nulle la plus à droite du vecteur $(3,6,0) - (3,4,2) = (0,2,-2)$ est négative. D'où :

$$x_1^3x_2^6 >_{grevlex} x_1^3x_2^4x_3^2$$

1.4 Terme, monôme et coefficient dominant

Pour un ordre monomial fixé, tout polynôme dans $K[x_1, \cdots, x_n]$ s'écrit de façon unique en ordonnant ses termes en ordre monomial décroissant.

Exemple 5. Considérons le polynôme $f = 2xy^2z - 7z^2 + x^3 - 9x^2z^2$ dans $\mathbb{Q}[x,y,z]$.

Ordre monomial	Écriture de f suivant l'ordre monomial
lexicographique	$f = x^3 - 9x^2z^2 + 2xy^2z - 7z^2$
lexicographique gradué	$f = -9x^2z^2 + 2xy^2z + x^3 - 7z^2$
lexicographique gradué inverse	$f = 2xy^2z - 9x^2z^2 + x^3 - 7z^2$

Pour faciliter la manipulation des polynômes, on définit certaines notions associées à un polynôme écrit selon l'ordre monomial fixé comme suit :

Définition 1.4.1. Soit $f = \sum_\alpha a_\alpha x^\alpha$ un polynôme non nul dans $K[x_1, \cdots, x_n]$ muni d'un ordre monomial $>$.

(i) Le *multidegré* de f est défini comme

$$\text{multideg}(f) = \max_> \{\alpha \in \mathbb{N}^n \quad | \quad a_\alpha \neq 0\}$$

(ii) Le *coefficient dominant* de f est défini comme

$$\text{LC}(f) = a_\beta \in K \quad o\grave{u} \quad \beta = \text{multideg}(f)$$

(iii) Le *monôme dominant* de f est défini comme

$$\text{LM}(f) = x^\beta \quad o\grave{u} \quad \beta = \text{multideg}(f)$$

(iv) Le *terme dominant* de f est défini comme

$$\text{LT}(f) = \text{LC}(f)\text{LM}(f)$$

Le lemme suivant nous donne deux propriétés importantes sur le degré d'un polynôme.

Lemme 1.4.2. Soient $f, g \in K[x_1, \cdots, x_n]$ deux polynômes non nuls. Alors :

(i) $multideg(fg) = multideg(f) + multideg(g)$

(ii) Si $f + g \neq 0$ alors $multideg(f + g) \leq max(multideg(f), multideg(g))$

Remarque 1.4.3. La terminologie liée aux polynômes, diffère dans la littérature. Dans (Faugére, 1999), par exemple, on trouve $HT(f)$ au lieu de $LM(f)$, $HM(f)$ au lieu de $LT(f)$ et $HC(f)$ au lieu de $LC(f)$.

1.5 L'algorithme de division dans $K[x_1, \cdots, x_n]$

L'algorithme de division des polynômes dans $K[x]$ peut être généralisé aux cas des polynômes à plusieurs variables en fixant un ordre monomial. En effet, diviser un polynôme $f \in K[x_1, \cdots, x_n]$ par une liste de polynômes $f_1, \cdots, f_s \in K[x_1, \cdots, x_n]$ revient à écrire f sous une forme

$$f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r$$

pour un choix adéquat des quotients $q_1, q_2, \cdots q_s$ et du reste r, des polynômes dans $K[x_1, \cdots, x_n]$.

L'idée de base de l'algorithme de division dans $K[x_1, \cdots, x_n]$, est d'éliminer le terme dominant de f (suivant un ordre monomial fixé) en multipliant un certain f_i par le terme qui convient, puis faire la soustraction. Les quotients et le reste de cette division dépendent de l'ordre dans lequel les f_i sont choisis à chaque étape de la division pour éliminer le terme dominant comme le montre l'exemple suivant :

Exemple 6. Considérons dans $\mathbb{Q}[x, y]$ le polynôme $f = xy^2 + 1$ et l'idéal engendré par

$$f_1 = xy + 1 \quad , \quad f_2 = y + 1.$$

Choisissons l'ordre *lexicographique* avec $x > y$. Pour éliminer $LT(f) = xy^2$, on a le choix entre soustraire yf_1 (réduire par f_1) ou xyf_2 (réduire par f_2) de f.

(i) Dans le premier cas, $f - yf_1 = xy^2 + 1 - xy^2 - y = -y + 1$. Comme $LT(f_1) = xy$ ne divise pas $LT(-y + 1) = -y$ alors la division sur f_1 est terminée pour cette étape (il se peut qu'il faudra l'appliquer de nouveau). On a alors $q_1 = y$. Comme $LT(f_2) = y$ divise $LT(-y + 1) = -y$ alors

$$(-y + 1) + 1f_2 = -y + 1 + y + 1 = 2.$$

La division par f_2 est terminée avec $q_2 = -1$, d'où

$$f = yf_1 + (-1)f_2 + 2$$

(ii) Dans le second cas, $f - xyf_2 = xy^2 + 1 - xy^2 - xy = -xy + 1$. Comme $LT(f_2) = y$ divise $LT(-xy + 1) = -xy$ alors la division sur f_2 continue :

$$(-xy + 1) - (-x)f_2 = -xy + 1 + xy + x = x + 1$$

Comme $LT(f_2) = y$ ne divise pas $LT(x + 1) = x$ alors la division sur f_2 est terminée avec $q_2 = xy - x$. Comme $LT(f_1) = xy$ ne divise pas $LT(x+1) = x$, alors pas de division par f_1, ce qui signifie que $q_1 = 0$ d'où

$$f = 0f_1 + (xy - x)f_2 + x + 1$$

En observant l'exemple ci-dessus, on remarque que le résultat de la division dépend du choix du polynôme réducteur.

Théorème 1.5.1. (Algorithme de division dans $K[x_1, \cdots, x_n]$) Soit $F = (f_1, \cdots, f_s)$ un vecteur de s polynômes non nuls dans $K[x_1, \cdots, x_n]$ muni d'un ordre monomial $>$. Alors, tout polynôme $f \in K[x_1, \cdots, x_n]$ peut s'écrire sous la forme

$$f = q_1f_1 + q_2f_2 + \cdots + q_sf_s + r$$

avec $q_i, r \in K[x_1, \cdots, x_n,]$ où on a soit $r = 0$ ou r est tel qu'aucun des monômes qui apparaissent dans r n'est divisible par un des termes dominants des f_i.

On dit que r est le *reste de la division* de f par F. De plus, si $q_if_i \neq 0$ alors, multideg$(f) \geq$ multideg(q_if_i) pour tout $1 \leq i \leq s$.

Démonstration. La démonstration de ce théorème est basée sur l'existence de

l'algorithme 1, qui permet de trouver les quotients et le reste de la division après un nombre fini d'itérations de la boucle principale (voir la preuve de l'exactitude et de la terminaison de l'algorithme en détails dans (Cox *et al.*, 1997) (page 62)).

Algorithm 1 Algorithme de division dans $K[x_1, \cdots, x_n]$.

Entrée : $f_1, \cdots, f_s, f$: liste finie de polynômes dans $K[x_1, \cdots, x_n]$.
Sortie : $q_1, \cdots, q_s, r$: liste finie de polynômes dans $K[x_1, \cdots, x_n]$.
$r = 0$
$p = f$
$q_i = 0$ pour tout $i = 1 \cdots s$
tant que $p \neq 0$ **faire**
  $i = 1$
  divisionoccured=faux
  tant que *divisionoccured* = faux *et* $i \leq s$ **faire**
    si $LT(f_i)$ *divise* $LT(p)$ **alors**
      $q_i = q_i + \frac{LT(p)}{LT(f_i)}$
      $p = p - \frac{LT(p)}{LT(f_i)} f_i$
      divisionoccured = vrai
    sinon
      $i = i + 1$
    fin si
  fin tant que
  si *divisionoccured* = faux **alors**
    $r = r + LT(p)$
    $p = p - LT(p)$
  fin si
fin tant que
  retourner $q_1, \cdots, q_s, r$

□

L'inconvénient de cet algorithme est que les quotients q_i et le reste r dépendent du choix de l'ordre des f_i dans le vecteur d'entrée F. Autrement dit, en changeant cet ordre, le reste et les quotients peuvent aussi changer, contrairement à l'algorithme de division dans le cas des polynômes à une seule variable où le quotient et le reste sont uniques. Par conséquent, cet algorithme ne permet pas de résoudre le

problème d'appartenance à un idéal. À savoir, si le reste de la division est $r = 0$ alors $f \in \langle f_1, \cdots, f_s \rangle$ mais si $r \neq 0$ alors, on ne peut pas conclure puisque en changeant l'ordre des f_i on peut trouver un reste nul. D'où la condition $r = 0$ est suffisante mais pas nécessaire pour résoudre le problème d'appartenance à un idéal.

Pour remédier à ce problème, on doit choisir un bon ensemble de générateurs de l'idéal $\langle f_1, \cdots, f_s \rangle$, qui puisse garantir l'unicité du reste de la division quelque soit l'ordre des f_i dans le vecteur d'entrée F. Cela fera l'objet du chapitre II.

CHAPITRE II

LES BASES DE GRÖBNER

2.1 Définitions et notations

Dans cette section, nous allons définir quelques notions préliminaires pour introduire les bases de Gröbner.

Définition 2.1.1. Soit $I \subseteq K[x_1, \cdots, x_n]$ un idéal différent de $\{0\}$ et soit $>$ un ordre monomial dans $K[x_1, \cdots, x_n]$.

(i) On note $LT(I)$ l'ensemble des termes dominants des éléments non nuls de I autrement dit,

$$LT(I) = \left\{ cx^{\alpha} \quad | \quad \exists f \in I : LT(f) = cx^{\alpha} \right\}$$

(ii) On note par $\langle LT(I) \rangle$ l'idéal engendré par les éléments de $LT(I)$.

Remarque 2.1.2. Si $I = \langle f_1, \cdots, f_s \rangle$ alors,

$$\langle LT(f_1), \cdots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle$$

Cette inclusion peut être stricte comme le montre l'exemple suivant :

Exemple 7. Considérons dans $\mathbb{Q}[x, y]$ muni de l'ordre lexicographique gradué

avec $(x > y)$, l'idéal

$$I = \langle x^3, x^2y + x \rangle$$

Posons $f_1 = x^3$ et $f_2 = x^2y + x$. On a alors, $x^2 \in I$ car $x^2 = xf_2 - yf_1$ d'où $x^2 = LT(x^2) \in \langle LT(I) \rangle$. Mais, x^2 n'est divisible ni par $x^3 = LT(f_1)$ ni par $x^2y = LT(f_2)$ donc

$$x^2 \notin \langle LT(f_1), LT(f_2) \rangle$$

Proposition 2.1.3. Soit $0 \neq I \subseteq K[x_1, \cdots, x_n]$ un idéal.

(i) $\langle LT(I) \rangle$ est un *idéal*, et

(ii) Il existe $g_1, \cdots, g_t \in I$ tels que $\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle$.

Esquisse de la preuve. (i) L'ensemble des monômes dominants des éléments non nuls de I engendre *l'idéal monomial* $\langle LM(f) \quad | \quad f \in I \setminus \{0\} \rangle$. Comme $LM(f)$ et $LT(f)$ diffèrent par une constante non nulle dans K, alors,

$$\langle LM(f) \quad | \quad f \in I \setminus \{0\} \rangle = \langle LT(f) \quad | \quad f \in I \setminus \{0\} \rangle = \langle LT(I) \rangle.$$

(ii) Par le lemme de Dickson qui stipule que tout idéal monomial admet un ensemble fini de monômes comme base (Théoème 5, page 69 dans (Cox *et al.*, 1997)), $LT(I) = \langle LM(g_1), \cdots, LM(g_t) \rangle$ pour un ensemble fini de polynômes $g_1, \cdots, g_t \in I$. Comme $LM(g_i)$ et $LT(g_i)$ diffèrent par une constante non nulle dans K, alors $\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle$. □

2.2 Théorème de la base de Hilbert

Théorème 2.2.1. Tout idéal $I \subseteq K[x_1, \cdots, x_n]$ admet un ensemble fini de *générateurs*. Autrement dit, il existe $g_1, \cdots, g_t \in I$ tels que

$$I = \langle g_1, \cdots, g_t \rangle.$$

Démonstration. (i) Si $I = \{0\}$, alors $I = \langle 0 \rangle$.

(ii) Si $I \neq \{0\}$ construisons un ensemble de générateurs pour I. Fixons un ordre monomial dans $K[x_1, \cdots, x_n]$. Alors par la proposition 2.1.3 :

$$\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle.$$

Montrons que $I = \langle g_1, \cdots, g_t \rangle$. On a $\langle g_1, \cdots, g_t \rangle \subseteq I$ car $(g_i)_{1 \leq i \leq t} \in I$. Soit $f \in I$. En appliquant l'algorithme de division de f par $g_1, \cdots, g_t$ on obtient une expression de la forme $f = q_1 g_1 + \cdots + q_t g_t + r$ telle qu'aucun terme de r n'est divisible par $LT(g_i)_{1 \leq i \leq t}$. On a alors :

$$r = f - q_1 g_1 - \cdots - q_t g_t = f - \sum_{i=1}^{t} q_i g_i$$

D'où $r \in I$. Si $r \neq 0$ alors $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle$ d'où $LT(r)$ est divisible par un certain $LT(g_i)$ d'où la contradiction. Ce qui conduit à $r = 0$. D'où $f = q_1 g_1 + \cdots + q_t g_t \in \langle g_1, \cdots, g_t \rangle$ ce qui veut dire que $I \subseteq \langle g_1, \cdots, g_t \rangle$. □

2.3 Les bases de Gröbner

Définition 2.3.1. Soit $K[x_1, \cdots, x_n]$ l'anneau des polynômes muni d'un ordre monomial. Un sous ensemble fini $G = \{g_1, \cdots, g_t\}$ d'un idéal non nul I dans $K[x_1, \cdots, x_n]$ est une *base de Gröbner* de l'idéal I si

$$\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle$$

Autrement dit, pour tout $f \in I$, $LT(f)$ est divisible par un certain $LT(g_i)_{1 \leq i \leq t}$.

Corollaire 2.3.2. En fixant un ordre monomial dans l'anneau des polynômes

$K[x_1, \cdots, x_n]$, tout idéal $I \subseteq K[x_1, \cdots, x_n]$ admet une base de Gröbner. De plus, toute base de Gröbner de I est une base pour I.

Démonstration. (i) Soit $\{0\} \neq I \subseteq K[x_1, \cdots, x_n]$. L'ensemble $G = \{g_1, \cdots, g_t\}$ construit dans la démonstration du théorème 2.2.1 est par définition une base de Gröbner pour I.

(ii) Si $\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$ alors, par l'argument donné dans la démonstration du théorème 2.2.1, on a que $I = \langle g_1, \cdots, g_t\rangle$ donc G est une base de I. □

Pour démontrer l'arrêt de certains algorithmes considéré par la suite, nous avons besoin d'introduire la *condition de la chaine ascendante* (due à Emmy Noether) comme l'énonce le théorème suivant :

Théorème 2.3.3. Pour toute chaine ascendante $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ d'idéaux dans $K[x_1, \cdots, x_n]$, il existe un entier $N \geq 1$ tel que

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

Démonstration. Posons $I = \bigcup_{j=1}^{\infty} I_j$. Montrons que I est un idéal dans $K[x_1, \cdots, x_n]$:

(i) $0 \in I$ car $0 \in I_j$ pour tout I_j.

(ii) Soient $f, g \in I$ tels que $f \in I_j$ et $g \in I_k$ pour certains $j \leq k$. Comme $I_j \leq I_k$ alors $f \in I_k$ car $f \in I_j$.

I_k est un idéal, et $f, g \in I_k$ alors $f + g \in I_k$. D'où $f + g \in I$.

(iii) Soit $r \in K[x_1, \cdots, x_n]$ alors $rf \in I_j$ car I_j est un idéal. D'où $rf \in I_j \subseteq I$.

Par le théorème de la base d'Hilbert, l'idéal I admet un ensemble fini de générateurs $I = \langle f_1, \cdots, f_t\rangle$. Chaque générateur f_i est contenu dans un idéal I_j pour un certain j. Soit $f_i \in I_{j_i}$ pour $j_i = 1 \cdots t$. Notons N le *maximum* des j_i alors $\forall i = 1 \cdots t$, $f_i \in I_N$. D'où $I = \langle f_1, \cdots, f_t\rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I$. □

2.4 Propriétés des bases de Gröbner

Pour chaque ordre monomial donné, un idéal polynômial admet une infinité de bases de Gröbner. Chacune d'entre elles vérifie les deux propriétés données par la proposition suivante :

Proposition 2.4.1. Soit $\{0\} \neq I \subseteq K[x_1, \cdots, x_n]$ un idéal et $G = \{g_1, \cdots, g_t\}$ une base de Gröbner pour I. Pour $f \in K[x_1, \cdots, x_n]$, il existe un unique polynôme $r \in K[x_1, \cdots, x_n]$ qui vérifie les deux propriétés suivantes :

(i) Aucun *terme* de r n'est divisible par un des termes $LT(g_i), \cdots, LT(g_t)$.

(ii) Il existe $g \in I$ tel que $f = g + r$.

En particulier, r est le reste de la division de f par G quelque soit l'ordre des g_i dans le vecteur d'entrée de l'algorithme de division. Il est appelé la *forme normale* du polynôme f par la division par G et on écrit $f \underset{G}{\rightarrow} r$.

Démonstration. L'algorithme de division donne une écriture de f sous la forme $f = q_1 g_1 + \cdots + q_t g_t + r$ pour un certain choix d'ordre attribué aux g_i. Donc la propriété (i) est satisfaite. De plus, en posant $g = q_1 g_1 + \cdots + q_t g_t \in I$, la propriété (ii) est aussi satisfaite. Pour montrer l'unicité de r, supposons qu'il existe g', r' qui satisfont les propriétés de la proposition 2.4.1, pour un autre choix de l'ordre des g_i dans l'algorithme de division. On a alors,

$$r - r' = g' - g \in I.$$

Donc, si $r \neq r'$ alors, $LT(r-r') \in \langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle$ d'où $LT(r-r')$ est divisible par $LT(g_i)$ pour un certain $1 \leq i \leq t$. Ce qui est impossible car aucun terme de r ni de r' n'est divisible par un des $LT(g_1), \cdots, LT(g_t)$. D'où $r - r'$ ne peut être non nul. D'où l'unicité de r. □

La proposition 2.4.1 permet de répondre à la question d'appartenance d'un polynôme quelconque à un idéal par le corollaire suivant :

Corollaire 2.4.2. Soit $G = \{g_1, \cdots, g_t\}$ une base de Gröbner pour un idéal $\{0\} \neq I \subseteq K[x_1, \cdots, x_n]$ et soit $f \in K[x_1, \cdots, x_n]$. Alors, $f \in I$ si et seulement si

$$f \underset{G}{\rightarrow} 0$$

Démonstration. Si le reste de la division de f par G est nul, alors $f \in I$. Inversement, si $f \in I$, alors $f = f + 0$ satisfait les conditions de la proposition 2.4.1 alors, $f \underset{G}{\rightarrow} 0$. □

Définition 2.4.3. Soit $F = (f_1, \cdots, f_s) \in K[x_1, \cdots, x_n]^s$ et $f \in K[x_1, \cdots, x_n]$. On note par $\overline{f}^F$ le reste de la division de f par $\{f_1, \cdots, f_s\}$ dans l'ordre d'apparition des f_i dans le vecteur F. Si $\{f_1, \cdots, f_s\}$ est une base de Gröbner pour l'idéal $\langle f_1, \cdots, f_s \rangle$, alors F peut être considéré comme l'ensemble non ordonné $\{f_1, \cdots, f_s\}$.

Autrement dit, la forme normale de f par la division par $\{f_1, \cdots, f_s\}$ est $\overline{f}^F$ indépendamment de l'ordre des f_i dans le vecteur F.

2.5 Les *S-polynômes* et le critère des *S-paires*

Dans cette section, nous allons introduire la notion des *S-polynômes* sur laquelle est basé l'algorithme de Buchberger pour la recherche d'une base de Gröbner pour un idéal polynômial.

Définition 2.5.1. Soient $f, g \in K[x_1, \cdots, x_n]$ deux polynômes non nuls. Posons $multideg(f) = \alpha$, $multideg(g) = \beta$ et $\gamma = (\gamma_1, \cdots, \gamma_n)$ où $\gamma_i = max\,(\alpha_i, \beta_i)_{1 \leq i \leq n}$.

(i) On appelle x^γ le *plus petit multiple commun* de $LM(f)$ et $LM(g)$, noté $ppcm(LM(f), LM(g))$.

(ii) Le *S-polynôme* de f et g est le polynôme $S(f,g)$ défini par

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

Exemple 8. Soient $f = x^3y - 2x^2$ et $g = 2xy^2 + x$ deux polynômes dans $\mathbb{Q}[x,y]$ muni de l'ordre lexicographique gradué avec $x > y$. Alors $multideg(f) = (3,1)$ et $multideg(g) = (1,2)$ d'où $\gamma = (3,2)$. Ce qui donne

$$S(f,g) = \frac{x^3y^2}{x^3y}f - \frac{x^3y^2}{2xy^2}g = -2x^2y - \frac{1}{2}x^3.$$

Remarque 2.5.2. Les S-polynômes seront utilisés par l'algorithme 2 pour le calcul d'une base de Gröbner.

Lemme 2.5.3. Soit $p = \sum_{i=1}^{t} p_i$ où $p_i \in K[x_1, \cdots, x_n]$ tels que $multideg(p_i) = \delta \in \mathbb{N}^n$ pour tout $1 \leq i \leq t$. Si $multideg(p) < \delta$ alors, p est une combinaison linéaire à coefficients dans K des *S-polynômes* $S(p_j, p_k)$ pour $1 \leq j < k \leq t$.

Démonstration. Soit $d_i = LC(p_i)$ alors, $LT(p_i) = d_i x^\gamma$. Comme $multideg(\sum_{i=1}^{t} p_i) < \delta$ alors $\sum_{i=1}^{t} d_i = 0$. Comme $LM(p_i) = LM(p_j) = x^\delta$ alors,

$$S\left(p_i, p_j\right) = \frac{x^\delta}{d_i x^\delta}p_i - \frac{x^\delta}{d_j x^\delta}p_j = \frac{1}{d_i}p_i - \frac{1}{d_j}p_j$$

d'où :

$$\begin{aligned}\sum_{i=1}^{t-1} d_i S(p_i, p_t) &= d_1\left(\frac{1}{d_1}p_1 - \frac{1}{d_t}p_t\right) + \cdots + d_{t-1}\left(\frac{1}{d_{t-1}}p_{t-1} - \frac{1}{d_t}p_t\right)\\ &= p_1 + \cdots + p_{t-1} - \frac{1}{d_t}\left(d_1 + d_2 + \cdots + d_{t-1}\right)p_t\\ &= p_1 + \cdots + p_{t-1} - \frac{1}{d_t}(-d_t)p_t \quad car \sum_{i=1}^{t} d_i = 0\\ &= p_1 + p_2 + \cdots + p_{t-1} + p_t. \end{aligned}$$

□

Théorème 2.5.4. (Théorème de Buchberger ou *critère des S-paires*) Soit I un idéal polynomial. Une base $G = \{g_1, \cdots, g_t\}$ de I est une base de Gröbner pour I si et seulement si pour toute paire $(i,j)_{1\leq i<j\leq t}$, le reste de la division de $S(g_i, g_j)$ par G (dans un ordre quelconque des g_i) est nul.

Démonstration. Voir la démonstration en détails dans (Cox *et al.*, 1997) (page 82). □

Exemple 9. Soit $I = \langle xy - y, x^2 - 1\rangle$ un idéal dans $Q[x,y]$ muni de l'ordre lexicographique $x > y$. On a que

$$S(xy - y, x^2 - 1) = x(xy - y) - y(x^2 - 1) = -xy + y = (-1)(xy - y).$$

Alors, $\overline{S(xy - y, x^2 - 1)}^{F} = 0$ où $F = \{xy - y, x^2 - 1\}$ et donc, par le théorème 2.5.4, $F = \{xy - y, x^2 - 1\}$ est une base de Gröbner pour I.

2.6 L'algorithme de Buchberger

La première version (non optimisée) de l'algorithme de Buchberger permet de calculer une base de Gröbner pour un idéal $I = \langle F\rangle$, où $F = \{f_1, \cdots, f_s\}$, en se

basant uniquement sur le critère des *S-paires* selon le processus suivant :

(i) Pour chaque paire de polynômes distincts $S(f_i, f_j) \in F \times F$, on calcule $S(f_i, f_j)$.

(ii) Si $\overline{S(f_i, f_j)}^F \neq 0$ alors, on ajoute $\overline{S(f_i, f_j)}^F$ à F.

(iii) On répète les étapes précédentes jusqu'à ce qu'on obtienne un ensemble F qui vérifie la condition du théorème 2.5.4.

Théorème 2.6.1. Soit $I = \langle f_1, \cdots, f_s \rangle \neq \{0\}$ un idéal dans $K[x_1, \cdots, x_n]$. Une base de Gröbner pour I peut être construite après un nombre fini d'étapes d'exécution de l'algorithme 2.

Algorithm 2 Algorithme de base de Buchberger.

Entrée : $F = \{f_1, \cdots, f_s\}$ un ensemble fini de polynômes.
Sortie : Une base de Gröbner $G = \{g_1, \cdots, f_t\}$ pour $\langle F \rangle$ avec $F \subseteq G$.
$G = F$
répéter
  $G' = G$
  pour chaque paire $\{p, q\}, p \neq q$ dans G' **faire**
    $r = \overline{S(p, q)}^{G'}$
    si $r \neq 0$ **alors**
      $G = G \cup \{r\}$
    fin si
  fin pour
jusqu'à $G = G'$
retourner G

L'application de l'algorithme 2 génère souvent des calculs inutiles. À savoir, si $\overline{S(p, q)}^{G'} = 0$ alors ce reste demeure invariant tout le temps d'exécution de l'algorithme même si on ajoute des éléments nouveaux au générateurs de la base G'. Une façon donc d'éliminer ces calculs inutiles consiste à ne considérer que les polynômes $S(f_i, f_j)$ pour $i \leq j-1$ à l'ajout d'un nouveau générateur f_j à la base G'. De plus, le lemme 2.6.2 va permettre de réduire encore le nombre de générateurs.

Lemme 2.6.2. Soit G une base de Gröbner d'un idéal $I \subseteq K[x_1, \cdots, x_n]$. Soit $p \in G$ un polynôme tel que $LT(p) \in \langle LT(G - \{p\})\rangle$. Alors, $G - \{p\}$ est aussi une base de Gröbner pour I.

Démonstration. G est une base de Gröbner pour I alors $\langle LT(G)\rangle = \langle LT(I)\rangle$. Si $LT(p) \in \langle LT(G - \{p\}\rangle$ alors $\langle LT(G - \{p\})\rangle = \langle LT(G)\rangle$. D'où par définition, $G - \{p\}$ est une base de Gröbner pour I. □

En ajustant tous les éléments d'une base de Gröbner de façon à avoir tous les coefficients dominants des générateurs égaux à 1 (*polynômes unitaires)* et en supprimant tous les polynômes $p \in G$ tels que $LT(p) \in \langle LT(G - \{p\}\rangle$, on obtient une base de Gröbner dite *minimale*. Cette base n'est pas unique.

Définition 2.6.3. La base de Gröbner *réduite* d'un idéal polynomial I, est une base de Gröbner G pour l'idéal I qui vérifie les deux conditions suivantes :

(i) $LC(p) = 1$ pour tout polynôme $p \in G$.

(ii) Pour tout $p \in G$ aucun monôme de p n'appartient à $\langle LT(G - \{p\})\rangle$.

Théorème 2.6.4. Soit $I \neq \{0\}$ un idéal polynomial. Alors, pour un ordre monomial fixé, I admet une base de Gröbner réduite qui est unique.

Démonstration. Les bases de Gröbner minimales de I ont toutes les mêmes termes dominants. Soit G une de ces bases minimales. On dit qu'un polynôme $g \in G$ est complètement réduit pour G , si aucun monôme dans g n'appartient à l'idéal $\langle LT(G - \{g\})\rangle$. Alors g est aussi complètement réduit pour toute autre base de Gröbner minimale $G^{'}$ pour I qui contient g car $LT(G) = LT(G^{'})$. Posons $g^{'} = \overline{g}^{G-\{g\}}$ et montrons que $G^{'} = (G - \{g\}) \cup \{g^{'}\}$ est une base de Gröbner minimale pour I. Comme $LT(g)$ n'est divisible par aucun élément de $LT(G-\{g\})$ alors $LT(g^{'}) = LT(g)$ d'où $LT(G^{'}) = LT(G)$ et par conséquent $\langle LT(G^{'})\rangle =$

$\langle LT(G)\rangle$. De plus $G^{'} \subseteq I$ alors $G^{'}$ est une base de Gröbner minimale pour I et par construction, $g^{'}$ est complètement réduit pour $G^{'}$. En répétant le processus pour tous les éléments de G, on obtient la base de Gröbner réduite pour I. Pour l'unicité, supposons que G et $\tilde{G}$ sont deux bases de Gröbner réduites pour l'idéal I et soit $g \in G$. Alors, il existe un polynôme $g^{'} \in \tilde{G}$ tel que $LT(g) = LT(g^{'})$. De plus $g \in I$ et $g^{'} \in I$ alors $g - g^{'} \in I$ d'où $\overline{g - g^{'}}^{G} = 0$. Comme $LT(g) = LT(g^{'})$ alors ces termes s'annulent dans $g - g^{'}$ et les termes restants ne sont divisibles par aucun des $LT(G)$ car g est réduit pour G et $g^{'}$ est réduit pour $\tilde{G}$ et $LT(G) = LT(\tilde{G})$. D'où : $\overline{g - g^{'}}^{G} = g - g^{'} = 0$ d'où $g = g^{'}$ ce qui conduit à $G = \tilde{G}$. □

Remarque 2.6.5. Une des applications du théorème 2.6.4 est de permettre de montrer que deux ensembles finis de polynômes $\{f_1, \cdots, f_s\}$ et $\{g_1, \cdots, g_t\}$ engendrent le même idéal polynomial. En effet, il suffit de fixer un ordre monomial et de calculer les bases de Gröbner réduites pour les deux idéaux $\langle f_1, \cdots, f_s\rangle$ et $\langle g_1, \cdots, g_t\rangle$. On a alors, $\langle f_1, \cdots, f_s\rangle = \langle g_1, \cdots, g_t\rangle$ si et seulement si les deux bases de Gröbner réduites coïncident.

CHAPITRE III

L'ALGORITHME F4

Dans l'algorithme de base de Buchberger, pour le calcul d'une base de Gröbner pour un idéal polynomial, le choix des paires de *S-polynômes* est arbitraire. Il en est de même pour le choix du polynôme réducteur parmi une liste de polynômes.

Buchberger a montré que ces deux choix n'affectent en aucun cas les résultats de l'algorithme si ce n'est qu'ils jouent un rôle crucial dans le temps de calcul. De plus, les meilleurs stratégies appliquées dans l'algorithme se basent uniquement sur les termes dominants (paire critique de plus petit degré). Cependant, dans le cas de l'existence de plusieurs paires critiques de meme degré, le choix arbitraire d'une telle paire peut affecter le temps de calcul. Face à une telle situation, l'une des solutions consiste à traiter un sous ensemble de paires simultanément. À partir de ce choix, on construit une matrice à laquelle on applique l'algorithme d'élimination de Gauss-Jordan. Cette technique basée sur des notions de l'algèbre linéaire a été introduite par Jean-Charles Faugère dans son algorithme appelé F4 (Faugére, 1999), pour le calcul de la base de Gröbner d'un idéal polynomial, ce qui est l'objet de ce chapitre.

3.1 Représentation matricielle des polynômes

L'objectif de ce chapitre étant de présenter l'algorithme F4, nous allons commencer par introduire les notions auxquelles il fait appel.

Définition 3.1.1. Si $F = (f_1, \cdots, f_s)$ est un *vecteur de S-polynômes* et $\mathcal{M}on_>(F) = (m_1, \cdots, m_k)$ le vecteur des monômes du support F triés par ordre décroissant suivant un ordre monomial $>$ alors, la représentation matricielle de F est la matrice notée $M(F)$ de taille $s \times k$ dont les éléments $M_{i,j}(F)$ correspondent chacun au coefficient du monôme m_j dans le polynôme f_i. Cette matrice vérifie l'équation

$$F^t = M(F) \times \mathcal{M}on_>(F)^t.$$

Exemple 10. Dans $\mathbb{Q}[x, y]$ muni de l'ordre *grlex* avec $x > y$ on considère les deux polynômes

$$f_1 = x^2y - 2y + x \ , \ f_2 = xy + \frac{1}{2}x^2 - y$$

Posons $F = (f_1, f_2)$ alors $\mathcal{M}on_{grlex}(F) = (x^2y, x^2, xy, x, y)$. D'où la matrice

$$M(F) = \begin{array}{c} \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{ccccc} x^2y & x^2 & xy & x & y \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & -2 \\ 0 & \frac{1}{2} & 1 & 0 & -1 \end{pmatrix} \end{array}$$

La représentation polynomiale de la ligne 1 correspond au polynôme

$$(1, 0, 0, 1, -2)(x^2y, x^2, xy, x, y)^t = x^2y + x - 2y = f_1$$

Réciproquement, si M est une matrice de taille $l \times m$ à coefficients $M_{i,j} \in K$ et $X = (x^{\alpha_1}, \cdots, x^{\alpha_m})$ un vecteur de monômes, alors la représentation polynomiale

de M par rapport à X est le vecteur F de l polynômes déterminé par

$$F^t = M.X^t = Rows(M, X) = \big(Rows_M(1), \cdots, Rows_M(l)\big)^t$$

où $Rows_M(i)$ pour $1 \leq i \leq l$, correspond à la représentation polynomiale de la ligne d'indice i dans la matrice M par rapport au vecteur de base X. Cette représentation est utilisée pour calculer le reste de la division d'un polynôme par un ensemble fini de polynômes en utilisant le calcul matriciel comme le montre l'exemple suivant :

Exemple 11. Soient dans $\mathbb{Q}[x, y]$ les polynômes

$$f = 2x^2 - y \ , \ f_1 = x - 1 \ , \ f_2 = y + 2.$$

Considérons l'ordre lexicographique avec $x > y$ et cherchons le reste de la division de f par (f_1, f_2). Comme $\frac{LM(f)}{LM(f_1)} = \frac{x^2}{x} = x \notin \mathbb{Q}$, alors on ajoute le polynôme $f_3 = xf_1 = x^2 - x$. On a alors, $\mathcal{M}on\big(\{f, f_1, f_2, f_3\}\big) = (x^2, x, y, 1)$, d'où la représentation matricielle suivante :

$$M = \begin{array}{c} \\ f \\ f_1 \\ f_2 \\ f_3 \end{array} \begin{array}{c} \begin{array}{cccc} x^2 & x & y & 1 \end{array} \\ \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 1 & -1 & 0 & 0 \end{pmatrix} \end{array}$$

Notons les lignes de la matrice M par L_1, L_2, L_3 et L_4. Pour obtenir la matrice échelonnée de M, nous allons effectuer des opérations élémentaires sur ses lignes dans l'ordre suivant :

1. Permuter L_1 et L_4.
2. Remplacer L_4 par la combinaison linéaire $L_4 - 2L_1$.

3. Remplacer L_4 par la combinaison linéaire $L_4 - 2L_2$.

4. Remplacer L_4 par la combinaison linéaire $L_4 + L_3$.

On obtient alors la forme échelonnée

$$\widetilde{M} = \begin{array}{c} \\ g_1 \\ g_2 \\ g_3 \\ g_4 \end{array} \begin{array}{c} \begin{array}{cccc} x^2 & x & y & 1 \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix} \end{array}$$

Chacun des polynômes g_1, g_2, g_3 et g_4 s'écrit comme combinaison linéaire des polynômes f, f_1, f_2, f_3 à coefficients dans $\mathbb{Q}$, en particulier le polynôme constant $g_4 = 4$. En substituant f_3 par xf_1 dans cette combinaison, on obtient une écriture de g_4 sous la forme $g_4 = f + h_1 f_1 + h_2 f_2$ avec $h_1, h_2 \in \mathbb{Q}[x, y]$. Ce qui entraine que 4 est un reste de division de f par l'ensemble (f_1, f_2). En effet, en retraçant les étapes de l'algorithme de division dans $\mathbb{Q}[x, y]$, on a :

(i) $2x^2 - y - 2x(x-1) = 2x - y$, d'où $f - 2xf_1 = 2x - y$.

(ii) $2x - y - 2(x-1) = 2 - y$, d'où $f - 2xf_1 - 2f_1 = f - 2(x+1)f_1 = 2 - y$.

(iii) $2 - y + (y+2) = 4$, d'où $f - 2(x+1)f_1 + f_2 = 4$.

Ce résultat peut être reconstruit à partir des opérations élémentaires effectuées sur les lignes de la matrice M. En effet, chaque opération correspond à une étape dans l'algorithme de division comme le montre le tableau suivant :

Opération dans la matrice M	Action dans l'algorithme de division
Remplacer L_4 par $L_4 - 2L_1$	$f - 2xf_1$
Remplacer L_4 par $L_4 - 2L_2$	$f - 2xf_1 - 2f_1$
Remplacer L_4 par $L_4 + L_3$	$f - 2xf_1 - 2f_1 + f_2$

3.2 La matrice de Macaulay

Définition 3.2.1. (Matrice de Macaulay) Soit $F = (f_1, \cdots, f_s)$ un vecteur de s polynômes et d un entier strictement positif. Alors, la *matrice de Macaulay* de degré d de F notée $M_d(F)$ est la représentation matricielle du vecteur $(g_1, \cdots, g_k)$ des polynômes $g_i \in F^{(d)}$, où $F^{(d)}$ est défini par

$$F^{(d)} = \{x^{\alpha_j} f_i \quad | \quad 1 \leq i \leq s, \quad x^{\alpha_j} \in K[x_1, \cdots, x_n] \; et \; |\alpha_j| + deg(f_i) \leq d\}$$

Exemple 12. Dans $\mathbb{Q}[x, y]$ muni de l'ordre lexicographique $x > y$ on considère les deux polynômes

$$f_1 = x^2 - xy + y^2 \; , \; f_2 = x + y$$

Posons $F = (f_1, f_2)$ et soient $d = 2$ et $\alpha \in \mathbb{N}^2$. On a alors :

(i) $|\alpha| + deg(f_1) \leq 2 \implies |\alpha| = 0 \implies \alpha = (0, 0)$ correspond exactement au monôme constant $x^0 y^0 = 1$.

(ii) $|\alpha| + deg(f_2) \leq 2 \implies |\alpha| \leq 1 \implies \alpha \in \{(0, 0), (1, 0), (0, 1)\}$ correspond aux trois monômes différents $x^0 y^0 = 1$, $xy^0 = x$ et $x^0 y = y$.

D'où $F^{(2)} = (f_1, f_2, xf_2, yf_2)$ et la matrice de Macaulay de F de degré 2 est

$$M_2(F) = \begin{array}{c} \\ f_1 \\ f_2 \\ xf_2 \\ yf_2 \end{array} \begin{array}{c} \begin{array}{ccccc} x^2 & xy & x & y^2 & y \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Définition 3.2.2. Si $M(F)$ est la représentation matricielle d'un vecteur de polynômes F, on note $\widetilde{M(F)}$ le résultat de l'algorithme d'élimination de Gauss-Jordan

appliqué à la matrice $M(F)$. Autrement dit, $\widetilde{M(F)}$ est la matrice unique réduite échelonnée en lignes de la matrice $M(F)$.

Définition 3.2.3. Soit F un ensemble fini de polynômes dans $K[x_1, \cdots, x_n]$ et $>$ un ordre monomial. Si $M(F)$ est la représentation matricielle de F, alors on appelle la représentation polynomiale de $\widetilde{M(F)}$ notée $\widetilde{F}$ ou $Rows\left(\widetilde{M(F)}\right)$, la *forme échelonnée* de F (ou élimination de Gauss) suivant l'ordre $>$.

Exemple 13. Dans l'exemple 10 précédent, après application de l'algorithme d'élimination de Gauss-Jordan sur la matrice

$$M(F) = \begin{array}{c} \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{ccccc} x^2y & x^2 & xy & x & y \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & -2 \\ 0 & \frac{1}{2} & 1 & 0 & -1 \end{pmatrix} \end{array}$$

on obtient la matrice suivante :

$$\widetilde{M(F)} = \begin{array}{c} \\ f_1 \\ 2f_2 \end{array} \begin{array}{c} \begin{array}{ccccc} x^2y & x^2 & xy & x & y \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & -2 \\ 0 & 1 & 2 & 0 & -2 \end{pmatrix} \end{array}$$

D'où la forme échelonnée de F est $\widetilde{F} = (f_1, 2f_2)$.

Théorème 3.2.4. Soit M une matrice de taille $d \times s$ et $Y = (y_1, \cdots, y_s)$ des variables telles que $F = Rows(M, Y)$ et $\widetilde{F} = Rows(\widetilde{M}, Y)$ où $\widetilde{M}$ est la forme réduite échelonnée en lignes de M (alors F et $\widetilde{F}$ sont des vecteurs de polynômes de degré 1 en Y). On définit pour l'ordre lexicographique $y_1 > y_2 > \cdots > y_s$ les ensembles suivants :

(i) $\widetilde{F^+} = \left\{ g \in \widetilde{F} \quad | \quad LM(g) \notin LM(F) \right\}$

(ii) $\widetilde{F^-} = \widetilde{F} \setminus \widetilde{F^+}$.

Alors, pour tout sous ensemble $\underline{F} \subseteq F$ tel que $|\underline{F}| = |LM(F)|$ et $LM(\underline{F}) = LM(F)$ on a $G = \widetilde{F^+} \cup \underline{F}$ est une *base triangulaire* du *R-module* V_F généré par F.

Autrement dit, $\forall f \in V_F, \exists(\lambda_1, \cdots, \lambda_k) \in R^k, \exists(g_1, \cdots, g_k) \in G^k$ tels que :

(i) $f = \sum_{i=1}^{k} \lambda_i g_i$.

(ii) $LM(g_1) = LM(f)$.

(iii) $LM(g_i) > LM(g_{i+1}) \quad \forall 1 \leq i < k$.

Démonstration. Comme les termes dominants de G sont deux à deux distincts, (garanti par l'algorithme d'élimination de *Gauss-Jordan* sur la matrice M), alors les éléments de G sont linéairement indépendants. Il suffit donc de montrer qu'ils génèrent tout l'espace V_F pour conclure.

Procédons par l'absurde : supposons qu'il existe $f \in V_F$ tel que $\overline{f}^G = f' \neq 0$. Alors il n'existe aucun $g \in G$ tel que $LM(g)$ divise $LM(f')$. Or $\widetilde{F}$ est une base de Gröbner pour V_F alors $\overline{f'}^{\widetilde{F}} = 0$. Donc il existe un polynôme $h \in \widetilde{F}$ pour lequel $LM(h)$ divise $LM(f')$ d'où la contradiction car $LM(h) \in LM(\widetilde{F^+}) \cup LM(\widetilde{F^-}) = LM(\widetilde{F^+}) \cup LM(\underline{F}) = LM(G)$. □

Ce théorème peut être transposé au cas des polynômes (en substituant les variables $y_1, \cdots, y_s$ par des monômes $x^{\alpha_1}, \cdots, x^{\alpha_s}$) comme l'énonce le corollaire suivant :

Corollaire 3.2.5. Soit F un sous ensemble fini de $R = K[x_1, \cdots, x_n]$, et $>$ un ordre monomial sur R. On définit l'ensemble $\widetilde{F^+} = \left\{ g \in \widetilde{F} \quad | \quad LM(g) \notin LM(F) \right\}$ où $\widetilde{F}$ est la forme échelonnée réduite de F. Alors, pour tout sous ensemble $\underline{F} \subseteq F$ tel que $|\underline{F}| = |LM(F)|$ et $LM(\underline{F}) = LM(F)$ on a $G = \widetilde{F^+} \cup \underline{F}$ est une *base triangulaire* de V_F comme *R-module* généré par F. Autrement dit, $\forall f \in V_F, \exists(\lambda_1, \cdots, \lambda_m) \in R^m, \exists(g_1, \cdots, g_m) \in G^m$ tels que :

(i) $f = \sum_{i=1}^{m} \lambda_i g_i$.

(ii) $LM(g_1) = LM(f)$.

(iii) $LM(g_i) > LM(g_{i+1}) \quad \forall 1 \leq i < m$.

Ce corollaire est utilisé par l'algorithme F4 pour la réduction des *S-polynômes*.

3.3 Les paires critiques de polynômes

La notion de *paire critique de polynômes* utilisée dans l'algorithme F4 correspond exactement aux *S-polynômes* définis auparavant, avec une formulation différente adaptée aux calcul matriciel.

Définition 3.3.1. Soit $\mathcal{M}on$ l'ensemble des monômes de $K[x_1, \cdots, x_n]$ muni d'un ordre monomial. Une *paire critique* des deux polynômes $f_i, f_j \in K[x_1, \cdots, x_n]$, est un élément de l'ensemble $\mathcal{M}on \times \mathcal{M}on \times K[x_1, \cdots, x_n] \times \mathcal{M}on \times K[x_1, \cdots, x_n]$ défini par

$$paire(f_i, f_j) = \big(ppcm_{i,j}, t_i, f_i, t_j, f_j\big)$$

où $ppcm_{i,j} = ppcm\,(LM(f_i), LM(f_j)) = t_i.LM(f_i) = t_j.LM(f_j)$.

Remarque 3.3.2. Par abus de langage on écrit (f, g) au lieu de $paire(f, g)$.

Définition 3.3.3. On appelle *degré de la paire critique* $p_{i,j} = (f_i, f_j)$, et on note $deg(p_{i,j})$, le degré du monôme $ppcm_{i,j} = ppcm\big(LM(f_i), LM(f_j)\big)$. De plus on définit les opérations de *projection* suivantes :

(i) $Left\,(p_{i,j}) = (t_i, f_i)$ noté $t_i f_i$ où $t_i = \dfrac{ppcm_{i,j}}{LM(f_i)}$.

(ii) $Right\,(p_{i,j}) = (t_j, f_j)$ noté $t_j f_j$ où $t_j = \dfrac{ppcm_{i,j}}{LM(f_j)}$.

Exemple 14. Considérons dans $\mathbb{Q}[x, y]$ muni de l'ordre lexicographique gradué avec $x > y$, les deux polynômes $f = x^2 - xy + 1$ et $g = 2xy + y^2 + x$.

On a $LM(f) = x^2$ et $LM(g) = xy$. Alors, $ppcm\big(LM(f), LM(g)\big) = x^2 y$ d'où :

(i) $paire(f,g) = (x^2y, y, f, x, g)$.

(ii) $Right\,(f,g) = (x,g)$ noté xg (image par multiplication).

(iii) $Left\,(f,g) = (y,f)$ noté yf (image par multiplication).

3.4 L'algorithme de base F4

Dans cette section, nous allons d'abord introduire le pseudo code de l'algorithme de base F4 tel qu'il est présenté dans l'article (Faugére, 1999) en expliquant le rôle de chaque procédure et en donnant les éléments de preuve d'exactitude et de finition de l'algorithme tels qu'ils sont développés dans l'article (Faugére, 1999), puis illustrer son fonctionnement pas à pas sur l'exemple 15.

Algorithm 3 Algorithme de base F4

Entrée : $F = \{f_1, \cdots, f_s\}$ un ensemble fini de polynômes.
Sortie : Une base de Gröbner $G = \{g_1, \cdots, g_t\}$ pour $\langle F \rangle$ avec $F \subseteq G$.
$G = F$
$\widetilde{F_0}^{+} = F$
$d = 0$
$P = \{paire(f,g)$ tel que $(f,g) \in G^2$ et $f \neq g\}$
tant que $P \neq \emptyset$ **faire**
  $d = d + 1$
  $P_d = Select(P)$ ▷ sélectionne la liste des paires critiques de plus petit degré
  $P = P \setminus P_d$
  $L_d = Left(P_d) \cup Right(P_d)$
  $\widetilde{F_d}^{+} = Reduction(L_d, G)$
  pour $h \in \widetilde{F_d}^{+}$ **faire**
    $P = P \cup \{paire(h,g)$ tel que $g \in G\}$
    $G = G \cup \{h\}$
  fin pour
fin tant que
  retourner G

Remarque 3.4.1. Les fonctions *Left* et *Right* utilisées dans l'algorithme 3, prennent en entrée un ensemble fini de paires critiques P et renvoient en sortie un ensemble fini de couples (t_i, f_i) tels que :

— $Left(P) = \{Left(p_{i,j}),$ pour toute paire critique $p_{i,j} \in P\}$.

— $Right(P) = \{Right(p_{i,j}),$ pour toute paire critique $p_{i,j} \in P\}$.

La fonction *Reduction* est une généralisation de la réduction d'un polynôme f par un sous ensemble fini G de $K[x_1, \cdots, x_n]$ à la réduction d'un sous ensemble fini de polynômes L par un autre sous ensemble fini de polynômes G. Elle retourne en sortie un sous ensemble fini $F \subseteq K[x_1, \cdots, x_n]$. Son pseudo code est le suivant :

Algorithm 4 Reduction

Entrée : $\begin{cases} L : & \text{sous ensemble fini de } \mathcal{M}on \times K[x_1, \cdots, x_n] \\ G : & \text{sous ensemble fini de } K[x_1, \cdots, x_n] \end{cases}$
Sortie : $\widetilde{F}^+$ sous ensemble fini de $K[x_1, \cdots, x_n]$ éventuellement vide.
$F = SymbolicPreprocessing\big(L, G\big)$
$\widetilde{F} =$ *Réduction de Gauss-Jordan* de F suivant l'ordre monomial fixé.
$\widetilde{F}^+ = \big\{f \in \widetilde{F}$ tel que $LM(f) \notin LM(F)\big\}$
retourner $\widetilde{F}^+$

La fonction *Reduction* fait appel à la fonction *SymbolicPreprocessing* qui représente la fonction principale de l'algorithme F4. En effet, cette dernière permet de calculer la matrice $M(F)$ et d'ajouter en fonction de L et G tous les polynômes nécessaires pour que la réduction de Gauss-Jordan appliquée à la matrice $M(F)$ contienne toutes les réductions possibles modulo G des éléments de l'ensemble L. L'appellation "Symbolic" doit son nom au fait qu'aucune opération arithmétique n'est effectuée sur les polynômes pour générer l'ensemble F comme le montre le pseudo code suivant :

Algorithm 5 SymbolicPreprocessing

Entrée : $\begin{cases} L: & \text{sous ensemble fini de } \mathcal{M}on \times K[x_1, \cdots, x_n] \\ G: & \text{sous ensemble fini de } K[x_1, \cdots, x_n] \end{cases}$
Sortie : F sous ensemble fini de $K[x_1, \cdots, x_n]$.
$F = \{tf \text{ tel que } (t, f) \in L\}$
$Done = LM(F)$ suivant l'ordre monomial fixé.
tant que $\mathcal{M}on(F) \neq Done$ **faire**
  $m =$ *Sélectionner un élément dans* $\mathcal{M}on(F) \setminus Done$
  $Done = Done \cup \{m\}$
  si $\exists f \in G, \exists m' \in \mathcal{M}on$ *tel que* $m = m' LM(F)$ **alors**
    $F = F \cup \{m' f\}$
  fin si
fin tant que
  retourner F.

Dans le cas où le nombre d'éléments de G est inférieur ou égal au nombre de monômes de F, l'analyse de la fonction *SymbolicPreprocessing* montre que sa complexité est *linéaire* ce qui justifie son efficacité en termes de temps d'exécution. Pour montrer que l'algorithme F4 calcule bien une base de Gröbner de l'idéal engendré par l'ensemble F, nous avons besoin des lemmes suivants :

Lemme 3.4.2. Soit G un sous ensemble fini de $K[x_1, \cdots, x_n]$ et L l'image par multiplication d'un sous ensemble fini de $\mathcal{M}on \times G$ et $\widetilde{F}^+ = Reduction\big(L, G\big)$ alors,

$$\forall h \in \widetilde{F}^+ : LM(h) \notin I = \langle LM(G) \rangle.$$

Démonstration. Soit F l'ensemble des polynômes issu de l'exécution de la fonction *SymbolicPreprocessing* (L, G). Supposons (par l'absurde) qu'il existe un polynôme $h \in \widetilde{F}^+$ tel que $t = LM(h) \in I = \langle LM(G) \rangle$. Alors il existe $g \in G$ tel que $LM(g)$ *divise* t. Donc $t \in \mathcal{M}on\big(\widetilde{F}^+\big) \subseteq \mathcal{M}on\big(\widetilde{F}\big) \subseteq \mathcal{M}on\big(F\big)$. D'où l'élément $\frac{t}{LM(g)} g$ est inséré dans F par la fonction *SymbolicPreprocessing*, ce qui contredit le fait que $LM(h) \notin LM(F)$. □

Lemme 3.4.3. Soit G un sous ensemble fini de $K[x_1, \cdots, x_n]$ et L l'image par multiplication d'un sous ensemble fini de $\mathcal{M}on \times G$ et $\widetilde{F}^+ = Reduction\big(L, G\big)$ alors,

(i) $\widetilde{F}^+ \subseteq I = \langle G \rangle$.

(ii) $\forall f \in V_L,\ \overline{f}^{G \cup \widetilde{F}^+} = 0$ où V_L est le *R-module* généré par L.

Démonstration. Si F est le résultat de la fonction *SymbolicPreprocessing* avec comme entrées L et G, alors F est évidemment un sous ensemble de $L \cup \langle G \rangle$ car l'ensemble F est initialisé au départ à L puis il est complété au fur et à mesure par des éléments de la forme $t.g$ tels que $t \in Mon$ et $g \in G$ donc $t.g \in \langle G \rangle$. De plus, il est évident que L est un sous ensemble de l'idéal engendré par G. Alors on a clairement $F \subseteq \langle G \rangle$ ce qui entraine que $\widetilde{F}^+ \subseteq \langle G \rangle$. Pour la deuxième partie du lemme, comme $F \subseteq \langle G \rangle$ alors tout sous ensemble de F est un sous ensemble de $\langle G \rangle$. En particulier, le sous ensemble $\underline{F}$ qui vérifie les conditions du théorème 3.2.4. D'où par le corollaire 3.2.5 on a $\forall f \in V_F, \quad \overline{f}^{G \cup \widetilde{F}^+} = 0$ ce qui conclue la démonstration car V_L est un sous module de V_F. □

Théorème 3.4.4. L'algorithme 3 (Algorithme de base F4) calcule une base de Gröbner G de l'idéal $I = \langle F \rangle \subseteq K[x_1, \cdots, x_n]$ telle que $F \subseteq G$.

Démonstration. La boucle principale *"tant que"* de l'algorithme 3, génère une suite croissante d'entiers naturels $\big(d_i\big)_{i \in \mathbb{N}}$ tel que $\widetilde{F_{d_i}}^+ \neq \emptyset$ pour tout $i \in \mathbb{N}$.

Soit $q_i \in \widetilde{F_{d_i}}^+$ et $J_i = \begin{cases} J_{i-1} \cup \langle LM(q_i) \rangle & \text{si } i > 0 \\ \big\{0\big\} & \text{si } i = 0 \end{cases}$.

Supposons (par l'absurde) que la boucle principale ne se termine pas. Par le lemme 3.4.2 on a la chaine strictement croissante $J_0 \subset J_1 \subset \cdots \subset J_i \subset J_{i+1} \subset \cdots$. D'où la contradiction (condition de la chaine ascendante du théorème 2.3.3) ce qui montre bien la terminaison de l'algorithme.

Montrons que l'algorithme calcule exactement une base de Gröbner pour l'idéal généré par F. On a par construction $G = \bigcup_{d\geq 0} \widetilde{F_d}^+$ avec $\widetilde{F_0}^+ = F$. Par le lemme 3.4.3 on a que G est un sous ensemble fini de $K[x_1, \cdots, x_n]$ tel que $F \subseteq G \subset \langle F \rangle$. Il reste à montrer que pour tout $g_1, g_2 \in G : (g_1, g_2) \notin P \implies \overline{S\big(g_1, g_2\big)}^G = 0$. Soit$\big(g_1, g_2\big) \in G^2$ tel que $\big(g_1, g_2\big) \notin P$. Alors la paire critique $(g_1, g_2) = \big(ppcm_{12}, t_1, g_1, t_2, g_2\big)$ a été sélectionnée à une étape antérieure (soit pour un certain entier d) par la fonction *Select*. On a alors $t_1 g_1 \in L_d$ et $t_2 g_2 \in L_d$. Par conséquent $S(g_1, g_2) = t_1 g_1 - t_2 g_2 \in V_{L_d}$ (le *R-module* généré par L_d). D'où par le lemme 3.4.3 $\overline{S\big(g_1, g_2\big)}^G = 0$. □

Pour clore le chapitre, nous allons illustrer en pas à pas le fonctionnement de l'algorithme de base F4 sur l'exemple 15.

Exemple 15. Dans $\mathbb{Q}[x, y, z]$ muni de l'ordre lexicographique gradué inverse avec $x > y > z$ on considère les polynômes

$$f_1 = x^2 + xy - 1,\ f_2 = x^2 - z^2,\ f_3 = xy + 1$$

Soit à calculer une base de Gröbner G pour l'idéal $I = \langle f_1, f_2, f_3 \rangle$. Pour commencer, les ensembles G et $\widetilde{F_0}^+$ sont initialisés à

$$G = \widetilde{F_0}^+ = F = \big\{f_1, f_2, f_3\big\}.$$

L'entier d est initialisé à 0 et l'ensemble P des paires critiques est initialisé à

$$\begin{aligned} P &= \big\{(f_1, f_2), (f_1, f_3), (f_2, f_3)\big\} \\ &= \big\{(x^2, 1, f_1, 1, f_2); (x^2y, y, f_1, x, f_3); (x^2y, y, f_2, x, f_3)\big\} \end{aligned}$$

On a alors

$$deg\big((f_1, f_2)\big) = deg(x^2) = 2.$$
$$deg\big((f_1, f_3)\big) = deg(x^2y) = 3.$$
$$deg\big((f_2, f_3)\big) = deg(x^2y) = 3.$$

Comme (f_1, f_2) est la seule paire critique dans P de plus petit degré égal à 2, la première itération de la boucle principale se réduit aux affectations suivantes :

$$d = 1.$$
$$P_1 = \big\{(f_1, f_2)\big\}.$$
$$P = \big\{(f_1, f_3), (f_2, f_3)\big\}$$

On a alors
$$\begin{cases} Left(f_1, f_2) = (1, f_1) \\ Right(f_1, f_2) = (1, f_2) \end{cases} \implies L_1 = \big\{f_1, f_2\big\}$$

La fonction *SymbolicPreprocessing* appliquée à L_1 et G construit l'ensemble $F = \big\{f_1, f_2, f_3\big\}$ d'où la matrice $M(F)$ associée est

$$M(F) = \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \end{array} \begin{array}{c} \begin{array}{cccc} x^2 & xy & z^2 & 1 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Par l'algorithme d'élimination de Gauss, on obtient la matrice

$$\widetilde{M(F)} = \begin{array}{c} \\ g_1 \\ g_2 \\ g_3 \end{array} \begin{array}{c} \begin{array}{cccc} x^2 & xy & z^2 & 1 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -2 \end{pmatrix} \end{array}$$

On a alors $\widetilde{F_1}^+ = \{g_3\} = \{z^2 - 2\}$ car g_3 est le seul polynôme dans $Rows\big(\widetilde{M(F)}\big)$ dont le terme dominant n'appartient pas à l'ensemble des termes dominants de F. Posons $f_4 = g_3$ et mettons à jour les ensembles G et P

$$\begin{aligned} P &= \big\{(f_1, f_3), (f_2, f_3), (f_1, f_4), (f_2, f_4), (f_3, f_4)\big\}. \\ G &= \big\{f_1, f_2, f_3, f_4\big\}. \end{aligned}$$

En considérant les nouveaux ensembles G et P, on passe à la deuxième itération de la boucle. Comme (f_1, f_3) et (f_2, f_3) sont les seules paires critiques dans P de plus petit degré égal à 3, on effectue les affectations suivantes :

$$\begin{aligned} d &= 2. \\ P_2 &= \big\{(f_1, f_3); (f_2, f_3)\big\}. \\ P &= \big\{(f_1, f_4), (f_2, f_4); (f_3, f_4)\big\} \end{aligned}$$

On a alors

$$\begin{cases} Left(f_1, f_3) = (y, f_1) \\ Right(f_1, f_3) = (x, f_3) \\ Left(f_2, f_3) = (y, f_2) \\ Right(f_2, f_3) = (x, f_3) \end{cases} \implies L_2 = \big\{yf_1, yf_2, xf_3\big\}$$

La fonction *SymbolicPreprocessing* appliquée à L_2 et G construit l'ensemble $F =$

$\{yf_1, yf_2, xf_3, yf_3, yf_4\}$ d'où la matrice $M(F)$ associée est

$$M(F) = \begin{array}{c} \\ yf_1 \\ yf_2 \\ xf_3 \\ yf_3 \\ yf_4 \end{array} \begin{array}{c} \begin{array}{ccccc} x^2y & xy^2 & yz^2 & x & y \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -2 \end{pmatrix} \end{array}$$

Par l'algorithme d'élimination de Gauss, on obtient la matrice

$$\widetilde{M(F)} = \begin{array}{c} \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \end{array} \begin{array}{c} \begin{array}{ccccc} x^2y & xy^2 & yz^2 & x & y \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

On a alors, $\widetilde{F_2}^+ = \{h_4\} = \{x+2y\}$ car h_4 est le seul polynôme dans $Rows\big(\widetilde{M(F)}\big)$ dont le terme dominant n'appartient pas à l'ensemble des termes dominants de F. Posons $f_5 = h_4$ et mettons à jour les ensembles G et P.

$$P = \big\{(f_1, f_5), (f_2, f_5), (f_3, f_5), (f_4, f_5), (f_1, f_4), (f_2, f_4), (f_3, f_4)\big\}.$$
$$G = \big\{f_1, f_2, f_3, f_4, f_5\big\}.$$

En considérant les nouveaux ensembles G et P, la troisième itération de la boucle ajoute le polynôme $f_6 = y^2 - \frac{1}{2}$ à l'ensemble G et met à jour l'ensemble des paires critiques P en ajoutant les nouvelles paires $(f_1, f_6), (f_2, f_6), (f_3, f_6), (f_4, f_6)$ et (f_5, f_6). Le reste des itérations de la boucle principale ne rajoute aucun nouveau

polynôme à l'ensemble G. Elle est rompue après avoir sélectionné toutes les paires critiques de P. Ainsi, l'algorithme se termine avec l'ensemble

$$G = \left\{ x^2 + xy - 1, x^2 - z^2, xy + 1, z^2 - 2, x + 2y, y^2 - \frac{1}{2} \right\}$$

comme base de Gröbner (non réduite) pour l'idéal

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

CHAPITRE IV

L'ALGORITHME F5

L'algorithme F5 a été introduit par (Faugère 2002) mais sans donner de preuves complètes de sa terminaison ni de sa correction. Sa compréhension détaillée a nécessité une dizaines d'années durant lesquelles des explications éparpillées dans plusieurs articles et documents ont vu le jour. Notamment, la version simplifiée de l'algorithme décrite au chapitre 10 du livre de référence (Cox *et al.*, 2015).

Le principe de l'algorithme F5 est basé sur un nouveau concept appelé la *signature* d'un polynôme dont les propriétés permettent efficacement d'optimiser les calculs en éliminant un nombre record de calculs inutiles à l'application de deux nouveaux critères (critère de réécriture et le critère F5), ce nombre pouvant atteindre la totalité des calculs inutiles dans le cas où le système d'entrée de l'algorithme est *régulier* (voir la définition 1.2.5).

En effet, dans le processus de calcul de la base de Gröbner pour un idéal $I = \langle f_1, \cdots, f_m \rangle$ par l'algorithme F4, les matrices générées ne sont pas souvent de rang plein. Ce qui signifie que les lignes de ces matrices ne sont pas linéairement indépendantes. Et comme chaque ligne dans ces matrices correspond a un produit tf_i où t est un monôme dans $K[x_1, \cdots, x_n]$, cette dépendance linéaire s'exprime sous la forme $\sum_{t,f_i} \lambda_{t,f_i} t f_i = 0$ avec $\lambda_{t,f_i} \in K$. En regroupant les termes pour chaque f_i on obtient une formule de la forme

$$\sum_{i=1}^{m} g_i f_i = 0, \quad g_i \in K[x_1, \cdots, x_n] \qquad (\alpha)$$

L'algorithme F5 s'applique aux systèmes dont les seuls vecteurs $(g_1, \cdots, g_m)$ qui vérifient la formule (α) sont ceux induits par les relations $f_i f_j - f_j f_i = 0$ ce qui est le cas pour toute *séquence régulière* de polynômes homogènes $f_1, \cdots, f_m$.

Dans ce chapitre, nous allons présenter la version de l'algorithme F5 telle qu'elle est décrite dans l'article (Faugère, 2002) en expliquant tous les pseudo codes des sous algorithmes. Pour commencer, nous allons définir les différentes notions auxquelles l'algorithme fait appels.

4.1 Vecteurs de polynômes et Syzygy

Dans toute la suite du document, R désigne l'anneau des polynômes $K[x_1, \cdots, x_n]$ et $\mathcal{M}on(R)$ désigne l'ensemble des monômes de R.

Un vecteur de polynômes $g = (g_1, \cdots, g_m) \in R^m \setminus \{0\}$ peut s'écrire comme combinaison linéaire finie, à coefficients dans $\mathcal{M}on(R)$, des vecteurs $\big(e_i\big)_{1 \leq i \leq m}$ de la base *canonique* (ou *standard*) de R^m. Les éléments de cette somme sont appelés les *termes du vecteur* g.

Exemple 16. Soit $R = \mathbb{Q}[x, y, z]$ muni de l'ordre lexicographique $x > y > z$. Le vecteur $g = (x^2 - 3y, z - x) \in R^2$ s'écrit de la forme

$$g = x^2 e_1 - 3y e_1 + z e_2 - x e_2$$

où $e_1 = (1, 0)$ et $e_2 = (0, 1)$ sont les vecteurs de la base canonique de R^2. L'ensemble des termes du vecteur g est

$$\big\{x^2 e_1, -3y e_1, z e_2, -x e_2\big\}.$$

Nous allons maintenant définir un ordre sur les termes d'un vecteur de polynômes.

Définition 4.1.1. Soit $>_R$ un ordre monomial défini sur R. On définit un ordre $\succ$ sur les termes d'un vecteur de polynômes dans R^m comme suit :

$$\forall (i,j) \in \{1, \cdots, m\}^2 : \; x^\alpha e_i \succ x^\beta e_j \iff \begin{cases} i < j & \text{ou} \\ i = j & \text{et } x^\alpha >_R x^\beta \end{cases}$$

Comme résultat direct de cette définition, on a

$$e_1 \succ e_2 \succ \cdots \succ e_{m-1} \succ e_m.$$

Exemple 17. Dans l'exemple 16 on a les relations suivantes :

(i) $x^2 e_1 \succ z e_2$ car $e_1 \succ e_2$.

(ii) $-x e_2 \succ z e_2$ car $x > z$.

Soient deux vecteurs $a = (a_1, \cdots, a_m) \in R^m$, $b = (b_1, \cdots, b_m) \in R^m$ et $f \in R$ un polynôme. On définit les opérations suivantes :

(i) $a \oplus b = (a_1 + b_1, \cdots, a_m + b_m) \in R^m$ (addition dans R^m).

(ii) $f \otimes a = (a_1 f, \cdots, a_m f) \in R^m$ (multiplication par les éléments de R).

Proposition 4.1.2. L'ensemble R^m muni des opérations $\oplus$ et $\otimes$ a la structure d'un *R-module*.

Démonstration. Soient $a = (a_1, \cdots, a_m) \in R^m$, $b = (b_1, \cdots, b_m) \in R^m$ et $f, g \in R$.

(i) Montrons que $f \otimes (a \oplus b) = f \otimes a \oplus f \otimes b$:

$$\begin{aligned} f \otimes (a \oplus b) &= f \otimes (a_1 + b_1, \cdots, a_m + b_m) \\ &= \big(f(a_1 + b_1), \cdots, f(a_m + b_m)\big) \\ &= \big(fa_1, \cdots, fa_m\big) \oplus \big(fb_1, \cdots, fb_m\big) \\ &= f \otimes a \oplus f \otimes b. \end{aligned}$$

(ii) Montrons que $(f + g) \otimes a = \big(f \otimes a\big) \oplus \big(g \otimes a\big)$:

$$\begin{aligned} (f + g) \otimes a &= \big((f + g)a_1, \cdots, (f + g)a_m\big) \\ &= \big(fa_1 + ga_1, \cdots, fa_m + ga_m\big) \\ &= \big(f \otimes a\big) \oplus \big(g \otimes a\big). \end{aligned}$$

(iii) Montrons que $(fg) \otimes a = f \otimes \big(g \otimes a\big)$:

$$\begin{aligned} (fg) \otimes a &= \big(fga_1, \cdots, fga_m\big) \\ &= f \otimes \big(ga_1, \cdots, ga_m\big) \\ &= f \otimes \big(g \otimes a\big). \end{aligned}$$

□

(iv) $1.a = (1.a_1, \cdots, 1.a_m) = a$.

Comme résultat immédiat de cette proposition, pour chaque idéal de la forme $I = \langle f_1, \cdots, f_m \rangle \subseteq R$, il existe un *morphisme de R-modules surjectif* v_F défini comme suit :

$$\begin{aligned} v_F : \qquad R^m &\longrightarrow I = \langle f_1, \cdots, f_m \rangle \\ g = (g_1, \cdots g_m) &\longmapsto v_F\big(g\big) = \sum_{i=1}^{m} f_i g_i \end{aligned}$$

Le morphisme v_F (appelé morphisme d'*évaluation*) tel qu'il est défini, vérifie les propriétés suivantes :

(i) $\forall i = 1 \cdots m, v_F\big(e_i\big) = f_i$.

(ii) $\forall i, j = 1 \cdots m, v_F\big(f_j e_i - f_i e_j\big) = 0 \in R$ (le polynôme nul).

(iii) v_F n'est jamais *injectif* pour $m \geq 2$ ($Ker(v_F) \neq \{0\}$) où $Ker(v_F)$ est le *noyau* du morphisme v_F qui est un *sous module* de R^m .

Définition 4.1.3. Soit $F = \big(f_1, \cdots, f_m\big) \in R^m$. On dit que le vecteur $g = (g_1, \cdots, g_m\big) \in R^m$ est un *F-Syzygy* si $v_F(g) = 0$.

Autrement dit, g est un *F-Syzygy* si $g \in Ker(v_F)$. On note alors $Ker(v_F)$ par $Syz(F)$.

Remarque 4.1.4. Si $F = \big(f_1, \cdots, f_m\big) \in R^m$ alors pour toute paire d'entiers positifs $\big(i, j\big)_{1 \leq i < j \leq m}$ on a

$$k_{ij} = f_i e_j - f_j e_i \in Syz(F)$$

Ces Syzygys *triviaux* sont connus sous le nom de *Syzygy de Koszul*. Dans le cas d'une séquence *régulière* de polynômes homogènes $f_1, \cdots, f_m$ (voir la définition 1.2.5), l'ensemble $Syz(F)$ coïncide avec le sous module $PSyz$ des Syzygys engendrés par les Syzygys de Koszul. Autrement dit, $Syz = PSyz$.

Définition 4.1.5. Soient $g = (g_1, \cdots, g_m)$ et $h = (h_1, \cdots, h_m)$ deux vecteurs dans R^m. L'*indexe* de g noté $index(g)$ est le plus petit entier i tel que $g_i \neq 0$. Posons $index(g) = i$ et $index(h) = j$. On écrit $g \succ h$ si et seulement si :

(i) $i < j$ ou

(ii) $i = j$ et $LM(g_i) >_R LM(h_i)$ où $>_R$ est un ordre monomial dans R.

Par convention, $\forall g \in R^m \quad g \succ 0$ (0 est le vecteur nul de R^m).

Exemple 18. Considérons les vecteurs suivants dans $\mathbb{Q}[x,y]^4$:

$$g = (0, x, y, x^2) \quad ; \quad h = (0, x^2, y, x^2) \quad ; \quad l = (0, 0, y, x).$$

On a alors :

$$index(g) = index(h) = 2 \quad ; \quad index(l) = 3.$$

En fixant l'ordre *grevlex* sur $\mathbb{Q}[x,y]$ avec $x > y$ on a :

— $g \succ l$ car $index(l) > index(g)$.

— $h \succ l$ car $index(l) > index(h)$.

— $h \succ g$ car $index(h) = index(g)$ et $x^2 >_{grevlex} x$.

Par extension à la notion de *terme dominant* par rapport à la relation d'ordre monomial $>$, on définit le *terme dominant* d'un vecteur de polynômes $g \in R^m$ par

$$LT(g) = LM(g_i).e_i$$

où $i = index(g)$ et e_i est le $i^{ème}$ vecteur de la base canonique de R^m.

Exemple 19. Dans l'exemple précédent, on a :

$$LT(g) = xe_2 \quad ; \quad LT(h) = x^2e_2 \quad ; \quad LT(l) = ye_3.$$

4.2 La signature d'un polynôme

Dans cette section, nous allons introduire la notion de *signature* d'un polynôme sur laquelle se base l'algorithme F5. Pour motiver la définition de signature d'un polynôme, notons que pour tout polynôme $f \in I = \langle f_1, \ldots, f_m \rangle \subseteq R$, il existe au

moins un vecteur de polynômes $(h_1, \ldots, h_m) \in R^m$ tel que

$$h_1 f_1 + h_2 f_2 + \cdots + h_m f_m = f.$$

Parmi ces vecteurs, on choisira un qui est minimal pour l'ordre $\succ$.

Définition 4.2.1. Soit $I = \langle f_1, \ldots, f_m \rangle \subseteq R$ et v le morphisme d'évaluation défini de R^m dans I. La *signature de* f dans R^m est $LM(h_k)e_k$, où $(h_1, \ldots, h_m) \in R^m$ vérifie

— $h_1 = h_2 = \cdots = h_{k-1} = 0$ et $h_k \neq 0$;

— $v(h_1, \ldots, h_m) = h_k f_k + h_{k+1} f_{k+1} + \cdots + h_m f_m = f$;

— si $v(h'_1, \ldots, h'_m) = f$ avec $h'_1 = \cdots = h'_{j-1} = 0$ et $h_j \neq 0$, alors $j \leq k$.

Montrons que la définition de signature d'un polynôme est bien définie.

Pour un monôme $t \in LM(I)$ posons

$$W(t) = \{g \in R^m \mid LM\left(v(g)\right) = t\}.$$

Comme v n'est pas injectif, l'ensemble $W(t)$ peut contenir plus qu'un élément. La proposition suivante nous permet d'associer à chaque monôme $t \in LM(I)$ un vecteur unique dans $W(t)$.

Proposition 4.2.2. Soit $I = \langle f_1, \cdots, f_m \rangle \subseteq R$ et v le morphisme d'évaluation défini de R^m dans I, et soit

$$\begin{aligned} w : \quad & LM(I) \longrightarrow R^m \\ & t \longmapsto min_{\succ} W\big(t\big) \end{aligned}$$

Si $(t_1, t_2) \in LM(I)^2$ tel que $t_1 \neq t_2$ alors $LT\big(w(t_1)\big) \neq LT\big(w(t_2)\big)$.

Démonstration. Fixons un ordre monomial $>$ dans R et posons $g = w(t_1)$ et $h = w(t_2)$. Supposons (par l'absurde) que $LT(g) = LT(h)$ et que $t_1 \neq t_2$ alors il existe un entier $k > 0$ tel que

$$\begin{cases} t_1 = \sum_{i=k}^{m} g_i f_i & \text{car } t_1 \in I \\ t_2 = \sum_{i=k}^{m} h_i f_i & \text{car } t_2 \in I \\ LM(g_k) = LM(h_k) & \text{car } LT(g) = LT(h) \end{cases}$$

Sans perte de généralité, supposons que $t_1 > t_2$. Alors $LM(t_1 - t_2) = t_1$. Comme $v(g) = t_1$ et $v(h) = t_2$ alors $v(g - h) = t_1 - t_2$. Autrement dit, $g - h$ est dans $W\left(LM(t_1 - t_2)\right) = W\left(t_1\right)$, alors par la minimalité de g on a que $g - h \succ g$. Or, en choisissant g_k et h_k *unitaires* (coefficient dominant égale à 1), ce qui est toujours possible, on obtient $index(g-h) > k$ car $LM(g_k) - LM(h_k) = 0$ et donc $g \succ (g - h)$ d'où la contradiction. □

4.3 Les polynômes signés

Définition 4.3.1. Un *polynôme signé* dans R^m est un couple $\left(ue_i, f\right)$ où $u \in \mathcal{M}on(R)$, $f \in R$ et e_i est un vecteur de la base standard de R^m.

Pour un polynôme signé $r = (ue_k, f)$ on définit les éléments suivants :

1. $poly(r) = f$: le polynôme de r.
2. $\mathcal{S}ign(r) = ue_k$: *signature* de r.
3. $LT(r) = LT(f)$: terme dominant de r.
4. $LM(r) = LM(f)$: monôme dominant de r.
5. $LC(r) = LC(f)$: coefficient dominant de r.

Remarque 4.3.2. Dans la suite du document, nous allons noter par $\mathcal{L}$ l'ensemble

des couples $\big(ue_i, f\big) \in R^m \times R$ pour désigner l'ensemble des polynômes signés dans R^m.

Pour manipuler les polynômes signés, nous allons définir quelques opérations.

Soient (ue_k, f) et (ve_j, g) deux polynômes signés dans R^m. Pour $\lambda \in K \setminus \{0\}$ et $t \in \mathcal{M}on(R)$ on définit les opérations suivantes :

(i) $\lambda.(ue_k, f) = (ue_k, \lambda f) \in \mathcal{L}$.

(ii) $t.(ue_k, f) = (tue_k, tf) \in \mathcal{L}$.

(iii) $(ue_k, f) + (ve_j, g) = \big(max_{\succ}\{ue_k, ve_j\}, f + g\big) \in \mathcal{L}$.

Exemple 20. Dans $\mathbb{Q}[x, y]^3$ on considère les polynômes signés $r = (xe_1, f)$, $s = (ye_1, g)$ et $u = (ye_2, h)$ avec $f, g, h \in \mathbb{Q}[x, y]$. En fixant l'ordre lexicographique $(x > y)$ on a :

1. $3r = 3(xe_1, f) = (xe_1, 3f)$.
2. $x^2 s = x^2(ye_1, g) = (x^2 ye_1, x^2 g)$.
3. $r + s = (xe_1, f) + (ye_1, g) = (xe_1, f + g)$ car $xe_1 \succ ye_1$.
4. $r - u = (xe_1, f) - (ye_2, h) = (xe_1, f - h)$ car $xe_1 \succ ye_2$.

4.4 Les paires critiques de polynômes signés

Définition 4.4.1. Soient $r_1, r_2 \in \mathcal{L}$. On appelle *paire critique* de r_1 et r_2 (dans cet ordre), le *5-uplet* $(ppcm_{12}, u_1, r_1, u_2, r_2)$ où :

(i) $ppcm_{1,2} = ppcm\big(LT(r_1), LT(r_2)\big) = u_1 LT(r_1) = u_2 LT(r_2)$.

(ii) $\mathcal{S}ign(u_1 r_1) \succ \mathcal{S}ign(u_2 r_2)$.

Le degré du monôme $ppcm_{1,2}$ est dit aussi le degré de la paire critique (r_1, r_2).

Exemple 21. Dans $\mathbb{Q}[x,y]^3$ on considère les polynômes signés

$$r = (xe_1, x^2 + xy)\ ;\ s = (e_1, xy - x)\ ;\ u = (ye_2, x + 2y)$$

En fixant l'ordre lexicographique gradué avec $(x > y)$ on a :

1. La paire critique de r et s dans cet ordre est (x^2y, y, r, x, s) car $ppcm(x^2, xy) = x^2y$ et $\mathcal{S}ign(yr) = xye_1 \succ \mathcal{S}ign(xs) = xe_1$.
2. La paire critique de r et u dans cet ordre est $(x^2, 1, r, x, u)$ car $ppcm(x^2, x) = x^2$ et $\mathcal{S}ign(1.r) = 1.xe_1 \succ \mathcal{S}ign(xu) = xye_2$.

De la même façon qu'on avait définit les *S-polynômes* au chapitre II, nous allons définir les *S-polynômes signés* d'une paire critique de polynômes signés.

Définition 4.4.2. Soient r_f et r_g deux polynômes signés dont la paire critique est (t, u, r_f, v, r_g) telle que $poly(r_f)$ et $poly(r_g)$ sont unitaires. On appelle *S-polynôme signé* de la paire critique (r_f, r_g) (dans cet ordre), le polynôme signé noté $S(r_f, r_g)$ défini par $S(r_f, r_g) = ur_f - vr_g$.

Exemple 22. Dans l'exemple précédent on a :

1. $S(r,s) = yr - xs = (xye_1, x^2y + xy^2) - (xe_1, x^2y - x^2) = (xye_1, xy^2 + x^2)$.
2. $S(u,r) = r - xu = (xe_1, x^2 + xy) - (xye_2, x^2 + 2xy) = (xe_1, -xy)$

4.5 Le critère de réécriture

Le critère de *réécriture* permet d'éliminer les calculs inutiles, générés par certaines paires critiques de polynômes signés, durant l'exécution de l'algorithme F5. Son principe consiste à garder en mémoire la trace des signatures des *S-polynômes* générés dans le temps pour pouvoir les comparer les unes aux autres. C'est donc plus semblable à une technique de programmation dont le but est de réutiliser au maximum les calculs antérieurs.

Définition 4.5.1. Soient $r_f = (x^\alpha e_i, f) \in \mathcal{L}$ et $\mathcal{B}$ un sous ensemble fini de $\mathcal{L}$. On dit que r_f est *réécrivable dans* $\mathcal{B}$ s'il existe un polynôme signé $r_g = (x^\beta e_i, g) \in \mathcal{B}$ tel que :

(i) x^β *divise* x^α.

(ii) r_g est généré par l'algorithme F5 après r_f.

Remarque 4.5.2. Par abus de langage, on écrit $x^\beta e_i$ *divise* $x^\alpha e_i$ si x^β *divise* x^α.

Définition 4.5.3. (Critère de réécriture). Soit $(r_f, r_g) = (t, u, r_f, v, r_g)$ une paire critique de polynômes signés dans R^m et $\mathcal{B}$ un sous ensemble fini de $\mathcal{L}$. On dit que la paire critique (r_f, r_g) satisfait le *critère de réécriture* dans $\mathcal{B}$ si l'un des deux polynômes signés ur_f ou vr_g est *réécrivable* dans $\mathcal{B}$.

Remarque 4.5.4. Pour le calcul d'une base de Gröbner d'un idéal $\langle f_1, \cdots, f_m \rangle$, l'algorithme initialise les signatures des polynômes $f_1, \cdots, f_m$ respectivement à $e_1, \cdots, e_m$. Pour cela, on construit en mémoire un tableau de règles de simplification appelé *Rule* à m entrées correspondants chacune à un vecteur $(e_i)_{i=1\cdots m}$ de la base standard de R^m. À chaque polynôme signé $r_k = (te_i, f_k)$ on ajoute à la $i^{ème}$ entrée de ce tableau le couple (t, k) ce qui permet à tout moment de vérifier si un certain polynôme signé satisfait le critère de réécriture.

Au départ, il n'y a aucune règle de simplification alors on a la procédure suivante pour l'initialisation de la table *Rule* :

Algorithm 6 Reset Simplification Rules.

Entrée : m Le nombre de polynômes en entrée de l'algorithme principal.
pour $i = 1$ à m **faire**
    $Rule[i] = \emptyset$
fin pour

Chaque fois qu'on rencontre une nouvelle règle de simplification, on met à jour

la table *Rule* en ajoutant la nouvelle règle à l'entrée correspondante à l'indice du vecteur de base de la signature du polynôme simplifié selon la procédure suivante :

Algorithm 7 Add Rule.

Entrée : $r_k = (te_i, f_k)$ un polynôme signé dans R^m.
Ajouter le couple (t, k) à la $i^{ème}$ entrée de la table de simplification *Rule*

La procédure de réécriture tente de réécrire un nouveau polynôme signé ur_k en utilisant la table des règles de simplification. Elle renvoie le nouveau polynôme s'il y a lieu de réécriture, sinon elle renvoie le polynôme lui même en sortie :

Algorithm 8 Algorithme Rewritten.

Entrée : $\begin{cases} u : & \text{monôme dans } K[x_1, \cdots, x_n] \\ r_k = (te_i, p) : & \text{polynome signé.} \end{cases}$
Sortie : Un polynôme signé.
$L = Rule[i] = \big([t_1, k_1], \cdots, [t_h, k_h]\big)$
pour $i = 1$ à h **faire**
  si $u.t$ est *divisible* par t_i **alors**
    retourner $\left(\frac{u.t}{t_i}, r_{k_i}\right)$
  fin si
fin pour
  retourner (u, r_k)

Pour vérifier qu'un polynôme signé ur_k est réécrivable, il suffit de comparer son indice à celui du polynôme résultant de la procédure *Rewritten* pour retourner *vrai* s'ils sont différents et *faux* sinon, selon le pseudo code suivant :

Algorithm 9 Algorithme IsRewritten.

Entrée : $\begin{cases} u : & \text{monôme dans } K[x_1, \cdots, x_n] \\ r_k = (te_i, p) : & \text{polynome signé.} \end{cases}$
Sortie : Bouléen.
$(v, r_l) = Rewritten\,\big(u, r_k\big)$
si $l \neq k$ **alors**
  retourner $Vrai$
fin si
  retourner $Faux$

Exemple 23. Dans $\mathbb{F}_2[x, y, z]$ muni de l'ordre lexicographique gradué $x > y > z$ on considère les polynômes $f_1 = x^2 + y^2$ et $f_2 = x^2 + z$ où $\mathbb{F}_2$ est l'anneau $\mathbb{Z}/2\mathbb{Z}$. Soient $r_{f_1} = (e_1, f_1)$ et $r_{f_2} = (e_2, f_2)$ (initialisation des signatures de f_1 et f_2 dans $\mathbb{F}_2[x, y, z]^2$). Alors $S\big(r_{f_1}, r_{f_2}\big) = \big(max\{e_1, e_2\}, f_1 - f_2\big) = \big(e_1, y^2 - z\big)$.

Posons $f_3 = y^2 - z$ et $r_{f_3} = \big(e_1, y^2 - z\big)$. On a alors la paire critique de r_{f_3} et r_{f_1} dans cet ordre est $\big(x^2y^2, x^2, r_{f_3}, y^2, r_{f_1}\big)$. On remarque que $y^2 r_{f_1}$ est réécrivable par $\big\{r_{f_3}\big\}$ car $\mathcal{S}ign\big(r_{f_3}\big) = e_1$ divise $y^2.\mathcal{S}ign\big(r_{f_1}\big) = y^2 e_1$ et r_{f_3} est généré après r_{f_1}. Ce qui signifie qu'il n'est pas nécessaire de calculer $S\big(r_{f_3}, r_{f_1}\big)$. En effet, on a clairement $S\big(f_1, f_2\big) = f_1 - f_2 = y^2 - z = f_3$, $S\big(f_3, f_1\big) = x^2 f_3 - y^2 f_1 = -y^4 - x^2 z$ et en appliquant l'algorithme de division on trouve $-y^4 - x^2 z = -y^2 f_3 - z f_1$ d'où $\overline{S\big(f_1, f_3\big)}^{\{f_1, f_2, f_3\}} = 0$. D'où par Buchberger, cette paire critique est inutile.

4.6 Le critère F5

Le critère F5 est basé sur une propriété des paires critiques de polynômes signés. Il permet d'éliminer une certaine classe des *S-polynômes signés* qui génèrent des calculs inutiles dans le processus de calcul de la base de Gröbner.

Définition 4.6.1. (Polynômes signés *non normalisés*) Soit $r_f = (x^\alpha e_i, f) \in \mathcal{L}$ et $\mathcal{B}$ un sous ensemble fini de $\mathcal{L}$. On dit que r_f est *non normalisé* par $\mathcal{B}$ s'il existe un polynôme signé $r_g = (x^\beta e_j, g) \in \mathcal{B}$ qui vérifie les deux conditions suivantes :

(i) $LM(g)$ *divise* x^α

(ii) $j > i$

Dans ce cas, on dit aussi que x^α est *top réductible* dans $\langle f_{i+1}, \cdots, f_m\rangle$.

Définition 4.6.2. (Critère F5) Soit $\mathcal{B}$ un sous ensemble fini de polynômes signés dans R^m. On dit que la paire critique (t, u, r_f, v, r_g) satisfait le critère F5 dans $\mathcal{B}$ si l'un des deux polynômes signés ur_f ou vr_g est *non normalisé* par $\mathcal{B}$.

Exemple 24. Dans $\mathbb{Q}[x, y, z]$ muni de l'ordre lexicographique gradué inverse avec $x > y > z$ on considère les polynômes $f_1 = x^2 + y$ et $f_2 = xy - z$.

Soient $r_{f_1} = (e_1, f_1)$ et $r_{f_2} = (e_2, f_2)$ (initialisation des signatures de f_1 et f_2 dans $\mathbb{Q}[x, y, z]^2$). Alors $S\big(r_{f_2}, r_{f_1}\big) = x(e_2, xy - z) - y(e_1, x^2 + y) = (ye_1, -xz - y^2)$.

Posons $f_3 = -xz - y^2$ avec $r_{f_3} = \big(ye_1, -y^2 - xz\big)$. On a alors

$$S\big(r_{f_3}, r_{f_2}\big) = x(ye_1, -y^2 - xz) + y(e_2, xy - z) = \big(xye_1, -x^2z - yz\big).$$

On remarque que $LM(f_2) = xy$ *divise* xy tel que $\mathcal{S}ign(xr_{f_3}) = xye_1$ et que $\mathcal{S}ign(r_{f_2}) = e_2$. Alors par définition, le polynôme signé xr_{f_3} est *non normalisé* dans l'ensemble des polynômes signés contenant r_{f_2}. Par conséquent, la paire critique $\big(r_{f_3}, r_{f_2}\big)$ répond au critère F5.

Avant d'énoncer le théorème principal sur lequel est basé l'algorithme F5, nous avons besoin des définitions suivantes :

Définition 4.6.3. Un polynôme signé $\big(ue_k, f\big)$ est dit *admissible* s'il existe un vecteur de polynômes $g \in v^{-1}(f)$ tel que $LT(g) = ue_k$ où v est le morphisme d'évaluation.

Définition 4.6.4. Soient P un sous ensemble fini de $\mathcal{L}$ et $r, t \in \mathcal{L}$ tel que $poly(r) = f \neq 0$. On dit que r admet une *t-représentation* sous P si

(i) $f = \sum_{p_i \in P} h_i.poly(p_i)$ où $h_i \in K[x_1, \cdots, x_n]$.

(ii) Pour tout $p_i \in P$ tel que $poly(p_i) \neq 0$ on a :

$$LM(t) > LM(h_i).LM(p_i) \text{ et } \mathcal{S}ign(r) \succ LM(h_i).\mathcal{S}ign(p_i).$$

On écrit alors $r = \mathcal{O}_P(t)$.

De plus, s'il existe $t^{'} \in \mathcal{L}$ tel que $\mathcal{S}ign(t) \succ \mathcal{S}ign(t^{'})$ et $LM(t) > LM(t^{'})$ tel que $r = \mathcal{O}_P(t^{'})$ alors on écrit $r = o_P(t)$.

Théorème 4.6.5. (Faugère, 2002) Soit $F = \{f_1, \cdots, f_m\}$ une liste finie de polynômes dans R et $G = \{r_1, \cdots, r_{n_G}\}$ une liste finie de polynômes signés dans R^m. Si les conditions suivantes sont vérifiées :

(i) $F \subseteq G_1 = \{poly(r_i) \text{ pour } r_i \in G\}$.

(ii) Tous les r_i sont admissibles pour $i = 1, \cdots, n_G$.

(iii) Pour tout $1 \leq i < j \leq n_G$ tel que la paire (r_i, r_j) est normalisée par G_1, on a soit $S(r_i, r_j) = 0$ ou $S(r_i, r_j) = o_{G_1}(u_i r_i)$ avec $u_i = \dfrac{ppcm(LM(g_i), LM(g_j))}{LM(r_i)}$.

Alors G_1 est une base de Gröbner pour l'idéal $I = \langle f_1, \cdots, f_m \rangle$.

Démonstration. Voir les la démonstration dans (Faugère, 2002). □

Remarque 4.6.6. Si dans la condition *iii* du théorème 4.6.5 on se restreint aux paires critiques de degré inférieur ou égal à un entier d, alors on obtient une *d-base* de Gröbner pour l'idéal I (une base de Gröbner pour l'idéal des polynômes de I de degré aux plus égale à d).

4.7 Description des algorithmes

Nous avons à présent tous les éléments qui nous permettent d'introduire les pseudos codes de l'algorithme F5.

Commençons par l'algorithme principal (algorithme 10) qui prend en entrée un vecteur de m polynômes $f_1, \cdots, f_m$ et retourne en sortie une base de Gröbner G pour l'idéal $\langle f_1, \cdots, f_m \rangle$:

Algorithm 10 Algorithme principal F5

Entrée : $F = (f_1, \cdots, f_m)$ un vecteur de polynômes.
Sortie : une base de Gröbner G pour l'idéal $\langle f_1, \cdots, f_m \rangle$.
$r_m = (e_m, f_m)$
$G_m = \{r_m\}$
$N = m$
$G = \emptyset$
pour $i = m - 1$ à 1 **faire**
    $G_i = F5\big(i, f_i, G_{i+1}\big)$
fin pour
pour $r \in G_1$ **faire**
    $G = G \cup poly(r)$
fin pour
retourner G

L'algorithme principal 10 fait appel au sous algorithme 11 suivant :

Algorithm 11 Algorithme F5

Entrée : $\begin{cases} i : & \text{entier tel que } 2 \leq i \leq m \\ f_i : & \text{polynôme dans } \{f_2, \cdots, f_m\} \\ G_{i+1} : & \text{sous ensemble fini de polynômes signés dans } R^m \end{cases}$
Sortie : un sous ensemble fini G_i de polynômes signés dans R^m.
$r_i = (e_i, f_i)$
$\psi_{i+1} = \big\{forme\, normale(poly(r)) \text{ pour tout } r \in G_{i+1}\big\}$
$G_i = G_{i+1} \cup \{r_i\}$
$P = \big\{CritPair\big(r_i, r, i, \psi_{i+1}\big) \text{ pour tout } r \in G_{i+1}\big\}$ par ordre décroissant sur le degré.
tant que $P \neq \emptyset$ **faire**
    $d = deg(first(P))$
    $P_d = \big\{p \in P \text{ tel que } deg(p) = d\big\}$
    $P = P \setminus P_d$
    $F = Spol(P_d)$
    $R_d = Reduction(F, G_i, i, \psi_{i+1})$
    pour $r \in R_d$ **faire**
        $P = P \cup \big\{CritPair\big(r, p, i, \psi_{i+1}\big) \text{ pour tout } p \in G_i\big\}$
        $G_i = G_i \cup \{r\}$
    fin pour
    Ordonner P par ordre décroissant sur le degré.
fin tant que
retourner G_i

L'algorithme principal F5 commence par initialiser l'ensemble des polynômes signés admissibles au singleton $G_m = \{(e_m, f_m)\}$. Puis il fait appel à un sous algorithme F5 par le biais d'une boucle principale à $m-1$ itérations allant de $m-1$ à 1 pour construire progressivement (algorithme *incrémental*) les ensembles $G_{m-1}, \cdots, G_1$.

Par le théorème 4.6.5, les ensembles $G'_{m-1}, \cdots, G'_1$ définis par

$$G'_k = \{poly(r) \mid r \in G_k\}$$

sont des bases de Gröbner respectives pour les idéaux $\langle f_{m-1}, f_m\rangle$, $\langle f_{m-2}, f_{m-1}, f_m\rangle$, $\cdots$, $\langle f_1, \cdots, f_m\rangle$.

À l'issue de chaque décrémentation de l'indice i de cette boucle principale, le nouveau polynôme signé $r_i = (e_i, f_i)$ est ajouté à l'ensemble G_{i+1} pour former l'ensemble G_i. Dès lors, l'ensemble des paires critiques P formé à partir de ce nouveau polynôme est construit par la fonction *CritPair* en ne considérant que les paires critiques qui ne satisfont pas le critère F5 selon le pseudo codes suivant :

Algorithm 12 CritPair

Entrée : $\begin{cases} k : & \text{entier} \\ r_1, r_2 : & \text{polynômes signés} \\ \psi : & \text{fonction qui retourne la forme normale d'un polynôme} \end{cases}$

Sortie : paire critique (t, u_1, r_1, u_2, r_2) ou $\emptyset$.

$p_1 = poly(r_1)$
$p_2 = poly(r_2)$
$t = ppcm\big(LM(p_1), LM(p_2)\big)$
$u_1 = \frac{t}{LM(p_1)}$
$u_2 = \frac{t}{LM(p_2)}$
si $u_2.\mathcal{S}ign(r_2) \succ u_1.\mathcal{S}ign(r_1)$ **alors**
    $CritPair(r_2, r_1, k, \psi)$
fin si
$t_1 e_{k_1} = \mathcal{S}ign(r_1)$
$t_2 e_{k_2} = \mathcal{S}ign(r_2)$
si $k_1 > k$ **alors**
    retourner $\emptyset$
fin si
si *forme normale*$\big(u_1.t_1\big) \neq u_1.t_1$ **alors**
    retourner $\emptyset$
fin si
si $k_2 = k$ et *forme normale*$\big(u_2.t_2\big) \neq u_2.t_2$ **alors**
    retourner $\emptyset$
fin si
retourner (t, u_1, r_1, u_2, r_2)

Une fois l'ensemble P de toutes les paires critiques construit, la procédure *Spol* permet de calculer les éléments de l'ensemble F qui correspondent aux *S-polynômes* des paires critiques dans P.

Pour sélectionner les paires en question, l'algorithme F5 adopte une stratégie qui consiste à traiter à la fois toutes les paires critiques de plus petit degré après élimination de celles qui répondent au critère de réécriture (paires inutiles) comme suit :

Algorithm 13 Spol

Entrée : $P = \{p_1, \cdots, p_s\}$ liste finie de paires critiques de polynômes signés.
Sortie : F sous ensemble fini de polynômes signés .
Soit $P_l = \left(t_l, u_l, r_{i_l}, v_l, r_{j_l}\right)$ pour $l = 1 \cdots s$.
$F = \emptyset$
pour $l = 1$ **à** s **faire**
  si *IsRewritten* $\left(u_l, r_{i_l}\right) = faux$ et *IsRewritten* $\left(v_l, r_{j_l}\right) = faux$ **alors**
    $N = N + 1$
    $r_N = \left(u_l.\mathcal{S}ign(r_{i_l}) \ , \ u_l.poly(r_{i_l}) - v_l.poly(r_{j_l})\right)$
    AddRule (r_N)
    $F = F \cup \{r_N\}$
  fin si
fin pour
Ordonner F par ordre croissant sur les signatures.
retourner F

Parmi les éléments de l'ensemble F des polynômes signés, la procédure *Reduction* tente de réduire tous ceux qui répondent au critère F5, car ils vont générer des paire critiques inutiles.

Algorithm 14 Reduction

Entrée :
- $ToDo, G$: deux listes finies de polynômes signés
- ψ : fonction qui retourne la forme normale d'un polynôme
- k : entier

Sortie : *Done* : liste finie de polynômes.
$Done = \emptyset$
tant que $ToDo \neq \emptyset$ **faire**
  $h =$ le plus petit élément de $ToDo$ (par rapport à la signature).
  $ToDo = ToDo \setminus \{h\}$
  $(h_1, ToDo_1) =$ *TopReduction*$(h, G \cup Done, k, \psi)$
  $Done = Done \cup \{h_1\}$
  $ToDo = ToDo \cup ToDo_1$
fin tant que
retourner *Done*

Dans le processus de réduction, après avoir vérifié que la séquence d'entrée est régulière, la fonction *TopReduction* permet de sélectionner tous les polynômes

admissibles normalisés et les ajouter à la nouvelle base.

Algorithm 15 TopReduction.

Entrée :
- r_{k_0} : polynôme signé
- G : liste finie de polynômes signés
- ψ : fonction qui retourne la forme normale d'un polynôme
- k : entier

Sortie : couple d'ensembles de polynômes signés éventuellement vides.

si $poly(r_{k_0}) = 0$ **alors**
  $Erreur$: Le système d'entrée n'est pas régulier.
  retourner $(\emptyset, \emptyset)$
fin si
$r = IsReducible(r_{k_0}, G, k, \psi)$
si $r = \emptyset$ **alors**
  retourner $\left(\frac{1}{LC(r_{k_0})} r_{k_0}, \emptyset\right)$
sinon
  $r_{k_1} = r$
  $u = \frac{LT(r_{k_0})}{LT(r_{k_1})}$
  si $\mathcal{S}ign(r_{k_0}) \succ u.\mathcal{S}ign(r_{k_1})$ **alors**
    $poly(r_{k_0}) = poly(r_{k_0}) - u.poly(rk_1)$
    retourner $(\emptyset, \{r_{k_0}\})$
  sinon
    $N = N + 1$
    $r_N = \left(u.\mathcal{S}ign(r_{k_1}), u.poly(r_{k_1}) - poly(r_{k_0})\right)$
    $AddRule\ (r_N)$
    retourner $(\emptyset, \{r_N, r_{k_0}\})$
  fin si
fin si

Pour implémenter cette fonction, on a besoin du résultat de la réduction d'un polynôme signé par la liste des polynômes de la nouvelle base. Tel est le rôle de la fonction *IsReducible* qui retourne exactement le polynôme sous sa forme réduite (si celui ci est réductible) ou simplement l'ensemble vide (s'il est irréductible).

Algorithm 16 IsReducible

Entrée : $\begin{cases} r_{i_0} : & \text{polynôme signé} \\ G = [r_{i_1}, \cdots, r_{i_d}] : & \text{liste finie de polynômes signés} \\ fonction\psi : & \text{retourne la forme normale d'un polynôme} \\ k : & \text{entier} \end{cases}$

Sortie : polynôme signé ou ensemble vide.

$t_j e_{k_j} = \mathcal{S}ign(r_{i_j})$ pour tout $r_{i_j} \in G$

$t_0 e_{k_0} = \mathcal{S}ign(r_{i_0})$

pour $j = 1$ à d **faire**

  si *toutes les conditions suivantes sont vérifiées :*

    (1) $u = \frac{LM(ri_0)}{LM(r_{i_j})} \in \mathcal{M}on(R)$

    (2) $\psi(ut_j) = ut_j$

    (3) $IsRewritten\ (u, r_{i_j}) = faux$

    (4) $ut_j e_{k_j} \neq t_0 e_{k_0}$

  alors retourner r_{i_j}

fin pour

retourner $\emptyset$

Pour illustrer le fonctionnement de l'algorithme F5, nous allons le dérouler en pas à pas sur l'exemple 25 tiré de l'article (Faugère, 2002).

Exemple 25. Dans l'anneau des polynômes $\mathbb{Q}[x, y, z, t]$ muni de l'ordre lexicographique gradué inverse avec $x > y > z > t$, considérons l'idéal $I = \langle f_1, f_2, f_3 \rangle$ avec $f_1 = yz^3 - x^2t^2$, $f_2 = xz^2 - y^2t$ et $f_3 = x^2y - z^2t$.

Pour calculer une base de Gröbner pour l'idéal I, l'algorithme F5 initialise la table des règles de simplification à vide $Rule[1] = Rule[2] = Rule[3] = \emptyset$, la valeur globale N à 3 et l'ensemble G_3 à $\{r_3\}$ où $r_3 = (e_3, f_3)$.

L'appel F5$(2, f_2, G_3)$ ajoute le polynôme signé $r_2 = (e_2, f_2)$ à G_3 pour construire l'ensemble $G_2 = \{r_3, r_2\}$ puis construit l'ensemble des paires critiques

$$P = \big\{(r_2, r_3)\big\} = \big\{(x^2yz^2, xy, r_2, z^2, r_3)\big\}.$$

L'ensemble P contient une seule paire de degré 5 alors $d = 5$.

On pose $P_5 = \big\{(x^2yz^2, xy, r_2, z^2, r_3)\big\}$ alors $P = \emptyset$.

$F = Spol(P_5) = \big\{r_4 = (xye_2, xy^3t - z^4t)\big\}$ (on choisit le polynôme unitaire selon la définition 4.4.2).

La variable N est incrémentée à 5 et la règle de simplification $(xy, 4)$ est ajoutée à la table $Rule[2]$.

La réduction de l'ensemble F par G_2 donne l'ensemble $R_5 = \{r_4\}$.

Mettons à jour $G_2 = \{r_3, r_2, r_4\}$ et construisons les nouvelles paires critiques

$$P = \big\{(r_4, r_2), (r_4, r_3)\big\}.$$

Comme la paire (r_4, r_3) répond au critère F5 alors elle est éliminée donc

$$P = \big\{(r_4, r_2)\big\} = \big\{(xy^3tz^2, z^2, r_4, y^3, r_2\big\}.$$

On a alors $d = 7$, $P_7 = \big\{(xy^3tz^2, z^2, r_4, y^3, r_2\big\}$ et $P = \emptyset$.

$F = Spol(P_7) = \big\{r_5 = (xyz^2e_2, z^6t + y^5t^2)\big\}$ et $N = 5$.

La réduction de r_5 par G_2 donne $R_7 = \big\{r_5 = (xyz^2e_2, z^6t + y^5t^2)\big\}$.

On met à jour $G_2 = \{r_3, r_2, r_4, r_5\}$ et on construit les nouvelles paires critiques : $P = \big\{(r_5, r_2), (r_5, r_3), (r_5, r_4)\big\}$. Il se trouve que toutes les paires répondent aux critère F5 donc elles sont inutiles.

À cette étape de l'algorithme, on a construit une base de Gröbner G_2 pour l'idéal $\langle f_2, f_3\rangle$. Il nous reste l'appel $F5(1, f_1, G_2)$ pour construire G_1 qui est une base de Gröbner pour l'idéal $\langle f_1, f_2, f_3\rangle$.

On ajoute $r_1 = (e_1, f_1)$ et on met à jour l'ensemble $G_1 = \{r_3, r_2, r_4, r_5, r_1\}$.

L'ensemble des nouvelles paires critiques est :

$$P = \big\{p_7 = (r_1, r_2), p_8 = (r_1, r_3), p_9 = (r_1, r_5), p_{10} = (r_1, r_4)\big\}.$$

La paire de plus petit degré est $p_7 = (xyz^3, x, r_1, yz, r_2)$ alors

$$d = deg(p_7) = 5,\ P_5 = \{p_7\},\ P = \{p_8, p_9, p_{10}\}.$$

$$F = Spol(P_7) = \big\{r_6 = (xe_1, y^3zt - x^3t^2)\big\}.$$

On ajoute la règle de simplification $(x, 6)$ à la table $Rule[1]$.

La réduction de P_5 par G_1 donne $R_5 = \{r_6\}$.

On met à jour les ensembles :

$$G_1 = \{r_3, r_2, r_4, r_5, r_1, r_6\}.$$

$$P = \big\{p_8, p_9, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}\big\}.$$

avec $p_{11} = (r_1, r_6)$, $p_{12} = (r_5, r_6)$, $p_{13} = (r_4, r_6)$, $p_{14} = (r_3, r_6)$, $p_{15} = (r_2, r_6)$. Comme les paires p_{11} et p_{12} répondent au critère F5 alors elles sont éliminées.

On a alors $P = \big\{p_8, p_9, p_{10}, p_{13}, p_{14}, p_{15}\big\}$.

$deg(p_8) = 6$ alors $d = 6$, $P_6 = \big\{p_8, p_{13}\big\}$ et $P = \big\{p_9, p_{10}, p_{14}, p_{15}\big\}$.

$F = Spol(P_6) = \big\{r_7 = (x^2e_1, z^5t - x^4t^2)\big\}$ et $N = 7$.

On ajoute la règle de simplification $(x^2, 7)$ à la table $Rule[1]$.

Comme r_7 n'est pas réductible par G_1 alors $R_6 = \{r_7\}$.

On met à jour les ensembles

$$G_1 = \{r_3, r_2, r_4, r_5, r_1, r_6, r_7\}.$$

$$P = \big\{p_9, p_{10}, p_{14}, p_{15}, p_{16} = (r_7, r_5), p_{17} = (r_7, r_2)\big\},$$

car les autres paires $(r_7, r_3), (r_7, r_4), (r_7, r_1)$ et (r_7, r_6) répondent au critère F5.

Le plus petit degré est 7 alors $d = 7$, $P_7 = \big\{p_{14}, p_{15}, p_{16}, p_{17}\big\}$ et $P = \big\{p_9, p_{10}\big\}$.

Les paires p_{14} et p_{15} répondent au critère de réécriture et les paires p_{16} et p_{17} génèrent les polynômes $r_8 = (zx^2e_1, y^5t^2 - x^4zt^2)$ et $r_9 = (x^3e_1, x^5t^2 - y^2z^3t^2)$.

On a alors $N = 9$ et $F = \big\{r_8, r_9\big\}$.

On ajoute les règles de simplification $(zx^2, 8)$ et $(x^3, 9)$ à la table $Rule[1]$.

Comme F n'est pas réductible par G_1 alors $R_7 = \big\{r_8, r_9\big\}$.

On met à jour les ensembles

$$G_1 = \{r_3, r_2, r_4, r_5, r_1, r_6, r_7, r_8, r_9\}.$$

$$P = \big\{p_9, p_{10}, p_{18} = (r_8, r_4), p_{19} = (r_8, r_3)\big\}.$$

les autres paires sont inutiles car elles répondent au critère F5.

On a alors : $d = 8$, $P = \big\{p_{19}\big\}$ et $P_8 = \big\{p_9, p_{10}, p_{18}\big\}$.

Les paires p_{10} et p_{18} répondent au critère de réécriture et p_9 génère le polynôme $r_{10} = (z^3te_1, y^6t^2 - x^2z^3t^3)$.

$F = Spol(P_8) = \big\{r_{10}\big\}$ et $N = 10$.

On ajoute la règle de simplification $(z^3t, 10)$ à la table $Rule[1]$.

Comme r_{10} n'est pas réductible par G_1 alors $R_8 = \{r_{10}\}$.

On met à jour les ensembles $G_1 = \{r_3, r_2, r_4, r_5, r_1, r_6, r_7, r_8, r_9, r_{10}\}$ et $P = \{p_{19}\}$ car les nouvelles paires $(r_10, r_j)_{1 \leq j \leq 9}$ répondent toutes au critère F5.

On a alors $d = deg(p_{19}) = 9$ et $P_9 = \{p_{19}\}$ et $P = \emptyset$.

$F = Spol(P_9) = \emptyset$ car p_{19} répond au critère de réécriture et donc $R_9 = \emptyset$ et l'algorithme s'arrête avec $G_1 = \{r_3, r_2, r_4, r_5, r_1, r_6, r_7, r_8, r_9, r_{10}\}$. Donc une base de Gröbner non réduite pour l'idéal $\langle f_1, f_2, f_3 \rangle$ est :

$$G = \{x^2y - z^2t, xz^2 - y^2t, xy^3t - z^4t, z^6t - y^5t^2, yz^3 - x^2t^2, y^3zt - x^3t^2,$$
$$z^5t - x^4t^2, y^5t^2 - x^4zt^2, x^5t^2 - y^2z^3t^2, y^6t^2 - x^2z^3t^3\}.$$

4.8 Amélioration et preuve de terminaison de l'algorithme F5

Dans son article original (Faugère, 2002), l'auteur n'a pas donné une preuve complète de la terminaison de l'algorithme F5. De plus, l'esquisse de la preuve présentée était conditionnée par une séquence régulière de polynômes homogènes en entrée de l'algorithme. Cette question resta alors ouverte pendant des années pour être l'objet de plusieurs publications donnant naissance à de nouvelles versions de l'algorithme F5 pour assurer sa terminaison. Le tableau ci dessous, tiré de (Eder et Faugère, 2017), résume les versions de l'algorithme F5 apparues dans l'ordre chronologique jusqu'en 2014, date à laquelle Galkin a montré dans (Galkin, 2014) l'exactitude de l'algorithme F5 pour n'importe quelle séquence de polynômes en entrée. De plus, il a donné une preuve détaillée de sa terminaison en apportant des modifications à l'algorithme original de Faugère.

Nom de l'algorithme	Référence
F5	Faugère (2002)
F5/2	Faugère and Joux (2003)
F5B	Ars (2005)
F5B	Stegers (2007)
F5t	Gash (2008, 2009)
F5C	Eder et Perry (2010)
F5A	Eder and Perry (2011)
F5+	Eder et al.(2011)
iF5A	Eder (2013)

CHAPITRE V

APPLICATIONS DES BASES DE GRÖBNER

Dans ce chapitre nous allons présenter quelques applications directes des bases de Gröbner dans la résolution de problèmes de différents domaines.

5.1 Résolution d'un système d'équations polynômiales

Grand nombre de problèmes dans divers domaines (géométrie, robotique, biochimie, cryptographie, théorie des graphes ...) se modélisent en systèmes d'équations polynomiales à plusieurs variables de la forme :

$$(I)\begin{cases} f_1(x_1,\cdots,x_n)=0 \\ f_2(x_1,\cdots,x_n)=0 \\ \vdots \\ f_m(x_1,\cdots,x_n)=0 \end{cases}$$

où $f_1,\cdots,f_m \in K[x_1,\cdots,x_n]$.

Le problème donc est de chercher les solutions du système (I) dans un domaine précis selon l'application.

L'une des méthodes de résolution efficace de ce système consiste a utiliser les bases de Gröbner. En effet, si le système (I) admet $(a_1,\cdots,a_n)$ comme solution, alors

tout polynôme f de la forme $f = \sum_{i=1}^{m} g_i f_i$ avec $g_i \in K[x_1, \cdots, x_n]$ s'annule aussi en $(a_1, \cdots, a_n)$. L'ensemble de ces polynômes forment alors un idéal polynomial comme on le verra dans la suite.

Définition 5.1.1. Soient $f_1, \cdots, f_m \in K[x_1, \cdots, x_n]$. L'ensemble $\big\{(a_1, \cdots, a_n) \in K^n$ tel que $f_i(a_1, \cdots, a_n) = 0 \ \forall \ i = 1 \cdots m\big\}$ est appelé une *variété affine* définie par les polynômes $f_1, \cdots, f_m$ sur le domaine K. Elle est notée $V_K(f_1 \cdots f_m)$.

Inversement, un sous ensemble $V \subset K^n$ est dit une variété affine sur K si $V = V_K(f_1 \cdots f_m)$ pour une certaine liste de polynômes $f_1, \cdots, f_m \in K[x_1, \cdots, x_n]$.

Exemple 26. (i) Dans $\mathbb{R}^2$, $V(x^2 + y^2 - 2)$ est l'ensemble des points du cercle de rayon $\sqrt{2}$ et dont le centre est l'origine $O(0, 0)$.

(ii) Dans $\mathbb{R}^2$, $V(x^2 - 1, x - y)$ est l'ensemble constitué des deux points

$$\big\{(1, 1), (-1, -1)\big\}.$$

Théorème 5.1.2. (*Théorème des zéros de Hilbert*) Soit K un corps et $\overline{K}$ sa clôture algébrique. Si $I = \langle f_1, \cdots, f_m \rangle$ est un idéal de polynômes dans $K[x_1, \cdots, x_n]$ alors

$$V_{\overline{K}}(I) = \emptyset \iff I = \langle 1 \rangle = K[x_1, \cdots, x_n]$$

Pour appliquer ce théorème au système (I), il suffit de calculer $G = \{g_1, \cdots, g_t\}$ une base de Gröbner pour l'idéal $I = \langle f_1, \cdots, f_s \rangle$ suivant l'ordre lexicographique $x_1 > x_2 > \cdots > x_n$. On a alors le système (I) admet au moins une solution dans K^n si et seulement si $G \neq \{1\}$.

Exemple 27. Soit à résoudre dans $\mathbb{R}^3$ le système suivant :

$$(1)\begin{cases} x^2+y^2+z^2-2=0 \\ x^2+3y^2-2=0 \\ 2xy-1=0 \end{cases}$$

Posons $\begin{cases} f_1(x,y,z)=x^2+y^2+z^2-2 \\ f_2(x,y,z)=x^2+3y^2-2 \\ f_3(x,y,z)=2xy-1 \end{cases}$

Utilisons *SageMath* pour calculer une base de Goebner G pour l'idéal

$I=\langle f_1,f_2,f_3\rangle$ suivant l'ordre lexicographique $x>y>z$:

```
In [1]: R=PolynomialRing(QQ,'x,y,z',order="lex")

        R.inject_variables()

Out[1]: Defining x, y, z

In [3]: gens=(x^2+y^2+z^2-2,x^2+3*y^2-2,2*x*y-1)
        I=R.ideal(gens)
        I.groebner_basis()

Out[3]: [x + 3*y*z^2 - 4*y, y^2 - 1/2*z^2, z^4 - 4/3*z^2 + 1/3]
```

On a alors $G=\{g_1,g_2,g_3\}$ avec $g_1=x+3yz^2-4y$, $g_2=y^2-\frac{1}{2}z^2$ et $g_3=z^4-\frac{4}{3}z^2+\frac{1}{3}$.

Comme $G\neq\{1\}$ alors le système (1) admet au moins une solution. Pour calculer ces solutions, il suffit de résoudre l'équation $g_3(z)=0$ puis de remplacer z dans l'équation $g_2(y,z)=0$ pour avoir les valeurs de y et enfin remplacer z et y dans l'équation $g_1(x,y,z)=0$ pour avoir les valeurs de x comme suit :

$$g_3(z)=0 \iff z\in\left\{1,-1,\tfrac{1}{3},\tfrac{-1}{3}\right\}$$

En substituant les valeurs de z dans l'équation $g_2(y,z)=0$ on obtient

$$(y,z) \in \left\{ \left(\pm\tfrac{1}{\sqrt{2}}, \pm 1 \right), \left(\pm\tfrac{1}{3\sqrt{2}}, \pm\tfrac{1}{3} \right) \right\}.$$

En substituant les valeurs de (y,z) dans l'équation $g_1(x,y,z)=0$ on obtient :

$$(x,y,z) \in \left\{ (\tfrac{5}{2}, 1, \pm\tfrac{1}{\sqrt{2}}), (-\tfrac{5}{2}, -1, \pm\tfrac{1}{\sqrt{2}}), (\tfrac{23}{18}, \tfrac{1}{3}, \pm\tfrac{1}{3\sqrt{2}}), (-\tfrac{23}{18}, \tfrac{-1}{3}, \pm\tfrac{1}{3\sqrt{2}}) \right\}.$$

5.2 Le problème *n-racines cyclique*

Le problème *n-racines cyclique* ou *n-cyclique* est l'un des systèmes de référence les plus connus dans les solveurs des systèmes polynomiaux. Il consiste à résoudre les systèmes d'équations polynomiales de la forme :

$$(C_n) \begin{cases} e_1(x_1, \cdots, x_n) = 0 \\ e_2(x_1, \cdots, x_n) = 0 \\ \vdots \\ e_n(x_1, \ldots, x_n) = 1 \end{cases}$$

où les $e_i(x_1, \cdots, x_n)$ désignent les polynômes *symétriques élémentaires* dans l'anneau des polynômes $K[x_1, \cdots, x_n]$.

L'une des approches efficace pour résoudre le système (C_n), est l'utilisation des bases de Gröbner. En particulier l'algorithme F5 qui réduit le temps de calcul de la base de Gröbner vu que les polynômes symétriques élémentaires forment une séquence régulière de polynômes homogènes ce qui élimine toutes les paires critiques inutiles dans le processus de calcul de la base de Gröbner.

Exemple 28. Soit à résoudre le système *3-cyclique* suivant :

$$(C_3)\begin{cases} e_1(x_1,x_2,x_3) = x_1+x_2+x_3 = 0 \\ e_2(x_1,x_2,x_3) = x_1x_2+x_1x_3+x_2x_3 = 0 \\ e_3(x_1,x_2,x_3) = x_1x_2x_3 = 1 \end{cases}$$

Utilisons *SageMath* pour calculer une base de Gröbner pour l'idéal $I = \langle e_1, e_2, e_3 - 1\rangle$ selon le code suivant :

```
In [3]: R=PolynomialRing(QQ,'x1,x2,x3',order="lex")

        R.inject_variables()
Out[3]: Defining x1, x2, x3

In [4]: gens=(x1+x2+x3,x1*x2+x1*x3+x2*x3,x1*x2*x3-1)
        I=R.ideal(gens)
        I.groebner_basis()
Out[4]: [x1 + x2 + x3, x2^2 + x2*x3 + x3^2, x3^3 - 1]
```

Après résolution de l'équation $x_3^3 - 1 = 0$ et la séquence des substitutions on obtient les solutions :

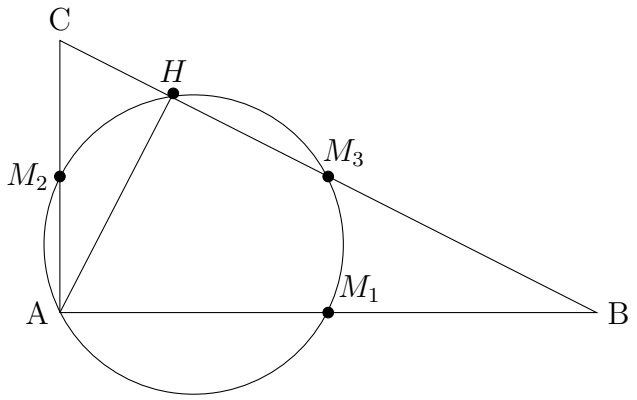
$$\left\{x_1 = e^{\frac{2}{3}i\pi(k+2j)}, x_2 = e^{\frac{2}{3}i\pi(k+j)}, x_3 = e^{\frac{2}{3}i\pi k}\right\} \quad avec\ k = 0,1,2\ et\ j = 1,2$$

5.3 Démonstrateur du théorème du cercle d'Apollonius

La base de Gröbner vue comme un nouvel objet mathématique est un outil puissant dans le développement des démonstrateurs automatiques des théorèmes de la géométrie. Le principe est de formuler les hypothèses du théorème à démontrer en un ensemble fini de polynômes à plusieurs variables $f_1, \cdots, f_m$ et la conclusion en un polynôme g puis de montrer que $g \in \langle f_1, \cdots, f_m\rangle$ qui signifie simplement que la conclusion est une conséquence des hypothèses.

Exemple 29. Soit a démontrer le théorème suivant :

Théorème 5.3.1. (*Le cercle d'Apollonius*) Soit ABC un triangle droit en A. Alors les médianes des trois cotés du triangle et la projection orthogonale de A sur le coté $[CB]$ appartiennent au même cercle.



Posons les coordonnées $A(0,0)$, $B(u_1,0)$ et $C(0,u_2)$ avec u_1 et u_2 des réels arbitraires. Notons par M_1, M_2 et M_3 les médianes des cotés respectifs $[AB]$, $[AC]$ et $[BC]$.

Posons $M_1(x_1,0)$, $M_2(0,x_2)$ et $M_3(x_3,x_4)$. D'où les conditions suivantes :

(i) $h_1 = 2x_1 - u_1 = 0$ du fait que $AM_1 = BM_1$.

(ii) $h_2 = 2x_2 - u_2 = 0$ du fait que $AM_2 = CM_2$.

(iii) $h_3 = 2x_3 - u_1 = 0$ et $h_4 = 2x_4 - u_2 = 0$ du fait que $BM_3 = CM_3$.

Posons $H(x_5,x_6)$. Comme (AH) est perpendiculaire à (BC) alors

$$h_5 = x_5u_1 - x_6u_2 = 0$$

Comme B, C et H sont colinéaires alors $h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0$.

Soit $\omega(x_7,x_8)$ le centre du cercle $\mathcal{T}$ qui passe par les trois médianes M_1, M_2

et M_3. On a alors les relations suivantes :

(i) $\omega M_1 = \omega M_2$ ce qui donne $h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_2 - x_8)^2 = 0$.

(ii) $\omega M_1 = \omega M_3$ ce qui donne $h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0$.

Comme les trois points A, B et C doivent être deux à deux distincts et que le choix des valeurs des variables u_1 et u_2 est arbitraire alors il faut ajouter les conditions $u_1 \neq 0$ et $u_2 \neq 0$. Pour exprimer ces deux conditions, on introduit deux nouvelles variables t_1 et t_2 ce qui nous donne à nouveau les conditions suivantes :

(i) $h_9 = u_1 t_1 = 1$ ce qui signifie que u_1 est inversible.

(ii) $h_{10} = u_2 t_2 = 1$ ce qui signifie que u_2 est inversible.

La conséquence des hypothèse du théorème est $\omega H = \omega M_1$, ce qui se traduit par

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0$$

On a alors les hypothèses du théorème formulées par le système d'équations suivant :

$$(1) \begin{cases} h_1 = 2x_1 - u_1 = 0 \\ h_2 = 2x_2 - u_2 = 0 \\ h_3 = 2x_3 - u_1 = 0 \\ h_4 = 2x_4 - u_2 = 0 \\ h_5 = x_5 u_1 - x_6 u_2 = 0 \\ h_6 = x_5 u_2 + x_6 u_1 - u_1 u_2 = 0 \\ h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_2 - x_8)^2 = 0 \\ h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0 \\ h_9 = u_1 t_1 - 1 = 0 \\ h_{10} = u_2 t_2 - 1 = 0 \end{cases}$$

Il faut donc montrer que la relation $\omega H = \omega M_1$ est une conséquence de ces hypothèses, autrement dit, il faut montrer que $g \in \langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, h_9, h_{10} \rangle$.

Interrogeons *SageMath* pour répondre à cette question par le code suivant :

```
In [1]: R=PolynomialRing(QQ,'u1,u2,t1,t2,x1,x2,x3,x4,x5,x6,x7,x8',order="lex")

        R.inject_variables()

Out[1]: Defining u1, u2, t1, t2, x1, x2, x3, x4, x5, x6, x7, x8

In [3]: gens=(2*x1-u1,2*x2-u2,2*x3-u1,2*x4-u2,x5*u1-x6*u2,
             x5*u2+x6*u1-u1*u2,(x1-x7)^2+x8^2-x7^2-(x2-x8)^2,
             (x1-x7)^2+x8^2-(x3-x7)^2-(x4-x8)^2,u1*t1-1,u2*t2-1)

In [4]: I=R.ideal(gens)

        g=(x5-x7)^2+(x6-x8)^2-(x1-x7)^2-x8^2

        g in I

Out[4]: True
```

5.4 Le problème *k-coloriage* d'un graphe

En théorie des graphes, la coloration d'un graphe non orienté $G = (X, E)$ à n sommets, avec X comme l'ensemble des sommets et E comme l'ensemble des arêtes, consiste à attribuer une couleur à chacun des sommets de G en respectant la condition que pour tout couple de sommets $(u, v) \in X^2$, si u est relié à v par une arête alors les couleurs attribuées aux sommets u et v sont différentes. Ainsi, pour un entier $2 \leq k \leq n$, on se pose la question : existe-t-il une coloration à k couleurs différentes pour le graphe G ?

Une façon de résoudre ce problème est de faire appel aux bases de Gröbner. Pour ce faire, on modélisera le problème sous forme d'idéal polynomial comme suit :

Soit $X = \{x_1, \cdots, x_n\}$ l'ensemble des sommets du graphe G , $\mathcal{C} = \{c_1, \cdots, c_k\}$ un ensemble de k couleurs différents et $\delta = \{\alpha \in \mathbb{C} \text{ tel que } \alpha^k = 1\}$. On définit une bijection de $\mathcal{C}$ dans δ qui associe à chaque couleur $c_i \in \mathcal{C}$ un élément unique $\alpha_i \in \delta$. On traduit l'opération d'attribution d'une couleur c_j à un sommet x par

la fonction c définie comme suit :

$$\begin{aligned} c: \quad & X \longrightarrow \delta \\ & x \longmapsto c(x) = \alpha_j \end{aligned}$$

Soit le polynôme $f(x) = \prod_{i=1}^{k}(x-\alpha_i) = x^k - 1$. Si $x \in X$ alors $f(c(x)) = 0$ signifie clairement que l'une des couleurs $c_1, \cdots, c_k$ est attribuée au sommet x.

Soient deux sommets différents x_i et x_j du graphe G. Si x_i et x_j sont reliés par une arrête, alors les couleurs qui leurs sont attribuées doivent être différentes. Autrement, dit il faut avoir la condition $c(x_i) \neq c(x_j)$.

Or $f(c(x_i)) = f(c(x_j)) = 0$ alors $c(x_i)^k - c(x_j)^k = 0$. Comme $c(x_i) \neq c(x_j)$ alors $\dfrac{c(x_i)^k - c(x_j)^k}{c(x_i) - c(x_j)} = 0$. Ce qui se traduit en terme de polynômes par les équations

$$\frac{f(x_i) - f(x_j)}{x_i - x_j} = 0, \quad \forall (x_i, x_j)_{i<j} \in E$$

Nous avons alors le systèmes d'équations polynomiales suivant :

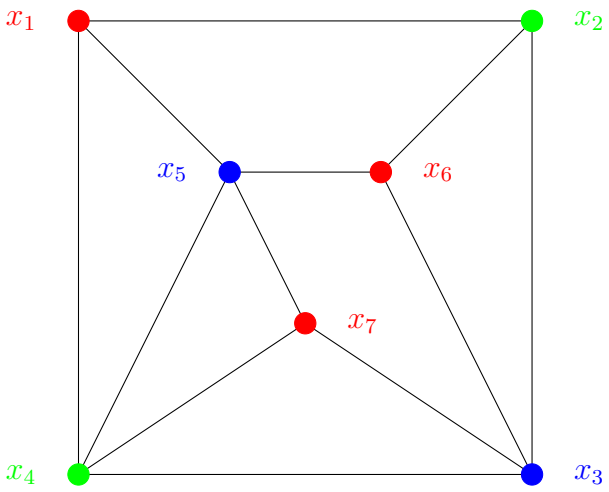
$$(I) \begin{cases} f(x_i) = 0, \quad \forall x_i \in X \\ \dfrac{f(x_i) - f(x_j)}{x_i - x_j} = 0, \quad \forall (x_i, x_j)_{i<j} \in E \end{cases}$$

En remplaçant $f(x_i)$ et $f(x_j)$ par leurs expressions respectives, ont obtient le système

$$(II) \begin{cases} x_i^k - 1 = 0, \quad \forall x_i \in X \\ \dfrac{x_i^k - x_j^k}{x_i - x_j} = 0, \quad \forall (x_i, x_j)_{i<j} \in E \end{cases}$$

En conclusion, le graphe G admet un *k-coloriage* si et seulement si le système (II) admet au moins une solution dans $\mathbb{C}^k$.

Exemple 30. Le graphe G suivant admet un *3-coloriage*.



Montrons ce résultat en utilisant les bases de Gröbner.

Posons $E = \{(x_i, x_j)_{1\leq i<j\leq 7}\}$ l'ensemble des arrêtes du graphe G. On a alors le systèmes d'équations polynomiales

$$(a) \begin{cases} p_i = x_i^3 - 1 = 0, \quad \forall i = 1 \cdots 7 \\ p_{i,j} = \dfrac{x_i^3 - x_j^3}{x_i - x_j} = x_i^2 + x_i x_j + x_j^2 = 0, \quad \forall (x_i, x_j)_{1\leq i<j\leq 7} \in E \end{cases}$$

Posons $P = \big\{(i,j) \in \mathbb{N}^2 \mid (x_i, x_j)_{1\leq i<j\leq 7} \in E\big\}$. Le système (a) est équivalent au système

$$(b) \begin{cases} p_i = x_i^3 - 1 = 0, \quad \forall i = 1 \cdots 7 \\ p_{i,j} = x_i^2 + x_j^2 + x_i x_j = 0 \qquad \forall (i,j) \in P \end{cases}$$

Utilisons *SageMath* pour vérifier que 1 n'est pas un élément de l'idéal polynomial

$$I = \langle p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_{1,2}, p_{1,4}, p_{1,5}, p_{2,3}, p_{2,6}, p_{3,4}, p_{3,6}, p_{3,7}, p_{4,5}, p_{4,7}, p_{5,6}, p_{5,7} \rangle$$

```
In [1]: R=PolynomialRing(QQ,'x1,x2,x3,x4,x5,x6,x7',order="lex")

        R.inject_variables()

Out[1]: Defining x1, x2, x3, x4, x5, x6, x7

In [2]: gens=(x1^3-1,x2^3-1,x3^3-1,x4^3-1,x5^3-1,x6^3-1,x7^3-1,
             x1^2+x2^2+x1*x2,x1^2+x5^2+x1*x5,x1^2+x4^2+x1*x4,
             x6^2+x2^2+x6*x2,x3^2+x2^2+x3*x2,x3^2+x4^2+x3*x4,
             x3^2+x6^2+x3*x6,x3^2+x7^2+x3*x7,x5^2+x7^2+x5*x7,
             x4^2+x5^2+x4*x5,x4^2+x7^2+x4*x7,x5^2+x6^2+x5*x6)
        I=R.ideal(gens)
        1 in I

Out[2]: False
```

Comme $1 \notin I$ alors $H \neq \{1\}$ et donc le système (b) admet au moins une solution. Autrement dit, le graphe G admet un *3-coloriage*.

Pour trouver une façon de colorer le graphe G, il suffit de calculer une solution du système (b) comme suit :

(i) $x_7^3 - 1 = 0$: prenons par exemple $x_7 = 1$.

(ii) $x_6 - x_7 = 0$ alors $x_6 = 1$.

(iii) $x_5^2 + x_5x_7 + x_7^2 = 0$: prenons par exemple $x_5 = e^{i\frac{2\pi}{3}}$.

(iv) $x_4 + x_5 + x_7 = 0$ alors $x_4 = e^{i\frac{4\pi}{3}}$.

(v) $x_3 - x_5 = 0$ alors $x_3 = e^{i\frac{2\pi}{3}}$.

(vi) $x_2 + x_5 + x_7 = 0$ alors $x_2 = e^{i\frac{4\pi}{3}}$.

(vii) $x_1 - x_7 = 0$ alors $x_1 = 1$.

Choisissons, par exemple, la bijection :

$$c(1) = \text{rouge}\,; \quad c\big(e^{i\frac{2\pi}{3}}\big) = \text{bleu}\,; \quad c\big(e^{i\frac{4\pi}{3}}\big) = \text{vert}.$$

On a alors la coloration suivante :

Sommets du graphe	Couleur associée
x_1, x_6, x_7	rouge
x_2, x_4	vert
x_5, x_3	bleu

5.5 La programmation linéaire en nombres entiers

Un problème de programmation linéaire en nombres entiers correspond à un système d'équations et inéquations linéaires (appelées contraintes) dont les inconnues sont à valeurs entières positives ou nulles et les coefficients sont entiers, avec une fonction objective f à optimiser (maximiser ou minimiser).

Nous allons nous intéresser à une classe de problèmes de la programmation linéaire en nombres entiers dont les contraintes sont de la forme $\leq$ et à coefficients positifs avec une fonction objective à minimiser. Après introduction des *variables d'écart* tout problème de cette classe peut s'écrire sous la forme canonique (standard) :

$$(PLE) \begin{cases} min\ f = CX \\ AX = B \end{cases}$$

où $X = (x_1, \cdots, x_n)$ est le vecteur des n inconnues, $C = (c_1, \cdots, c_n) \in \mathbb{Z}^n$, $B = (b_1, \cdots, b_m) \in \mathbb{N}^m$ et A est une matrice de taille $m \times n$ à coefficients dans $\mathbb{N}$.

On dit qu'un vecteur $X \in \mathbb{N}^n$ est une solution *réalisable* pour le système (PLE) si

$$AX = B$$

L'une des approches pour résoudre le système (PLE) est d'utiliser les bases de Gröbner. Pour cela, il faut transformer les contraintes en polynômes en introduisant de nouvelles variables.

Pour chaque équation $a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i$ on introduit une variable z_i telle que

$$z_i^{a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n} = z_i^{b_i}$$

En multipliant toutes les équations coté par coté on obtient une équation de la forme

$$\prod_{j=1}^{n} \left(\prod_{i=1}^{m} z_i^{a_{ij}} \right)^{x_j} = \prod_{i=1}^{m} z_i^{b_i} \qquad (\alpha)$$

Proposition 5.5.1. (Cox *et al.*, 1998) Soit K un corps. On définit le morphisme :

$$\begin{aligned} \phi : \quad K[y_1, \cdots, y_n] &\longrightarrow K[z_1, \cdots, z_m] \\ y_j &\longmapsto \phi(y_j) = \prod_{i=1}^{m} z_i^{a_{ij}} \quad \forall\, j = 1 \cdots n \end{aligned}$$

tel que

$$\forall\, g \in K[y_1, \cdots, y_n],\ \phi\left(g(y_1, \cdots, y_n)\right) = g\left(\phi(y_1), \cdots, \phi(y_n)\right).$$

Alors $(a_1, \cdots, a_n) \in \mathbb{N}^n$ est une solution réalisable pour le système (PLE) si et seulement si

$$\phi\left(y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n}\right) = z_1^{b_1} z_2^{b_2} \cdots z_m^{b_m}.$$

Exemple 31. Soit à résoudre le problème linéaire suivant :

$$(PLE1) \begin{cases} min\ x_1 + 2x_2 + x_3 + 12x_4 \\ 3x_1 + 2x_2 + x_3 + x_4 = 10 \\ 4x_1 + x_2 + x_3 = 5 \end{cases}$$

On introduit les variables z_1 et z_2 telles que

$$\begin{cases} z_1^{3x_1 + 2x_2 + x_3 + x_4} = z_1^{10} \\ z_2^{4x_1 + x_2 + x_3} = z_2^{5} \end{cases}$$

En multipliant les équations coté par coté on obtient l'équation

$$z_1^{3x_1+2x_2+x_3+x_4} \times z_2^{4x_1+x_2+x_3} = z_1^{10} \times z_2^5$$

d'où $(z_1^3 \times z_2^4)^{x_1} \times (z_1^2 \times z_2)^{x_2} \times (z_1 \times z_2)^{x_3} \times (z_1)^{x_4} = z_1^{10} \times z_2^5$.

On définit le morphisme

$$\begin{aligned} \phi : \quad K[y_1, y_2, y_3, y_4] &\longrightarrow K[z_1, z_2] \\ y_1 &\longmapsto \phi(y_1) = z_1^3 z_2^4 \\ y_2 &\longmapsto \phi(y_2) = z_1^2 z_2 \\ y_3 &\longmapsto \phi(y_3) = z_1 z_2 \\ y_4 &\longmapsto \phi(y_4) = z_1 \end{aligned}$$

Par la proposition 5.5.1, $(x_1, \cdots, x_n)$ est une solution réalisable si et seulement si

$$\phi\left(y_1^{x_1} y_1^{x_2} y_1^{x_3} y_1^{x_4}\right) = z_1^{10} z_2^5$$

Proposition 5.5.2. Soient $f_1, \cdots, f_n \in K[z_1, \cdots, z_m]$ et G une base de Gröbner pour l'idéal $I = \langle f_1 - y_1, \cdots, f_n - y_n \rangle$ suivant l'ordre lexicographique $z_1 > \cdots > z_m > y_1 > \cdots > y_n$. Pour chaque $f \in K[z_1, \cdots, z_m]$ on pose $g = \overline{f}^G$. On a alors

$$f \in K[f_1, \cdots, f_n] \iff g \in K[y_1, \cdots, y_n]$$

Démonstration. Voir la preuve dans (Cox *et al.*, 1998) page 365. □

Par la proposition 5.5.2, si $z_1^{b_1} \cdots z_m^{b_m} \in Im(\phi)$ alors

$$\exists (x_1, \cdots, x_n) \in \mathbb{N}^n \quad tel\ que \quad \phi\left(y_1^{x_1} \cdots y_n^{x_n}\right) = z_1^{b_1} \cdots y_n^{b_m}$$

Dans l'exemple précédent on considère l'idéal

$$I = \langle z_1^3 z_2^4 - y_1, z_1^2 z_2 - y_2, z_1 z_2 - y_3, z_1 - y_4 \rangle \in K[z_1, z_2, y_1, y_2, y_3, y_4]$$

Soit $f = z_1^{10} z_2^5$. Utilisons *SageMath* pour calculer $g = \overline{f}^G$ (le reste de la division de f par la base de Gröbner G pour l'idéal I suivant l'ordre lexicographique $z_1 > z_2 > y_1 > y_2 > y_3 > y_4$).

```
In [1]: R=PolynomialRing(QQ,'z1,z2,y1,y2,y3,y4',order="lex")

        R.inject_variables()
Out[1]: Defining z1, z2, y1, y2, y3, y4

In [2]: gens=(z1^3*z2^4-y1,z1^2*z2-y2,z1*z2-y3,z1-y4)
        I=R.ideal(gens)
        I.groebner_basis()
Out[2]: [z1 - y4, z2*y3^3 - y1, z2*y4 - y3, y1*y4 - y3^4, y2 - y3*y4]

In [3]: f=z1^10*z2^5
        f.reduce(I)

Out[3]: y3^5*y4^5
```

Comme $g = y_3^5 y_4^5 \in K[y_1, y_2, y_3, y_4]$ alors $(x_1, x_2, x_3, x_4) = (0, 0, 5, 5)$ est une solution réalisable mais pas forcément optimale, car elle ne prend pas en considération la fonction objective. Pour chercher une solution optimale, il faut définir un nouvel ordre monomial qui dépend de la fonction objective.

Définition 5.5.3. Soit $\succeq$ un ordre monomial dans $K[z_1, \cdots, z_m, y_1, \cdots, y_n]$. On dit que $\succeq$ est *adapté* au système (PLE) s'il vérifie les propriétés suivantes :

(i) Pour tout monôme $\alpha \in K[z_1, \cdots, z_m, y_1, \cdots, y_n]$ contenant un z_i et pour tout monôme $\beta \in K[z_1, \cdots, z_m, y_1, \cdots, y_n]$ contenant uniquement les y_j on a : $\alpha \succeq \beta$.

(ii) Pour tous vecteurs $X_1, X_2 \in \mathbb{N}^n$ on a :

$$\begin{cases} \phi\left(Y^{X_1}\right) = \phi\left(Y^{X_2}\right) \\ CX_1 \geq CX_2 \end{cases} \quad \Longrightarrow \; Y^{X_1} \succeq Y^{X_2}$$

Le théorème suivant permet de trouver une solution optimale pour le système (PLE).

Théorème 5.5.4. Soit un problème de programmation linéaire en nombre entiers sous la forme standard (PLE) avec $f_j = \prod_{i=1}^{m} z_i^{a_{ij}}$ comme définis précédemment. Soit G une base de Gröbner pour l'idéal $I = \langle f_1 - y_1, \cdots, f_n - y_n \rangle \subset K[z_1 \cdots z_m, y_1 \cdots y_n]$ suivant un ordre monomial adapté au système (PLE).

Si $f = z_1^{b_1} \cdots z_m^{b_m} \in K[z_1 \cdots z_m, y_1 \cdots y_n]$ tel que

$$\overline{f}^G = y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n} \in K[y_1, \cdots, y_n]$$

alors $(a_1, a_2, \cdots, a_n)$ est une solution optimale pour le système (PLE).

Démonstration. Voir la preuve dans (Cox *et al.*, 1998) (page 367). □

Reprenons l'exemple précédent et utilisons *SageMath* pour calculer une solution optimale en choisissant un ordre monomial adapté au système $(PLE1)$ selon le code suivant :

```
In [1]: TX=TermOrder('lex',2)
        TY=TermOrder('wdeglex',(1,2,1,12))
        Tc=TX+TY
        R=PolynomialRing(QQ,'z1,z2,y1,y2,y3,y4',order= Tc)
        R.inject_variables()
Out[1]: Defining z1, z2, y1, y2, y3, y4

In [2]: gens=(z1^3*z2^4-y1,z1^2*z2-y2,z1*z2-y3,z1-y4)
        I=R.ideal(gens)
        f=z1^10*z2^5
        f.reduce(I)
Out[2]: y2^5
```

Comme $g = y_2^5 \in K[y_1, y_2, y_3, y_4]$ alors $(x_1, x_2, x_3, x_4) = (0, 5, 0, 0)$ est une solution réalisable et optimale pour le système $(PLE1)$.

CONCLUSION

Depuis son fondement, qui date des années 1960, la théorie des bases de Gröbner ne cesse de susciter l'intérêt de la communauté mathématique pour tenter d'apporter des réponses à des questions ouvertes dans plusieurs domaines, notamment en algèbre computationnelle et en combinatoire algébrique. Ces deux disciplines mathématiques pour lesquelles la théorie des bases de Gröbner joue un rôle crucial, offrent continuellement des perspectives à explorer dans cette direction.

RÉFÉRENCES

Cox, D., Little, J. et O'Shea, D. (1997). *Ideals, varieties, and algorithms* (second éd.). Undergraduate Texts in Mathematics. Springer-Verlag, New York. An introduction to computational algebraic geometry and commutative algebra.

Cox, D., Little, J. et O'Shea, D. (1998). *Using algebraic geometry*, volume 185 de *Graduate Texts in Mathematics*. Springer-Verlag, New York. http://dx.doi.org/10.1007/978-1-4757-6911-1. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1007/978-1-4757-6911-1

Cox, D. A., Little, J. et O'Shea, D. (2015). *Ideals, varieties, and algorithms* (fourth éd.). Undergraduate Texts in Mathematics. Springer, Cham. An introduction to computational algebraic geometry and commutative algebra, http://dx.doi.org/10.1007/978-3-319-16721-3. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1007/978-3-319-16721-3

Eder, C. et Faugère, J.-C. (2017). A survey on signature-based algorithms for computing Gröbner bases. *J. Symbolic Comput.*, *80*(part 3), 719–784. http://dx.doi.org/10.1016/j.jsc.2016.07.031. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1016/j.jsc.2016.07.031

Faugére, J.-C. (1999). A new efficient algorithm for computing Gröbner bases (F_4). volume 139 61–88. Effective methods in algebraic geometry (Saint-Malo, 1998)

Faugère, J.-C. (2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). Dans *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, 75–83. ACM, New York. http://dx.doi.org/10.1145/780506.780516. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1145/780506.780516

Galkin, V. V. (2014). Termination of the F5 algorithm. *Program. Comput. Softw.*, *40*(2), 47–57. Translated from Programmirovanie **4**0 (2014), no. 2, http://dx.doi.org/10.1134/S0361768814020042. Récupéré de https://doi-org.proxy.bibliotheques.uqam.ca/10.1134/S0361768814020042