UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE (EDMI)

Année : 2020 N^o d'ordre : 156

THÈSE DE DOCTORAT UNIQUE

Mention : Mathématiques et Modélisation

Option : Codage, Cryptologie, Algèbre et Applications

Présentée par

Yatma DIOP

Sujet : **Bases de Gröbner-Shirshov sur les anneaux de valuation et Caractérisation de certaines bases de Gröbner non commutatives finies**

Soutenue le 02 novembre 2020 devant le jury :

PRÉSIDENT	Pr. Cheikh Thiécoumba GUÉYE	Université Cheikh Anta Diop de Dakar
RAPPORTEURS	Pr. Edgar MARTINEZ-MORO	Université de Valladolid
	Pr. El Mamoun SOUIDI	Université Mohammed V de Rabat
EXAMINATEURS	Pr. Mamadou BARRY	Université Cheikh Anta Diop de Dakar
	Pr. Mohamed Ben Fraj Ben MAAOUIA	Université Gaston Berger de Saint-Louis
	Pr. Mamadou SANGHARÉ	Université Cheikh Anta Diop de Dakar
DIRECTEURS DE THÈSE	Pr. Djiby SOW	Université Cheikh Anta Diop de Dakar
	Dr. Laila MESMOUDI	Université Cheikh Anta Diop de Dakar

Bases de Gröbner-Shirshov sur les anneaux de valuation et caractérisation de certaines bases de Gröbner non commutatives finies

YATMA DIOP

A la mémoire de ma mère Khar Diop,
de mon ami et collègue Cheikh Sadibou Ba,
Vous me manquez énormément.

Dédicaces

Ce travail est dédié à :

— mes parents : ma défunte mère Khar Diop et mon père Aliou Diop

— à ma tanta Oumou Niasse

— mes frères Oumar Diop, Pape Malick Diop, Doudou Diop, Babacar Diop, Ablaye Diop, Cheikh Tidiane Diop, Mouhamed Diop, Assane Diop et, Ousseynou Diop

— mes sœurs Aida Diop et Ndeye Penda Diop.

Dédicace spéciale à mon épouse, ma bien aimée Aïssatou Konté.

Remerciements

Je remercie ALLAH Le Tout Puissant
Le Clément et Le Miséricordieux

Je remercie sincèrement Professeur Cheikh Thiécoumba Guéye d'avoir accepté de présider mon jury de soutenance de thèse.

Je remercie également les Professeurs Edgar Martinez Moro et El Mamoun Souidi d'avoir accepté la lourde responsabilité de rapporteurs qui leur a été confiée.

Mes remerciemets vont également à l'endroit des Professeurs Mamadou Barry, Mohamed Ben Fraj Ben Maaouia et Mamadou Sangharé d'avoir accepté de sièger à mon jury de thèse entant qu'examinateurs.

Je remercie très chaleureusement mes encadreurs Pr. Djiby SOW et Dr. Laila MESMOUDI. Sans leurs conseils, suggestions, critiques constructives, ouverture, disponibilié et sens d'écoute, ce travail n'aurait jamais abouti. Je vous en serai toujours reconnaissant.

Je remercie également tous les enseignants qui, du primaire à l'université en passant par le collège et le lycée, m'ont tenu dans leurs classes. Du fonds du cœur et où qu'ils soient, je leur dis MERCI pour tout le temps qu'ils ont dépensé pour me faire acquérir des connaissances.

Merci à mon professeur et ami El Hadji Amadou Guéye, un homme ouvvert, serviable, humble et généreux.

J'adresse aussi mes remerciements à mes amis et compagnons Demba Dia, Ismaila Dione, Gilbert Ndolane Dione Aliou Diop, Soda Diop, Habib Fall, Mbaye Fall, Abdoulaye Maïga, Moustapha Biaye Mané, Moussa Mbaye, Mahamadou Sall, Moussa Sall, Bernard Ousmane Sané, Michel Seck, Guy Wamba.

Un grand merci au CEA-MITIC pour son soutien financier m'ayant permis de participer à la conférence "3rd MAMAA" et d'y faire une communication.

Table des matières

Introduction générale

Historique : Au début du $\overline{\text{XX}}^{\text{e}}$ siècle, les anneaux de polynômes à plusieurs indéterminées et à coefficients dans un corps ont été largement étudiés. L'un des problèmes récurrents de l'époque était de savoir "Comment tester l'appartenance d'un polynôme f à un idéal $\mathcal{I}$". Ce problème est communément appelé l'"Ideal Membership Problem" (IMP). Il est bien connu que l'anneau de polynômes en une seule indéterminée est principal et euclidien. Ainsi, le test d'appartenance d'un polynôme f à un idéal $\mathcal{I}$ se réalise en faisant la division euclidienne de f par un polynôme g engendrant $\mathcal{I}$. Or, les anneaux de polynômes à plusieurs indéterminées ne sont ni principaux ni euclidiens ; d'où la difficulté de résoudre l'IMP. Pour étudier les polynômes à plusieurs indéterminées, les chercheurs faisaient alors le parallèle avec les polynômes en une seule indéterminée. Au fil du temps, des avancées importantes ont été obtenues. Les premières de ces avancées remontent aux travaux de Maccaulay, Dickson et Hilbert.

- Maccaulay a montré que l'ensemble $\mathbb{M}$ des monômes de $\mathbb{K}[\mathrm{X}_1, \mathrm{X}_2, ..., \mathrm{X}_\mathrm{n}]$ peut toujours être muni d'un ordre total.
- Dickson a prouvé que tout idéal $\mathcal{I}$ de $\mathbb{K}[\mathrm{X}_1, \mathrm{X}_2, ..., \mathrm{X}_\mathrm{n}]$ engendré par des monômes admet une partie génératrice minimale finie.
- Hilbert a montré que tout idéal $\mathcal{I}$ de $\mathbb{K}[\mathrm{X}_1, \mathrm{X}_2, ..., \mathrm{X}_\mathrm{n}]$ admet une partie génératrice finie.

En dépit de ces avancées, l'IMP est résté non résolu. En 1939, Wolgang Gröbner a publié un papier sur des applications des idées de Maccaulay concernant les ordres totaux sur les monômes. Et plus tard, il proposa à son étudiant en thèse Bruno Buchberger de réfléchir sur la résolution de l'IMP. Dans [13], Buchberger a d'abord conçu un algorithme généralisant la division euclidienne. Cependant, cet algorithme

ne donne pas nécessairement un reste unique ; d'où son inefficacité. Puis, il a établi pour tout idéal donné, l'existence d'une partie génératrice G fixant le reste de la division d'un polynôme f par G. Cette partie génératrice permet alors de résoudre efficacement le problème posé. Elle a été baptisée base de Gröbner par Buchberger en guise de reconnaissance et de remerciements à son direteur de thèse.
Buchberger a également donné un algorithme qui permet de déterminer une base de Gröbner d'un idéal à partir d'une partie génératrice quelconque dont l'existence est garantie par le théorème de la base de Hilbert.

Bien que les travaux de Buchberger sont plus populaires, A. I. Shirshov, un étudiant de l'école russe d'algèbre non associative a développé à la même époque la même théorie sur les algèbres de Lie. Il a cherché à répondre à la question suivante : "Comment déterminer une base linéaire d'une algèbre de Lie définie par des générateurs et des relations ?". Introduisant la notion de composition, il finit par trouver un algorithme généralement infini qui répond tout de même à sa question. Ses travaux (voir [55]) sont plus connus dans les milieux de recherche asiatiques où la théorie est appelée Bases de Gröbner-Shirshov.
Parllèlement, un concept analogue (voir [36]), a été développé en géométrie algébrique par le mathématicien japonais Heisuke Hironaka qui l'a baptisé base standard.

A partir des années 70, les bases de Gröbner ont connu plusieurs généralisations. Dans [5] publié en 1978, Bergman fait la généralisation en algèbre non associative. Puis, les bases de Gröbner non commutatives sur un corps ont été largement étudiées et caractérisées dans [46], [48],... .

Parallèlement, les bases de Gröbner sur un anneau ont été développées. Dans cette généralisation, les auteurs remplacent le corps de base par un anneau. Puis, ils redéfinissent les bases de Gröbner en tenant en compte des particularités de l'anneau considéré. La diversité des anneaux a naturellement fait de cette partie un vaste champ de recherches avec des résultats tout aussi intéressants. Ainsi, en 1988, dans [50], Pan étend la notion de base de Gröbner à des idéaux de polynômes à coefficients dans un anneau principal tandis que Kandry-Rody et Kapur, dans [38], faisaient simultanément un travail similaire sur les idéaux de polynômes à coefficients dans

un anneau euclidien. Plus tard, Kapur et Yongyang publient des résultats de leurs travaux portant sur les bases de Gröbner sur les anneaux admettant des diviseurs de zéro. Voir [40].

Récemment, une nouvelle approche a été proposée par Bokut *et al.* dans [9]. L'idée est de faire passer la structure algébrique des monômes d'un monoïde à un semi-anneau.

En plus d'avoir permis de résoudre l'IMP, les bases de Gröbner ont de nombreuses applications. La résolution des systèmes d'équations non linéaires est l'une des plus importantes de ces applications. En effet, dans les systèmes d'équations non linéaires, les bases de Gröbner donnent un analogue de l'élimination de Gauss utilisée pour résoudre les systèmes linéaires. Or, les systèmes non linéaires sont présents dans plusieurs domaines notamment en cryptologie [14, 15], en théorie des codes correcteurs d'erreurs [16, 42], en optimisation [1], en robotique [28], etc. Ceci explique l'utilisation accrue des bases de Gröbner dans tous ces domaines et motive davantage les recherches. Les bases de Gröbner constituent le principal outil d'analyse de sécurité en cryptographie multivariée qui est l'une des pistes privilégiées pour la cryptographie post-quantique.

Motivations : Des thèses de doctorat dans le domaine des bases de Gröbner ont déjà été soutenues au sein de l'Ecole Doctorale de Mathématiques et Informatique. Dans sa thèse [11] soutenue le 28 février 2014, Bouesso A. S. E. M. a étudié les bases de Gröbner dynamiques. Puis, Nafissatou Diarra a étudié dans sa thèse [22], soutenue le 12 août 2017, les bases de Gröbner sur les D-A-anneaux. C'est dans le cadre de la poursuite de ces travaux de recherche dèjà entamé sur les bases de Gröbner qu'il nous a été proposé de réfléchir sur des problèmes actuels concernant cette théorie notamment :

— l'étude des bases de Gröbner non commutatives finies ;
— la généralisation de la nouvelle approche, encore peu explorée, proposée dans [9] aux anneaux de valuation.

Contributions : Nos investigations nous ont valu deux contributions.

— **Première contribution :** La généralisation des bases de Gröbner aux anneaux de polynômes non commutatifs $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ a entrainé la perte

partielle de la finitude de l'algorithme de Buchberger. Il se pose alors la question de savoir si un idéal non commutatif donné admet une base de Gröbner finie ou non. En 1998, D. Eisenbud, I. Peeva et B. Strumfels publient le papier [27] dans lequel ils résolvent partiellement le problème. Plus précisément, ils ont construit un homomorphisme surjectif γ de l'anneau non commutatif $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ vers l'anneau commutatif $\mathbb{K}[x_1, x_2, ..., x_n]$ des polynômes et ont montré que pour tout idéal $\mathcal{I}$ de $\mathbb{K}[x_1, x_2, ..., x_n]$, l'idéal $\gamma^{-1}(\mathcal{I})$ de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ admet une base de Gröbner finie. Ils ont également donné une méthode de construction d'une base de Gröbner finie de tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ s'exprimant sous la forme précédemment indiquée.
La question inverse nous a alors intéressé. Autrement dit, nous avons cherché à répondre à la question suivante : "soit $\mathcal{J}$ un idéal de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ admettant une base de Gröbner finie, existe-t-il un idéal $\mathcal{I}$ de $\mathbb{K}[x_1, x_2, ..., x_n]$ tel que $\mathcal{J} = \gamma^{-1}(\mathcal{I})$?".
Partis d'une analyse minutieuse des bases de Gröbner construites dans [27], nous avons établi les conditions nécessaires et suffisantes pour que la réponse à la question précédente soit affirmative. Nous avons montré, dans le papier [24] "Diop Y., Sow D. *On finite noncommutative Gröbner bases. Algebra Colloquium* 27 : 3(2020) 381 − 388", que sous certaines conditions, tout idéal non commutatif admettant une base de Gröbner finie s'exprime sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, où $\mathcal{I}$ est un idéal de $\mathbb{K}[x_1, x_2, ..., x_n]$.
Ce résultat sera présenté en détail dans le Chapitre 2.

— **Deuxième contribution :** En 2013, Bokut, Chen et Mo ont proposé un nouveau type de généralisation des bases de Gröbner dans le papier [9]. Leur idée est de faire passer la strucutre des monômes d'un monoïde à un semi-anneau. Nous avons adapté cette approche aux anneaux de valuation. Comparés aux bases de Gröbner classiques, les résultats de cette investigation donnent une double extension des bases de Gröbner :
  — une extension sur les monômes qui sont munis d'une structure de semi-anneau ;
  — une extension sur les coefficients qui sont munis d'une structure d'anneau

admettant des diviseurs de zéro : les anneaux de valuation.

De ce travail, résulte le papier [23] "Diop Y., Mesmoudi L., Sow D. *Semiring based Gröbner-Shirshov over a noetherian valuation ring. Associative and Non-associative Algebras and Applications. Springer Proceedings in Mathematics & Statistics, vol* 311(2020)*, pp* 183 − 198. *Springer, Cham*".

Le Chapitre 3 est une présentation détaillée de ce travail.

Plan de la thèse : Cette thèse est divisée en trois chapitres.

— **Chapitre** 1 **:** Rappels sur les bases de Gröbner.
Dans ce chapitre, on revient sur les notions de base et les résultats permettant de se familiariser aux bases de Gröbner et de comprendre le contenu des autres chapitres.

— **Chapitre** 2 **:** Sur la finitude des bases de Gröbner non commutatives.
Dans ce chapitre, on présentera en détail notre contribution portant sur la caractérisation de certains idéaux non commutatifs admettant des bases de Gröbner finies.

— **Chapitre** 3 **:** Bases de Gröbner-Shirshov sur un anneau de valuation.
Ce chapitre est une présentation de notre contribution portant sur la généralisation des bases de Gröbner-Shirshov aux anneaux de valuation.

Chapitre 1

Rappels sur les bases de Gröbner

Ce chapitre est consacré aux rappels sur les bases de Gröbner. Il est composé de trois sections. Dans la première section, on reviendra sur les bases de Gröbner commutatives sur un corps, dans la deuxième et la troisième sections intitulées respectivemnt Bases de Gröbner non commutatives sur un corps et Bases de Gröbner sur un anneau, on taitera les généralisations des bases de Gröbner. Pour chacune de ces sections, on introduira les concepts de base et les notations que nous utilisons. Le lecteur peut se réfèrer aux documents [20, 34] pour les détails concernant les notions élémentaires essentielles que sont anneaux, corps, idéaux, anneaux de polynômes à plusieurs indéterminées.

I Bases de Gröbner commutatives sur un corps

Il est connu que l'anneau $\mathbb{K}[X]$ des polynômes en une seule indéterminée est principal et euclidien.
Ainsi, le test d'appartenance d'un polynôme g à un idéal $\mathcal{I}$ de $\mathbb{K}[X]$ se réalise facilement par la division euclidienne de g par un polynôme f engendrant $\mathcal{I}$.
Par contre, l'anneau $\mathbb{K}[X_1, X_2, ..., X_n]$ des polynômes à plusieurs indéterminées n'est ni principal ni euclidien. Néanmoins, le théorème de la base de Hilbert affirme que tout idéal $\mathcal{I}$ de $\mathbb{K}[X_1, X_2, ..., X_n]$ admet au moins une partie génératrice finie. Faisant le parallèle avec l'anneau des polynômes en une seule indéterminée, on développe dans $\mathbb{K}[X_1, X_2, ..., X_n]$ un analogue de la division euclidienne afin de faire le test

d'appartenance. Puis, on verra que pour un idéal $\mathcal{I}$ donné, il peut exister des parties génératrices qui ne garantissent pas nécessairement l'unicité du reste de la division d'un polynôme f. Ces parties génératrices ne sont donc pas efficaces dans la résolution de l'IMP. Certaines parties génératrices ayant des propriétés particulières garantissent l'unicité du reste de la division d'un polynôme f. Ces dernières que nous appelerons plus tard bases de Gröbner permettent donc de résoudre l'IMP de façon efficace.

Les bases de Gröbner commutatives sur un corps sont le cas classique des bases de Gröbner. Elles ont été développées par B. Buchberger dans sa thèse de doctorat alors qu'il cherchait à résoudre le problème de l'appartenance d'un polynôme à un idéal [13].

I - 1 Notations

Etant donnés un corps commutatif $\mathbb{K}$ et un alphabet fini $X = \{X_1, X_2, ..., X_n\}$,

- l'anneau $\mathbb{K}[X_1, X_2, ..., X_n]$ des polynômes commutatifs à coefficients dans $\mathbb{K}$ et à indéterminées dans X est noté $\mathbb{K}[X]$;
- pour tout $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{N}^n$, le monôme ${X_1}^{\alpha_1}{X_2}^{\alpha_2}...{X_n}^{\alpha_n}$ est noté X^α ;
- L'ensemble $\{X^\alpha | \alpha \in \mathbb{N}^n\}$ des monômes est noté $\mathbb{M}$;
- l'idéal engendré par un sous-ensemble G de $\mathbb{K}[X]$ est noté $\langle G \rangle$.
- Le nombre d'éléments d'un ensemble fini G est appelé cardinal de G et noté card(G).

I - 2 Concepts de base

I - 2 - a Support d'un polynôme

Définition I - 2.1. *Tout polynôme* $f \in \mathbb{K}[X]$ *s'exprime de façon unique à une permutation près sous la forme*

$$f = \sum_{i \in \Lambda} a_i X^{\alpha_i},\ a_i \in \mathbb{K}\backslash\{0\},\ \alpha_i \in \mathbb{N}^n,\ \Lambda \textit{ est fini et } \alpha_i \neq \alpha_j \textit{ si } i \neq j$$

L'ensemble des monômes intervenant dans cette expression forme le support de f *noté* Supp(f).

I - 2 - b Degré d'un monôme et degré d'un polynôme

Définition I - 2.2.

— *Pour tout* $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{N}^n$*, l'entier naturel* $|\alpha| = \alpha_1 + \alpha_2 + ... + \alpha_n$ *est appelé degré du monôme* X^α*. On le note* $\deg(X^\alpha)$*.*

— *Le degré d'un polynôme* f *est le maximum des degrés des éléments de son support.*

I - 2 - c Relation de divisibilité entre monômes

Définition I - 2.3. *On dit qu'un monôme* X^α *divise un monôme* X^β *s'il existe un monôme* X^γ *tel que* $X^\beta = X^\alpha X^\gamma = X^{\alpha+\gamma}$ *où* $\alpha + \gamma = (\alpha_1 + \gamma_1, \alpha_2 + \gamma_2, ..., \alpha_n + \gamma_n)$*.*

Exemple I - 2.1. *Le monôme* X^2Z *divise* X^2Y^3Z *mais il n'y a aucune relation de divisibilité entre* XY *et* XZ *dans l'anneau à trois indéterminées* $\mathbb{K}[X, Y, Z]$*.*

I - 2 - d Ordre monomial

Dans l'écriture d'un polynôme en une seule indéterminée, les monômes sont très souvent rangés suivant leur degré. Le monôme de plus haut degré étant souvent désigné sous l'expression "monôme de tête". On peut vérifier que cet ordre défini à partir du degré est total, un bon ordre et compatible avec la multiplication des monômes. On l'étend à l'anneau commuatif des polynômes à plusieurs indéterminées. Plus précisément, on a la définition suivante.

Définition I - 2.4. *Un ordre* $\prec$ *sur* $\mathbb{M}$ *est appelé ordre monomial si :*

— $\prec$ *est total ;*

— $\prec$ *est un bon ordre ;*

— $\prec$ *est compatible avec la multiplication des monômes.*

Exemple I - 2.2. *Les ordres définis ci-après sont des ordres monomiaux.*

— *L'ordre lexicographique* $\prec_{lex}$ *défini par* $X^\alpha \prec_{lex} X^\beta$ *si et seulement si la première composante non nulle de* $\alpha - \beta$ *est négative.*

— *L'ordre lexicographique gradué* $\prec_{\text{grlex}}$ *défini par*

$$X^\alpha \prec_{\text{grlex}} X^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta| \\ \quad ou \\ |\alpha| = |\beta| \text{ et } X^\alpha \prec_{\text{lex}} X^\beta \end{cases}$$

En considérant l'alphabet $\{X, Y, Z\}$ *avec* $Z \prec Y \prec X$, *on a* $Z^4 \prec_{\text{lex}} XYZ \prec_{\text{lex}} X^2Z$ *et* $XYZ \prec_{\text{grlex}} X^2Z \prec_{\text{grlex}} Z^4$.

Remarque I.1. *Sur l'anneau des polynômes en une seule indéterminée, tous les ordres monomiaux sont identiques. Ainsi, on ne parle que de l'ordre du degré.*

Définition I - 2.5. *Soient* $f \in \mathbb{K}[X]$, $G \subset \mathbb{K}[X]$ *et* $\prec$ *un ordre monomial fixé.*

1. *Le maximum du support de* f *relativement à* $\prec$ *est appelé* ***monôme dominant*** *de* f *et noté* $\text{LM}_\prec(f)$.
   L'ensemble des monômes dominants de G *est* $\text{LM}_\prec(G) = \{\text{LM}_\prec(f) | f \in G\}$.
2. *Le coefficient de* $\text{LM}_\prec(f)$ *est appelé* ***coefficient dominant*** *de* f *et noté* $\text{LC}_\prec(f)$.
   L'ensemble des coefficients dominants de G *est* $\text{LM}_\prec(G) = \{\text{LM}_\prec(f) | f \in G\}$.
3. *Le produit* $\text{LC}_\prec(f)\text{LM}_\prec(f)$ *est appelé* ***terme dominant*** *de* f *et noté* $\text{LT}_\prec(f)$.
   L'ensemble des termes dominants de G *est* $\text{LT}_\prec(G) = \{\text{LT}_\prec(f) | f \in G\}$.

S'il n'y a aucun risque de confusion alors on notera uniquement LM, LC *et* LT *au lieu de* $\text{LM}_\prec$, $\text{LC}_\prec$ *et* $\text{LT}_\prec$.

Exemple I - 2.3. *Soit* $f = 2X^2Z + XYZ - Z^4$. *Alors*

1. $\text{LM}_{\prec_{lex}}(f) = X^2Z$, $\text{LC}_{\prec_{lex}}(f) = 2$, $\text{LT}_{\prec_{lex}}(f) = 2X^2Z$.
2. $\text{LM}_{\prec_{grlex}}(f) = Z^4$, $\text{LC}_{\prec_{grlex}}(f) = -1$, $\text{LT}_{\prec_{grlex}}(f) = -Z^4$.

Définition I - 2.6. *Etant donnés un ordre monomial et des monômes* X^α *et* X^β. *On note par* $\text{CM}(X^\alpha, X^\beta)$ *l'ensemble des multiples communs à* X^α *et* X^β. *Le plus petit élément de* $\text{CM}(X^\alpha, X^\beta)$ *est appelé* ***plus petit commun multiple*** *de* X^α *et* X^β. *Il est noté* $\text{LCM}(X^\alpha, X^\beta)$.

Exemple I - 2.4. *On considère les monômes* X^2Z, XYZ *et* Z^4. *Alors :*

— $LCM(X^2Z, XYZ) = X^2YZ$;

— $LCM(X^2Z, Z^4) = X^2Z^4$;

— $LCM(XYZ, Z^4) = XYZ^4$.

Proposition I - 2.1. *Etant fixé un ordre monomial, tout polynôme* f *de* $\mathbb{K}[X_1, X_2, ..., X_n]$ *s'écrit de façon unique sous la forme :*

$$f = \sum_{i \in \Lambda} a_i X^{\alpha_i},\ a_i \in \mathbb{K}\backslash\{0\}, \Lambda \text{ un sous} - \text{ensemble fini de } \mathbb{N}\ X^{\alpha_i} \prec X^{\alpha_j} \text{ si } i < j$$

I - 2 - e Algorithme de réduction

La notion d'ordre monomial permet également de définir sur l'anneau des polynômes à plusieurs indéterminées un analogue de la division euclidienne. La réduction définie ci-après constitue l'outil de base de cette "division".

Définition I - 2.7. *Soit* $f, g \in \mathbb{K}[X]$, *et* $G \subset \mathbb{K}[X]$, " $\prec$ " *un ordre monomial sur* $\mathbb{M}$.

• f *est dit* ***réductible*** *modulo* g *(ou* g*-réductible) s'il existe un couple* $(X^\alpha, X^\beta) \in \text{Supp}(f) \times \mathbb{M}$ *tel que* $X^\alpha = X^\beta LM(g)$. *Dans ce cas, le polynôme* $h = f - \frac{a_\alpha}{LC(g)} X^\beta g,\ a_\alpha \neq 0$ *étant le coefficient du monôme* X^α *dans* f, *est appelé réduit de* f *modulo* g *et est noté :* $f \xrightarrow{g} h$ *ou* $h = Red(f, g, \prec)$.

Si $X^\alpha = LM(f)$, *on dit que* f *est* ***top-réductible*** *modulo* g *et* h *est appelé le* ***top-réduit*** *de* f *modulo* g.

• f *est réductible modulo* G *s'il existe* $g \in G$ *tel que* f *soit* g*-réductible.*

• f *est dit* ***réduit*** *ou* ***irréductible*** *modulo* f (*respectivement modulo* G) *s'il ne peut se réduire modulo* f (*respectivement modulo* G).

• f ***se réduit totalement*** *en* h *modulo* G *s'il existe une suite de réductions du type* $f \xrightarrow{G} h_1 \xrightarrow{G} h_2 ... \ h_{m-1} \xrightarrow{G} h_m = h$ *telle que* h *soit irréductible modulo* G.

• *Si* f *est irréductible modulo tout élément de* G *alors on dit que* f *est irréductible ou totalement réduit modulo* G. *L'ensemble des polynômes totalement réduits modulo* G *est noté* G_r.

L'algorithme de réduction décrit ci-dessous permet de réduire un polynôme modulo un ensemble de polynômes donné. On y utilise la top-réduction qui permet d'éliminer à chaque étape le terme dominant du polynôme obtenu précédemment en donnant un polynôme dont le monôme dominant est strictement plus petit. Ceci sera un aspect très important dans la démonstration de la terminaison de l'algorithme.

Algorithme 1 : Réduction Totale

Entrée : $(f, G, \prec)$

Sortie : r : *irréductible modulo* G

```
1  r ← 0;
2  Tant que f ≠ 0 Faire
3  |  Si LM(f) = X^α LM(g), X^α ∈ M, g ∈ G Alors
4  |  |  f ← f − (LC(f)/LC(g)) X^α g
5  |  Sinon
6  |  |  r ← r + LT(f);
7  |  |  f ← f − LT(f);
8  |  FinSi
9  Fin
10 Retourner r
```

Théorème I.1. *L'algorithme de réduction se termine.*

Démonstration. *On pose* $f_0 = f$ *et* f_i *est le résultat de la* i-ème *itération. Si l'algorithme est infini, on obtient la suite infinie strictement décroissante suivante :* $LM(f_0) \succ LM(f_1) \succ ... \succ LM(f_t) \succ ...$ *; ce qui est contraire au caractère de bon ordre de* $\prec$*. L'algorithme est donc bien fini.* □

Exemple I - 2.5. *Ici, on fait la réduction du polynôme* $f = XY^2 + Y^2Z^2 + Z$ *par* $G = \{g_1 = XY + X, g_2 = Y^2 - Z, g_3 = X^2 + YZ^2\}$ *en considérant* $\prec_{lex}$ *où* $Z \prec Y \prec X$.
Première itération :
$LM(f) = XY^2 = YLM(g_1) \Rightarrow f \leftarrow f - Yg_1 = -XY + Y^2Z^2 + Z$
Deuxième itération :
$LM(f) = LM(g_1) \Rightarrow f \leftarrow f + g_1 = X + Y^2Z^2 + Z$

Troisième itération :
$\mathrm{LM(f)} = \mathrm{X} \neq \mathrm{X}^{\alpha}\mathrm{LM(g)}\ \forall\ (\mathrm{X}^{\alpha}, \mathrm{g}) \in \mathbb{M} \times \mathrm{G} \Rightarrow \mathrm{r} \leftarrow \mathrm{X}$ *et* $\mathrm{f} \leftarrow \mathrm{f} - \mathrm{X} = \mathrm{Y}^2\mathrm{Z}^2 + \mathrm{Z}$
Quatrième itération :
$\mathrm{LM(f)} = \mathrm{Y}^2\mathrm{Z}^2 = \mathrm{Z}^2\mathrm{LM}(\mathrm{g}_2) \Rightarrow \mathrm{f} \leftarrow \mathrm{f} - \mathrm{Z}^2\mathrm{g}_2 = \mathrm{Z}^3 + \mathrm{Z}$
Cinquième itération :
$\mathrm{LM(f)} = \mathrm{Z}^3 \neq \mathrm{X}^{\alpha}\mathrm{LM(g)}\ \forall\ (\mathrm{X}^{\alpha}, \mathrm{g}) \in \mathbb{M} \times \mathrm{G} \Rightarrow \mathrm{r} \leftarrow \mathrm{X} + \mathrm{Z}^3$ *et* $\mathrm{f} \leftarrow \mathrm{f} - \mathrm{Z}^3 = \mathrm{Z}$
Sixième itération :
$\mathrm{LM(f)} = \mathrm{Z} \neq \mathrm{X}^{\alpha}\mathrm{LM(g)}\ \forall\ (\mathrm{X}^{\alpha}, \mathrm{g}) \in \mathbb{M} \times \mathrm{G} \Rightarrow \mathrm{r} \leftarrow \mathrm{X} + \mathrm{Z}^3 + \mathrm{Z}$ *et* $\mathrm{f} \leftarrow \mathrm{f} - \mathrm{Z} = 0$
Sortie de la boucle : $\mathrm{r} = \mathrm{X} + \mathrm{Z}^3 + \mathrm{Z}$

Le théorème suivant est une conséquence de l'algorithme de réduction.

Théorème I.2. *Soit* $\mathrm{G} \subset \mathbb{K}[\mathrm{X}]$ *et* $\mathrm{f} \in \mathbb{K}[\mathrm{X}]$. *Il existe* $(\mathrm{g}, \mathrm{r}) \in \langle \mathrm{G} \rangle \times \mathrm{G}_{\mathrm{r}}$ *tel que* $\mathrm{f} = \mathrm{g} + \mathrm{r}$.

Pour la preuve de ce théorème, il suffit d'appliquer au couple (f, G) l'algorithme de réduction précédemment décrit.

Remarque I.2. *Il est important de noter que, contrairement à la division euclidienne, l'algorithme de réduction ne donne pas nécessairement un reste unique comme le montre l'exemple suivant.*

Exemple I - 2.6. *On reprend les données de l'exemple précédent. Cette fois, on décide de commencer la réductionn par* g_2.
$\mathrm{f} = \mathrm{XY}^2 + \mathrm{Y}^2\mathrm{Z}^2 + \mathrm{Z},\ \mathrm{G} = \{\mathrm{g}_1 = \mathrm{XY} + \mathrm{X},\ \mathrm{g}_2 = \mathrm{Y}^2 - \mathrm{Z},\ \mathrm{g}_3 = \mathrm{X}^2 + \mathrm{YZ}^2\}$ *et* $\prec_{\mathrm{lex}}$ *avec* $\mathrm{X} \succ \mathrm{Y} \succ \mathrm{Z}$.
Première itération :
$\mathrm{LM(f)} = \mathrm{XY}^2 = \mathrm{XLM}(\mathrm{g}_2) \Rightarrow \mathrm{f} \leftarrow \mathrm{f} - \mathrm{Xg}_2 = \mathrm{XZ} + \mathrm{Y}^2\mathrm{Z}^2 + \mathrm{Z}$
Deuxième itération :
$\mathrm{LM(f)} = \mathrm{XZ} \neq \mathrm{X}^{\alpha}\mathrm{LM(g)}\ \forall\ (\mathrm{X}^{\alpha}, \mathrm{g}) \in \mathbb{M} \times \mathrm{G} \Rightarrow \mathrm{r} \leftarrow \mathrm{XZ}$ *et* $\mathrm{f} \leftarrow \mathrm{f} - \mathrm{XZ} = \mathrm{Y}^2\mathrm{Z}^2 + \mathrm{Z}$
Troisième itération :
$\mathrm{LM(f)} = \mathrm{Y}^2\mathrm{Z}^2 = \mathrm{Z}^2\mathrm{LM}(g_2) \Rightarrow f \leftarrow \mathrm{f} - \mathrm{Z}^2\mathrm{g}_2 = \mathrm{Z}^3 + \mathrm{Z}$
Quatrième itération :
$\mathrm{LM(f)} = \mathrm{Z}^3 \neq \mathrm{X}^{\alpha}\mathrm{LM(g)}\ \forall\ (\mathrm{X}^{\alpha}, \mathrm{g}) \in \mathbb{M} \times \mathrm{G} \Rightarrow \mathrm{r} \leftarrow \mathrm{XZ} + \mathrm{Z}^3$ *et* $\mathrm{f} \leftarrow \mathrm{f} - \mathrm{Z}^3 = \mathrm{Z}$

Cinquième itération :
$\mathrm{LM(f)} = \mathrm{Z} \neq \mathrm{X}^{\alpha}\mathrm{LM(g)}\ \forall\ (\mathrm{X}^{\alpha}, \mathrm{g}) \in \mathbb{M} \times \mathrm{G} \Rightarrow \mathrm{r} \leftarrow \mathrm{XZ} + \mathrm{Z}^3 + \mathrm{Z}$ *et* $\mathrm{f} \leftarrow \mathrm{f} - \mathrm{Z} = 0$
Sortie de la boucle : $\mathrm{r} = \mathrm{XZ} + \mathrm{Z}^3 + \mathrm{Z}$.

En changeant le chemin de parcours dans G, le résultat a également changé. On se pose alors la question de savoir s'il existe des conditions pour que le reste de l'algorithme de réduction soit unique. Dans la suite, on verra que si G est une base de Gröbner alors le résultat de l'algorithme est unique et ne dépend pas du chemin choisi ; d'où la paricularité des bases de Gröbner.

I - 3 Bases de Gröbner commutatives sur un corps

I - 3 - a Généraliés sur les bases de Gröbner commutatives sur un corps

Définition I - 3.1. *Un idéal est dit monomial s'il peut être engendré par des monômes.*

Exemple I - 3.1. *L'idéal* $\mathcal{I} = \langle \mathrm{X}^2\mathrm{Y}, \mathrm{Y}^2, \mathrm{XZY} \rangle$ *est un idéal monomial de* $\mathbb{R}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$.

Définition I - 3.2. *Soit* $\mathrm{G} \subset \mathbb{K}[\mathrm{X}]$, $\mathcal{I} = \langle \mathrm{G} \rangle$ *et* $\prec$ *un ordre monomial. On dit que* G *est une base de Gröbner de* $\mathcal{I}$ *relativement à* $\prec$ *si* $\langle \mathrm{LM(G)} \rangle = \langle \mathrm{LM}(\mathcal{I}) \rangle$.

Une fois la définition établie, la question est de savoir comment les bases de Gröbner résolvent-elles toujours le problème posé. La réponse se trouve dans le théorème suivant.

Théorème I.3. *Si* G *est une base de Gröbner alors pour tout polynôme* f *il existe un unique couple* $(\mathrm{g}, \mathrm{r}) \in \langle \mathrm{G} \rangle \times \mathrm{G_r}$ *tel que* $\mathrm{f} = \mathrm{g} + \mathrm{r}$.

Démonstration. *Soit* f *un polynôme et* G *une base de Gröbner. On applique à* f *l'algorithme de réduction modulo* G *empruntant deux chemins différents. Ainsi, on a :* $\mathrm{f} = \mathrm{g_1} + \mathrm{r_1} = \mathrm{g_2} + \mathrm{r_2}$, $\mathrm{g_1}, \mathrm{g_2} \in \langle \mathrm{G} \rangle$, $\mathrm{r_1}, \mathrm{r_2} \in \mathrm{G_r}$.
$\mathrm{g_1} + \mathrm{r_1} = \mathrm{g_2} + \mathrm{r_2} \Rightarrow \mathrm{g_1} - \mathrm{g_2} = \mathrm{r_2} - \mathrm{r_1} \in \langle \mathrm{G} \rangle$. *Or* G *est une base de Gröbner. Si* $\mathrm{r_2} - \mathrm{r_1} \neq 0$ *alors* $\mathrm{LM}(\mathrm{r_2} - \mathrm{r_1}) \in \langle \mathrm{LM(G)} \rangle$ *; ie* $[\mathrm{Supp}(\mathrm{r_1}) \bigcup \mathrm{Supp}(\mathrm{r_2})] \bigcap \langle \mathrm{LM}(G) \rangle \neq \varnothing$ *; ce qui est absurde. D'où* $\mathrm{r_2} - \mathrm{r_1} = 0$ *; ie* $\mathrm{r_1} = \mathrm{r_2}$. □

Définition I - 3.3. *Soient* f *un polynôme,* G *une base de Gröbner et* (g, r) *l'unique élément de* $\langle \mathrm{G} \rangle \times \mathrm{G}_\mathrm{r}$ *tel que* $\mathrm{f} = \mathrm{g} + \mathrm{r}$. *Alors, le polynôme* r *est appelé* ***forme normale*** *de* f *modulo* G. *On note* $\mathrm{r} = \mathrm{NF}(\mathrm{f}, \mathrm{G}, \prec)$ *ou* $\mathrm{r} = \mathrm{NF}(\mathrm{f}, \mathrm{G})$ *ou* $\mathrm{r} = \mathrm{NF}(\mathrm{f})$ *s'il n'y aucune ambiguité sur l'ensemble* G *et l'ordre monomial* $\prec$.

L'unicité du reste est très importante et le théorème suivant en résulte.

Théorème I.4. *Soit* G *une base de Gröbner d'un idéal* $\mathcal{I}$ *relativement à un ordre monomial* $\prec$ *et* f *un polynôme. Alors* $\mathrm{f} \in \mathcal{I}$ *si et seulement si* $\mathrm{NF}(\mathrm{f}, \mathrm{G}, \prec) = 0$.

Ainsi, les bases de Gröbner résolvent donc efficacement le problème de l'appartenance d'un polynôme à un idéal donné et se distinguent des parties génératrices quelconques. Ceci conduit à la question de savoir comment se caractérisent les bases de Gröbner. Tout d'abord, on a la définition suivante.

Définition I - 3.4. *Soient* f *et* g *deux polynômes et* $X^\gamma = \mathrm{LCM}[\mathrm{LM}(\mathrm{f}), \mathrm{LM}(\mathrm{g})]$. *On appelle S-polynôme de* f *et* g *le polynôme noté* $\mathrm{S\text{-}pol}(\mathrm{f}, \mathrm{g})$ *défini par* $\mathrm{S\text{-}pol}(\mathrm{f}, \mathrm{g}) = \frac{\mathrm{X}^\gamma}{\mathrm{LT}(\mathrm{f})}\mathrm{f} - \frac{\mathrm{X}^\gamma}{\mathrm{LT}(\mathrm{g})}\mathrm{g}$.

Exemple I - 3.2. *On donne* $\mathrm{f} = 2\mathrm{X}^2\mathrm{Y} + 4\mathrm{Y}^2 - 6\mathrm{Z}^3,\ \mathrm{g} = \mathrm{Y}^3 + 3\mathrm{XZ} + 1 \in \mathbb{R}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. *Sur l'alphabet* $\{\mathrm{X}, \mathrm{Y}, \mathrm{Z}\}$, *on fixe l'ordre* $\mathrm{Z} \prec \mathrm{Y} \prec \mathrm{X}$.

1. *Suivant l'ordre lexicographique* $\prec_{\mathrm{lex}}$, $\mathrm{LM}(\mathrm{f}) = \mathrm{X}^2\mathrm{Y}$ *et* $\mathrm{LM}(\mathrm{g}) = \mathrm{XZ}$.
   Alors $\mathrm{LCM}(\mathrm{LM}(\mathrm{f}), \mathrm{LM}(\mathrm{g})) = \mathrm{X}^2\mathrm{YZ}$ *et*

$$\begin{aligned}\mathrm{S-Pol}(\mathrm{f}, \mathrm{g}) &= \frac{\mathrm{X}^2\mathrm{YZ}}{2\mathrm{X}^2\mathrm{Y}}\mathrm{f} - \frac{\mathrm{X}^2\mathrm{YZ}}{\mathrm{XZ}}\mathrm{g} \\ &= \mathrm{Z}(\mathrm{X}^2\mathrm{Y} + 2\mathrm{Y}^2 - 3\mathrm{Z}^3) - \mathrm{XY}(\mathrm{Y}^3 + 3\mathrm{XZ} + 1) \\ &= -\mathrm{XY}^4 - \mathrm{XY} + 2\mathrm{Y}^2\mathrm{Z} - 3\mathrm{Z}^4.\end{aligned}$$

2. *Suivant l'ordre lexicographique gradué* $\prec_{\mathrm{grlex}}$, $\mathrm{LM}(\mathrm{f}) = \mathrm{X}^2\mathrm{Y}$ *et* $\mathrm{LM}(\mathrm{g}) = \mathrm{Y}^3$.
   Alors $\mathrm{LCM}(\mathrm{LM}(\mathrm{f}), \mathrm{LM}(\mathrm{g})) = \mathrm{X}^2\mathrm{Y}^3$ *et*

$$\begin{aligned}\mathrm{S-Pol}(\mathrm{f}, \mathrm{g}) &= \frac{\mathrm{X}^2\mathrm{Y}^3}{2\mathrm{X}^2\mathrm{Y}}\mathrm{f} - \frac{\mathrm{X}^2\mathrm{Y}^3}{\mathrm{Y}^3}\mathrm{g} \\ &= \mathrm{Y}^2(\mathrm{X}^2\mathrm{Y} + 2\mathrm{Y}^2 - 3\mathrm{Z}^3) - \mathrm{X}^2(\mathrm{Y}^3 + 3\mathrm{XZ} + 1) \\ &= -3\mathrm{Y}^2\mathrm{Z}^3 - 3\mathrm{X}^3\mathrm{Z} + 2\mathrm{Y}^2 - \mathrm{X}^2.\end{aligned}$$

Calculé en fonction des monômes dominants, le S-Polynôme dépend de l'ordre monomial choisi. Cependant, on peut remarquer que pour toute paire (f, g) de polynômes et tout ordre monomial $\prec$ fixé, $LM[S\text{-}Pol(f, g)] \prec LCM[LM(f), LM(g)]$.

Le théorème suivant est le résultat fondamental des bases de Gröbner. Il donne une caractérisation complète de ces dernières à partir des S-polynômes. Le lecteur peut se réfèrer à [20, page 74] pour la preuve.

Théorème I.5 (Critère de Buchberger)**.** *Soient* $G \subset \mathbb{K}[X]$ *et* $\prec$ *un ordre monomial. Les assertions suivantes sont équivalentes.*

1. G *est une base de Gröbner.*
2. *Pour toute paire* $(f, g) \in G^2$, $S\text{-}Pol(f, g) \xrightarrow{G} 0$

Ce théorème est l'outil principal utilisé pour vérifier si un ensemble donné est une base de Gröbner ou non relativement à un ordre monomial fixé.

Exemple I - 3.3. *On donne* $G = \{g_1 = 2X^2Y + 4X + 6,\ g_2 = Z^2 + Y + 1\} \subset \mathbb{R}[X, Y, Z]$. *Alors* G *est une base de Gröbner relativement à l'ordre* $\prec_{grlex}$ *induit par l'ordre alphabétique* $Z \prec Y \prec X$.
En effet, $S\text{-}Pol(g_1, g_2) = \frac{X^2YZ^2}{2X^2Y} g_1 - \frac{X^2YZ^2}{Z^2} g_2 = -X^2Y^2 - X^2Y + 2XZ^2 + 3Z^2 = h_1$
$h_1 \xrightarrow{g_1} h_1 + \frac{1}{2}Yg_1 = -X^2Y + 2XZ^2 + 2XY + 3Z^2 + 3Y = h_2$
$h_2 \xrightarrow{g_1} h_2 + \frac{1}{2}g_1 = 2XZ^2 + 2XY + 3Z^2 + 2X + 3Y + 3 = h_3$
$h_3 \xrightarrow{g_2} h_3 - 2Xg_2 = 3Z^2 + 3Y + 3 = h_4$
$h_4 \xrightarrow{g_2} h_3 - 3g_2 = 0$

L'efficacité des bases de Gröbner dans la résolution du test d'appartenance conduit également à la question de savoir si tout idéal admet une telle base. La réponse est donnée par l'algorithme de Buchberger. Cet algorithme construit une base de Gröbner à partir d'une partie génératrice quelconque dont l'existence est garantie par le théorème de la base de Hilbert.

Théorème I.6 (Théorème de la base de Hilbert)**.** *Tout idéal* $\mathcal{I}$ *de* $\mathbb{K}[X]$ *admet une partie génératrice finie.*

Démonstration. *Voir [20, page 74]*

L'algorithme de Buchberger suivant découle du Théorème I.5. Il permet de construire une base de Gröbner d'un idéal $\mathcal{I}$ à partir d'une partie génératrice G par des ajouts successifs des réduits non nuls des S-Polynômes. Il est évident que les S-polynômes définis dans l'ensemble G (retourné) seront tous réduits à zéro.

Algorithme 2 : Algorithme de Buchberger

Entrée : $(G, \preceq)$, où G est un ensemble de ployômes et $\preceq$, un ordre monomial.

Sortie : Base de Gröbner de $\mathcal{I} = \langle G \rangle$

```
P ← {(f, g) ∈ G²};
Tant que P ≠ ∅ Faire
    Retirer un élément (f, g) de P;
    Si h = Réduction Totale(G, Spol(f, g) ≼) ≠ 0 Alors
        P ← P ∪ {(h, g), g ∈ G};
        G ← G ∪ {h};
Fin
Retourner G
```

Proposition I - 3.1. *L'algorithme de Buchberger se termine.*

Démonstration. *Rappelons que* $\mathbb{K}[X]$ *est noethérien.*
Soit $G \subset \mathbb{K}[X]$*. Si tous les* S-polynômes *définis dans* G *sont réduits à zéro, il est évident que l'algorithme se termine et renvoie* G *à la sortie.*
Supposons qu'il existe $f,\ g \in G$ *tels que* $\text{S-pol}(f, g) \xrightarrow{G} r_1 \neq 0$*. Alors,* G *est remplacé par* $G_1 = G \cup \{r_1\}$*. Soit tous les* S-polynômes *définis dans* G_1 *sont réduits à zéro, soit ce n'est pas le cas. Dans le premier cas, l'algorithme s'arrête, dans le second, on itère le processus.*
Supposons que cette itération continue infiniment. On obtient la suite de bases de $\mathcal{I}$ *suivante*

$$G_0 = G \subset G_1 \subset ... \subset G_m \subset ...,$$

avec $G_{i+1} = G_i \cup \{r_i\}$ *où l'existence de* $f,\ g \in G_i$ *tels tels que* $\text{S-pol}(f, g) \xrightarrow{G_i} r_i \neq 0$ *est une condition nécessaire à la continuité de l'algorithme.*

On pose $\mathrm{LM}(\mathrm{G_i}) = \{\mathrm{LM(g)}|\mathrm{g} \in \mathrm{G_i}\},\ \mathrm{i} = 0, 1, ...$
$\mathrm{G_{i+1}} = \mathrm{G_i} \cup \{\mathrm{r_i}\} \Rightarrow\ \mathrm{LM}(\mathrm{r_i})$ *n'est divisible par aucun monôme dominant de* $\mathrm{G_i}$. *Donc* $\mathrm{LM}(\mathrm{r_i}) \notin \langle \mathrm{LM}(\mathrm{G_i})\rangle$. *On en déduit que la suite d'idéaux monomiaux suivante :*

$$\langle \mathrm{LM}(\mathrm{G_0})\rangle \subset \langle \mathrm{LM}(\mathrm{G_1})\rangle \subset ... \subset \langle \mathrm{LM}(\mathrm{G_m})\rangle \subset ...$$

est strictement croissante et infinie ; ce qui est impossible.
Ainsi, la suite $(\mathrm{G_i})_{\mathrm{i}\in\mathbb{N}}$ *est stationnaire ; d'où la finitude de l'algorithme de Buchberger.*□

De l'algorithme de Buchberger, on déduit le résultat suivant.

Théorème I.7. *Tout idéal de* $\mathbb{K}[\mathrm{X}]$ *admet une base de Gröbner finie relativement à tout ordre monomial.*

Exemple I - 3.4. *Construisons une base de Gröbner de l'idéal* $\mathcal{I} = \langle \mathrm{G}\rangle$ *relativement à l'ordre monomial fixé.* $\mathrm{G} = \{\mathrm{g_1} = \mathrm{X^2Y} - 1,\ \mathrm{g_2} = \mathrm{XY^2} - \mathrm{X}\},\ \mathrm{Y} \prec \mathrm{X},\ \prec = \prec_{\mathrm{lex}}$.
Déroulement de l'algorithme
$\mathrm{G^{comp}} \leftarrow \mathrm{G}$
$\mathrm{P} \leftarrow \{(\mathrm{g_1}, \mathrm{g_2})\}$
$\mathrm{P} \neq \varnothing$ *; on choisit la paire* $(\mathrm{g_1}, \mathrm{g_2})$
$\mathrm{P} \leftarrow \varnothing$
$\mathrm{S\text{-}pol}(\mathrm{g_1}, \mathrm{g_2}) = \mathrm{Yg_1} - \mathrm{Xg_2}$
$= X - Y$
$= \mathrm{g_3}$ (*irréductible*)
$\mathrm{P} \leftarrow \{(\mathrm{g_1}, \mathrm{g_3}),\ (\mathrm{g_2}, \mathrm{g_3})\}$
$\mathrm{G^{comp}} \leftarrow \{\mathrm{g_1}, \mathrm{g_2}, \mathrm{g_3}\}$
$\mathrm{P} \neq \varnothing$ *; on choisit la paire* $(\mathrm{g_1}, \mathrm{g_3})$
$\mathrm{P} \leftarrow \{(\mathrm{g_2}, \mathrm{g_3})\}$
$\mathrm{S\text{-}pol}(\mathrm{g_1}, \mathrm{g_3}) = \mathrm{g_1} - \mathrm{XYg_3}$
$= \mathrm{xy^2} - 1 \xrightarrow{\mathrm{g_2}} \mathrm{X} - 1 \xrightarrow{\mathrm{g_3}} \mathrm{Y} - 1 = \mathrm{g_4}$ (*irréductible*)
$\mathrm{P} \leftarrow \{(\mathrm{g_2}, \mathrm{g_3}),\ (\mathrm{g_1}, \mathrm{g_4}),\ (\mathrm{g_2}, \mathrm{g_4}),\ (\mathrm{g_3}, \mathrm{g_4})\}$
$\mathrm{G^{comp}} \leftarrow \{\mathrm{g_1}, \mathrm{g_2}, \mathrm{g_3}, \mathrm{g_4}\}$
$\mathrm{P} \neq \varnothing$ *; on choisit la paire* $(\mathrm{g_2}, \mathrm{g_3})$.
$\mathrm{P} \leftarrow \{(\mathrm{g_1}, \mathrm{g_4}),\ (\mathrm{g_2}, \mathrm{g_4}),\ (\mathrm{g_3}, \mathrm{g_4})\}$

$\text{S-pol}(g_2, g_3) = g_2 - Y^2 g_3$
$= Y^3 - X \xrightarrow{g_3} Y^3 - Y \xrightarrow{g_4} Y^2 - Y \xrightarrow{g_4} 0$
$P \neq \varnothing$ *; on choisit la paire* (g_1, g_4).
$P \leftarrow \{(g_2, g_4),\ (g_3, g_4)\}$
$\text{S-pol}(g_1, g_4) = g_1 - X^2 g_4 = X^2 - 1 \xrightarrow{g_3} XY - 1 \xrightarrow{g_3} Y^2 - 1 \xrightarrow{g_4} Y - 1 \xrightarrow{g_4} 0$
$P \neq \varnothing$ *; on choisit la paire* (g_2, g_4).
$P \leftarrow \{(g_3, g_4)\}$
$\text{S-pol}(g_2, g_4) = g_2 - XYg_4 = XY - X \xrightarrow{g_4} 0$
$P \neq \varnothing$ *; on choisit la paire* (g_3, g_4).
$P \leftarrow \varnothing$
$\text{S-pol}(g_3, g_4) = Yg_3 - Xg_4 = X - Y^2 \xrightarrow{g_3} Y - Y^2 \xrightarrow{g_4} 0$
$P = \varnothing$ *: La boucle s'arrête.*
$G^{\text{comp}} = \{g_1 = X^2Y - 1,\ g_2 = XY^2 - X,\ g_3 = X - Y,\ g_4 = Y - 1\}$ *est une base de Gröbner de de* $\mathcal{I} = \langle g_1, g_2 \rangle$.

Remarque I.3. *Dorénavant, même sans aucune précision, toute base de Gröbner commutative considérée est finie.*

Il est clair que si G est une base de Gröbner d'un idéal $\mathcal{I}$ alors $G \bigcup \{f\}$ est une base de Gröbner de $\mathcal{I}$ pour tout $f \in \mathcal{I}$. Ainsi, on peut construire une base de Gröbner avec un "nombre élevé" d'éléments. On se pose alors la question de savoir si pour tout idéal donné $\mathcal{I}$ il existe un nombre minimal d'éléments contenus dans chacune de ses bases de Gröbner. La réponse est affirmative et sera donnée par des bases de Gröbner avec des propriétés particulières. Ces bases de Gröbner aux propriétés particulères sont classées en deux familles : les bases de Gröbner minimales et les bases de Gröbner réduites. Elles fixent leur nombre d'éléments à un entier m bien défini et se distinguent des bases de Gröbner quelconques.

I - 3 - b Bases de Gröbner minimales

Définition I - 3.5. *Une base de Gröbner* G *est dite* ***minimale*** *si pour tout* $g \in G$, *on a :*

1. $\text{LC}(g) = 1$ *;*

2. $\mathrm{LM}(g)$ *est irréductible modulo* $G\backslash\{g\}$.

Exemple I - 3.5. $G' = \{g'_1 = X + 2Z^2,\ g'_2 = Y^2 + 2Z - 1\} \subset \mathbb{R}[X, Y, Z]$ *est une base de Gröbner minimale relativement à l'ordre* $\prec_{\mathrm{lex}}$ *induit par l'ordre alphabétique* $Z \prec Y \prec X$.

Remarque I.4. *Si* G *est une base de Gröbner minimale de* $\mathcal{I}$ *alors pour tout* $g \in G$, $G\backslash\{g\}$ *n'est pas une base de Gröbner de* $\mathcal{I}$.

Proposition I - 3.2. *De toute base de Gröbner d'un idéal, on peut extraire une base de Gröbner minimale de cet idéal.*

Démonstration. *Soit* $\mathcal{I}$ *un idéal et* G *une base de Gröbner de* $\mathcal{I}$. *Supposons qu'il existe* $g_1, g_2 \in G$ *tels que* $\mathrm{LM}(g_1)$ *divise* $\mathrm{LM}(g_2)$.
$\mathrm{LM}(g_1)$ *divise* $\mathrm{LM}(g_2)$ *implique que* $G\backslash\{g_1\}$ *est une base de Gröbner de* $\mathcal{I}$. *En effet, si* $\mathrm{LM}(g_1)$ *divise* $\mathrm{LM}(g_2)$ *alors* g_2 *est réductible modulo* g_1 *en un polynôme* $g'_2 \in \mathcal{I}$ *;* $g_2 \xrightarrow{g_1} g'_2$.
$g'_2 \in \mathcal{I} \Rightarrow g'_2 \xrightarrow{G} 0$. *Or,* $\mathrm{LM}(g'_2) \prec \mathrm{LM}(g_2)$. *Donc* $g'_2 \xrightarrow{G\backslash\{g_2\}} 0$.
Finalement, $g_2 \xrightarrow{G\backslash\{g_2\}} 0$. *On en déduit que* $g_2 \in \langle G\backslash\{g_2\}\rangle$. *D'où* $\langle G\rangle = \langle G\backslash\{g_2\}\rangle$.
En continuant ce processus d'élimination, on obtient $\langle G\rangle = \langle G\backslash\{g_2, g_3, ..., g_t\}\rangle$ *telle qu'il n'y ait aucune relation de division entre deux éléments différents de* $\mathrm{LM}(G\backslash\{g_2, g_3, ..., g_t\})$. *En rendant unitaire l'ensemble* $G\backslash\{g_2, g_3, ..., g_t\}$, *on obtient une base de Gröbner minimale de* $\mathcal{I} = \langle G\rangle$. □

De la preuve précédente, on déduit l'algorithme suivant qui constuit une base de Gröbner minimale à partir d'une base de Gröbner donnée.

Algorithme 3 : Construction de base de Gröbner minimale

Entrée : G une base de Gröbner de $\langle G \rangle$

Sortie : G′ base de Gröbner minimale de $\langle \mathrm{G} \rangle$

```
G' ← ∅;
Tant que G ≠ ∅ Faire
    prendre un g ∈ G vérifiant LM(g) = min(LM(G));
    G ← G\{f ∈ G | LM(f) ∈ ⟨LM(g)⟩};
    G' ← G' ⋃ {1/LC(g) g}
Fin
Retourner G'
```

Exemple I - 3.6. *On veut trouver une base de Gröbner minimale de l'idéal engendré par l'ensemble* $\mathrm{G} = \{\mathrm{g}_1 = \mathrm{X}^2\mathrm{Y} - 1,\ \mathrm{g}_2 = \mathrm{XY}^2 - \mathrm{X},\ \mathrm{g}_3 = \mathrm{X} - \mathrm{Y},\ \mathrm{g}_4 = \mathrm{Y} - 1\}$.
On remrque d'abord que G *est une base de Gröbner relativement à l'ordre lexicographique induit par l'ordre alphabétique* $\mathrm{Y} \prec \mathrm{X}$. *En appliquant l'algorithme à* G, *on a :*
initialisation : $\mathrm{G}' \leftarrow \varnothing$
$\mathrm{LM}(\mathrm{g}_4) = \min(\mathrm{LM}(\mathrm{G})) \Rightarrow \mathrm{G} \leftarrow \mathrm{G}\backslash\{\mathrm{f} \in \mathrm{G} \mid \mathrm{LM}(\mathrm{f}) \in \langle \mathrm{LM}(\mathrm{g}_4)\rangle\} = \{\mathrm{g}_3\}$
$\mathrm{G}' \leftarrow \{\mathrm{g}_4\}$
$\mathrm{LM}(\mathrm{g}_3) = \min(\mathrm{LM}(\mathrm{G})) \Rightarrow \mathrm{G} \leftarrow \mathrm{G}\backslash\{\mathrm{f} \in \mathrm{G} \mid \mathrm{LM}(\mathrm{f}) \in \langle \mathrm{LM}(\mathrm{g}_3)\rangle\} = \varnothing$
$\mathrm{G}' \leftarrow \{\mathrm{g}_4, \mathrm{g}_3\}$
Comme G *est vide, l'algorithme s'arrête.* $\mathrm{G}' = \{\mathrm{g}_4, \mathrm{g}_3\}$ *est une base de Gröbner minimale de* $\langle \mathrm{G} \rangle$.

Proposition I - 3.3. *Soient* G *et* G′ *des bases de Gröbner d'un idéal* $\mathcal{I}$ *de* $\mathbb{K}[\mathrm{X}]$.

1. *Si* G *est minimale alors* $\mathrm{card}(\mathrm{G}) \leqslant \mathrm{card}(\mathrm{G}')$.
2. *Si* G *et* G′ *sont toutes deux minimales alors* $\mathrm{card}(\mathrm{G}) = \mathrm{card}(\mathrm{G}')$.

Démonstration. *Soient* G *et* G′ *deux bases de Gröbner minimales d'un idéal* $\mathcal{I}$.
Soit $\mathrm{g} \in \mathrm{G}$. *Alors, il existe* $(\mathrm{g}', \mathrm{X}^\alpha) \in \mathrm{G}' \times \mathbb{M}$ *tel que* $\mathrm{LM}(\mathrm{g}) = \mathrm{X}^\alpha \mathrm{LM}(\mathrm{g}')$ $(\star)$.
Supposons qu'il existe deux couples $(\mathrm{g}'_1, X^{\alpha_1})$ *et* $(\mathrm{g}'_2, X^{\alpha_2})$ *qui vérifient la relation* $(\star)$ *; c'est à dire* $\mathrm{LM}(g) = X^{\alpha_1}\mathrm{LM}(g'_1) = X^{\alpha_2}\mathrm{LM}(\mathrm{g}'_2)$.
$\mathrm{g}'_1 \neq \mathrm{g}'_2 \Rightarrow \mathrm{g}'_1 - \mathrm{g}'_2 \in \mathcal{I}\backslash\{0\}$. *Donc, il existe* $(\mathrm{g}_1, \mathrm{X}^\beta) \in \mathrm{G} \times \mathbb{M}$ *vérifiant la relation* $\mathrm{LM}(\mathrm{g}'_1 - \mathrm{g}'_2) = \mathrm{X}^\beta \mathrm{LM}(\mathrm{g}_1)$. *Or* $\mathrm{LM}(\mathrm{g}'_1 - \mathrm{g}'_2) = \max\{\mathrm{LM}(\mathrm{g}'_1), \mathrm{LM}(\mathrm{g}'_2)\}$.

$$\begin{cases} \mathrm{LM}(g'_1) = X^{\beta}\mathrm{LM}(g_1) \\ \textit{ou} \\ \mathrm{LM}(g'_2) = X^{\beta}\mathrm{LM}(g_1) \end{cases} \Rightarrow \mathrm{LM}(g) = \begin{cases} X^{\alpha_1}X^{\beta}\mathrm{LM}(g_1) \\ \textit{ou} \\ X^{\alpha_2}X^{\beta}\mathrm{LM}(g_1) \end{cases}$$

$\mathrm{LM}(g_1)$ *divise* $\mathrm{LM}(g)$ *; ce qui contredit la minimalité de* G*.*
Donc $g'_1 = g'_2$*.*
De façon similaire, on montre que pour tout $g' \in G'$*, il existe un unique* $g \in G$ *dont le monôme dominant divise celui de* g'*. Il y a donc une bijection entre* G *et* G'*. D'où* $\mathrm{card}(G) = \mathrm{card}(G')$*.* □

En somme, le cardinal d'une base de Gröbner minimale d'un idéal est le plus petit nombre d'éléments contenu dans une base de Gröbner de cet idéal. De plus, l'existence d'une base de Gröbner minimale est prouvée dans ce qui suit.

I - 3 - c Bases de Gröbner réduites

Définition I - 3.6. *Une base de Gröbner* G *est dite* ***réduite*** *si pour tout* $g \in G$*, on a :*

1. $\mathrm{LC}(g) = 1$ *;*
2. g *est irréductible modulo* $G\backslash\{g\}$*.*

Exemple I - 3.7. $G = \{Y^2 + Y, X + Y + 1\}$ *est une base de Gröbner réduite de* $\langle G\rangle$ *relativement à* $\prec_{\mathrm{lex}}$ *avec* $Z \prec X \prec Y$*.*

On peut remarquer que toute base de Gröbner réduite est aussi minimale. Cependant, s'il est possible qu'un idéal admette plusieurs bases de Gröbner minimales, il n'en est pas ainsi pour les bases de Gröbner réduites. On a la propriété suivante.

Propriété I.1. *Tout idéal* $\mathcal{I}$ $\mathbb{K}[X]$ *admet une et une seule base de Gröbner réduite.*

Démonstration.
• *Existence*
Soit $\mathcal{I}$ *un idéal et* G*, une base de Gröbner minimale de* $\mathcal{I}$*.*
On pose $G' = \{\mathrm{NF}(g, G\backslash\{g\}), g \in G\}$*. Alors* $\mathrm{LM}(G') = \mathrm{LM}(G)$*. Ainsi,*

$$\langle \mathrm{LM}(\mathcal{I})\rangle = \langle \mathrm{LM}(G)\rangle = \langle \mathrm{LM}(G')\rangle. \quad (1)$$

Montrons que $\langle G\rangle = \langle G'\rangle$.
L'inclusion $\langle G'\rangle \subseteq \langle G\rangle$ *est évidente.*
Soit $f \in \langle G\rangle$. *Il existe* $g \in G$ *tel que* $LM(g)$ *divise* $LM(f)$. *Puisque* $LM(G') = LM(G)$, *il existe* $g' \in G'$ *tel que* $LM(g')$ *divise* $LM(f)$. *On réduit* f *par* g'. *On obtient* $f \xrightarrow{g'} f_1$. *De même* $f_1 \in \langle G\rangle$ *entraîne qu'il existe* $g'_1 \in G'$ *tel que* $LM(g'_1)$ *divise* $LM(f_1)$. *Enréduisant* f_1 *par* g'_1, *on a* $f_1 \xrightarrow{g'_1} f_2$.
En continuant cette réduction, il se crée la suite strictement décroissante $LM(f_1) \succ LM(f_2) \succ ... \succ LM(f_i) \succ ...$. *Comme toute suite strictement décroissante de monôme est stationnaire, il existe un entier* m *tel que* $f_i = 0\ \forall i \geqslant m$. *Il s'en suit que* $f \in \langle G'\rangle$. *Par suite,* $\langle G\rangle \subseteq \langle G'\rangle$. *Donc* $\langle G\rangle = \langle G'\rangle$ (2)
Les relations (1) *et* (2) *entrainent que* G' *est une base de Gröbner de* $\langle G\rangle$.
Par construction de G', $NF(g', G') = g'$ *pour tout* $g' \in G'$.
• *Unicité*
Supposons que $\mathcal{I}$ *admet deux bases de Gröbner réduites distinctes* G *et* G'.
Remarquons que toute base de Gröbner réduite est une base de Gröbner minimale.
Supposons qu'il existe $g \in G\backslash G'$. *Alors, il existe un unique* $g' \in G'$ *tel que* $LM(g') = LM(g)$.
$g \neq g' \Rightarrow g - g' \neq 0$ *et* $LM(g - g') \in Supp(g - LT(g)) \bigcup Supp(g' - LT(g'))$.
$g - g' \in \mathcal{I} \Rightarrow LM(g - g') \in \langle LM(G)\rangle = \langle LM(G')\rangle$.
Si $LM(g - g') \in Supp(g - LT(g))$ *alors* $Supp(g - LT(g)) \bigcap \langle LM(G)\rangle \neq \varnothing$. *Ceci implique qu'il existe un monôme de* g *qui est réductible modulo* G. *Ainsi,* $g \neq NF(g, G\backslash\{g\})$ *; ce qui est absurde. On en déduit que* $LM(g - g') \notin Supp(g - LT(g))$.
De même, $LM(g - g') \notin Supp(g' - LT(g'))$. *D'où* $g - g' = 0$ *; ie* $g = g'$. *Ainsi,* $G\backslash G' = \varnothing$.
De façon analogue, on montre que $G'\backslash G = \varnothing$. *Le résultat en découle.* □

On dispose également d'une procédure permettant de déterminer l'unique base de Gröbner réduite d'un idéal.

Exemple I - 3.8. *On veut trouver l'unique base de Gröbner réduite de l'idéal engendré par l'ensemble* $G = \{g_1 = X^2Y - 1,\ g_2 = XY^2 - X,\ g_3 = X - Y,\ g_4 = Y - 1\}$.

Algorithme 4 : Construction de base de Gröbner réduite

Entrée : G : base de Gröbner minimale

Sortie : G' : l'unique Base de Gröbner réduite de $\langle G \rangle$

```
G ← ∅;
Tant que G_1 ≠ G' Faire
    Prendre un élément g ∈ G;
    G_1 ← G_1 ∪ {g};
    G' ← G' ∪ {NF(g, G \ {g})}
Fin
Retourner G'
```

On a précédemment vu que $G' = \{g_3 = X - Y,\ g_4 = Y - 1\}$ *est une base de Gröbner minimale de* $\langle G \rangle$. *On peut appliquer l'algorithme précédent à* G'. *On obtient :*
$G" = \{NF(g_4, \{g_3\}), NF(g_3, \{g_4\})\} = \{X - 1, Y - 1\}$.
L'ensemble $G" = \{X - 1, Y - 1\}$ *est l'unique base de Gröbner réduite de* $\langle G \rangle$.

II Bases de Gröbner non commutatives sur un corps

Les bases de Gröbner non commuatatives sont une généralisation des bases de Gröbner commutatives. Comme dans le cas de toute généralisation, des notions peuvent être redéfinies et des propriétés peuvent être perdues. On verra notamment que la non commutativité entraîne la perte partielle de l'unicité du S-polynôme et la finitude de l'algorithme de Buchberger.
Cette section est articulée de la même manière que la précédente et à chaque notion (algorithme, théorème,...), on donnera son analogue. Les articles [9, 7, 6, 46, 48] de T. Mora sont les principales références de cette section.

II - 1 Notations

Etant donnés un corps commutatif $\mathbb{K}$ et un alphabet fini $X = \{X_1, X_2, ..., X_n\}$,
— l'anneau $\mathbb{K}\langle X_1, X_2, ..., X_n \rangle$ des polynômes non commuatifs est noté $\mathbb{K}\langle X \rangle$;
— l'ensemble $\{X_{i_1} X_{i_2} ... X_{i_t}, X_{i_j} \in X\}$ des monômes est noté $\mathbb{M}$;
— pour tout polynôme f, le support de f est noté Supp(f).

II - 2 Concepts de base

II - 2 - a Degré d'un monôme et degré d'un polynôme

Définition II - 2.1.

— *Soit* $u_i = X_{i_1}X_{i_2}...X_{i_t} \in \mathbb{M}$. *L'entier naturel* t *est appelé degré de* u_i. *On note* $t = \deg(u_i) = \deg(X_{i_1}X_{i_2}...X_{i_t})$.

— *Le degré d'un polynôme* f *est le maximum des degrés de ses monômes.*

II - 2 - b Relation de divisibilté entre monômes

Définition II - 2.2. *On dit qu'un monôme* u *divise un monôme* v *s'il existe* $(t, w) \in \mathbb{M} \times \mathbb{M}$ *tel que* $v = tuw$.

II - 2 - c Ordre monomial

Définition II - 2.3. *Un ordre* $\prec$ *sur* $\mathbb{M}$ *est appelé ordre monomial si :*

— $\prec$ *est total ;*

— $\prec$ *est un bon ordre ;*

— $\prec$ *est compatible avec la multiplication ; c'est à dire, pour tous monômes* t, u, v, w,

$u \prec v \Rightarrow tuw \prec tvw$.

Exemple II - 2.1. *L'ordre lexicographique gradué défini par*

$$u \prec_{grlex} v \Leftrightarrow \begin{cases} \deg(u) < \deg(v) \\ \deg(u) = \deg(v) \text{ et } u \prec_{lex} v \end{cases}$$

est un ordre monomial. Par contre l'ordre lexicographique n'est pas un ordre monomial.

Remarque II.1. *Etant donné un ordre monomial, les définitions et notations de plus petit multiple commun, monôme dominant, coefficient dominant, terme dominant restent les mêmes que dans la Section* 1.

II - 2 - d Algorithme de réduction

Définition II - 2.4. *Soit* $f, g \in \mathbb{K}\langle X\rangle$, $G \subset \mathbb{K}\langle X\rangle$ *et* " $\prec$ " *un ordre monomial.*

• f *est dit* ***réductible*** *modulo* g *(ou* g*-réductible) s'il existe un triplet* $(u, v, w) \in \mathrm{Supp}(f) \times \mathbb{M} \times \mathbb{M}$ *tel que* $u = vLM(g)w$. *Dans ce cas, le polynôme* $h = f - \frac{a_\alpha}{LC(g)}vgw$, *où* $a_\alpha \neq 0$ *étant le coefficient du monôme* u *dans* f, *est appelé réduit de* f *modulo* g *et est noté :* $f \xrightarrow{g} h$.

Si $u = LM(f)$, *on dit que* f *est* ***top-réductible*** *modulo* g *et* h *est appelé le* ***top-réduit*** *de* f *modulo* g.

• *Les notions de réduction modulo un ensemble, de réduction totale restent les mêmes que dans la section* 1.

Comme dans la première setion, la réduction conduit à l'algorithme suivant.

Algorithme 5 : Réduction Totale

Entrée : $(f, G, \prec)$
Sortie : r : irréductible modulo G

```
1  r ← 0;
2  Tant que f ≠ 0 Faire
3  |  Si LM(f) = uLM(g)v, u, v ∈ M, g ∈ G Alors
4  |  |  f ← f − (LC(f)/LC(g))ugv
5  |  Sinon
6  |  |  r ← r + LT(f);
7  |  |  f ← f − LT(f);
8  |  FinSi
9  Fin
10 Retourner r
```

Théorème II.1. *L'algorithme de réduction se termine.*

De même, le théorème suivant est une conséquence de l'algorithme de réduction totale.

Théorème II.2. *Soit* $G \subset \mathbb{K}\langle X\rangle$ *et* $f \in \mathbb{K}\langle X\rangle$. *Il existe* $(g, r) \in \langle G\rangle \times G_r$ *tel que* $f = g + r$.

Remarque II.2. *La décomposition d'un polynôme* f *sous la forme* $\mathrm{f} = \mathrm{g} + \mathrm{r}$, *où* $(\mathrm{g}, \mathrm{r}) \in \langle \mathrm{G} \rangle \times \mathrm{G}_{\mathrm{r}}$ *n'est pas nécessairement unique.*

II - 3 Bases de Gröbner non commutatives sur un corps

II - 3 - a Bases de Gröbner non commutatives sur un corps

Définition II - 3.1. *Un idéal est dit monomial s'il peut être engendré par des monômes.*

Définition II - 3.2. *Soit* $G \subset \mathbb{K}\langle \mathrm{X} \rangle$, $\mathcal{I} = \langle G \rangle$ *et* " $\prec$ " *un ordre monomial. On dit que* G *est une base de Gröbner de* $\mathcal{I}$ *relativement à* $\prec$ *si* $\langle \mathrm{LM(G)} \rangle = \langle \mathrm{LM}(\mathcal{I}) \rangle$.

Théorème II.3. *Si* G *est une base de Gröbner alors pour tout polynôme* f *il existe un unique couple* $(\mathrm{g}, \mathrm{r}) \in \langle \mathrm{G} \rangle \times \mathrm{G}_{\mathrm{r}}$ *tel que* $\mathrm{f} = \mathrm{g} + \mathrm{r}$.
Le polynôme r *est appelé* ***forme normale*** *de* f *modulo* G. *On note* $\mathrm{r} = \mathrm{NF}(\mathrm{f}, \mathrm{G}, \prec)$ *ou* $\mathrm{r} = \mathrm{NF(f)}$ *s'il n'y aucune ambiguïté sur l'ensemble* G *et l'ordre monomial* $\prec$.

La notion de composition définie ci-après joue exactement le même rôle que celle de S-polynôme dans $\mathbb{K}[\mathrm{X}]$. Plus précisément, les compositions permettent de caractériser les bases de Gröbner. Cependant, contrairement au cas des S-polynômes, ni l'existence ni l'unicité de compositions entre deux polynômes ne sont garanties.

Définition II - 3.3. *Soient* f *et* g *deux polynômes.*

1. *S'il existe* $\mathrm{u}, \mathrm{v} \in \mathbb{M}$ *tels que* $\mathrm{LM(f)u} = \mathrm{vLM(g)}$ *et* $\deg(\mathrm{LM(f)}) > \deg(\mathrm{v})$ (*ou de façon équivalente* $\deg(\mathrm{LM(f)}) + \deg(\mathrm{LM(g)}) > \deg(\mathrm{u}) + \deg(\mathrm{v})$) *alors on appelle* ***composition d'intersection*** *des polynômes* f *et* g *relativement à* $\mathrm{w} = \mathrm{LM(f)u} = \mathrm{vLM(g)}$ *le polynôme* $\frac{\mathrm{f}}{\mathrm{LC(f)}}\mathrm{u} - \mathrm{v}\frac{\mathrm{g}}{\mathrm{LC(g)}}$. *On le note* $(\mathrm{f}, \mathrm{g})_{\mathrm{w}}$.
2. *S'il existe* $\mathrm{u}, \mathrm{v} \in \mathbb{M}$ *tels que* $\mathrm{LM(f)} = \mathrm{uLM(g)v}$ *alors on appelle* ***composition d'inclusion*** *des polynômes* f *et* g *relativement à* $\mathrm{w} = \mathrm{LM(f)} = \mathrm{uLM(g)v}$, *le polynôme* $\frac{\mathrm{f}}{\mathrm{LC(f)}} - \mathrm{u}\frac{\mathrm{g}}{\mathrm{LC(g)}}\mathrm{v}$. *Il est également noté* $(\mathrm{f}, \mathrm{g})_{\mathrm{w}}$.

Dans les deux cas, l'ensemble des composotions entre f *et* g *est noté* $\mathrm{Comp(f, g)}$.

Calculées en fonction des monômes dominants, les compositions dépendent de l'ordre monomial choisi. Cependant, on a la proporiété suivante.

Remarque II.3. *Pour toute paire* $\mathrm{f}, \mathrm{g} \in \mathbb{K}\langle \mathrm{X} \rangle$*, on a :*

1. $\mathrm{Comp}(\mathrm{f}, \mathrm{f})$ *n'est pas nécessairement égal à* $\{0\}$ *;*
2. $\mathrm{Comp}(\mathrm{f}, \mathrm{g})$ *peut être vide ou admettre plus d'un élément ;*
3. *si* $\mathrm{Comp}(\mathrm{f}, \mathrm{g}) \neq \varnothing$ *alors* $\mathrm{LM}[(\mathrm{f}, \mathrm{g})_{\mathrm{w}}] \prec \mathrm{LCM}[\mathrm{LM}(\mathrm{f}), \mathrm{LM}(\mathrm{g})]$ *pour tout* $(\mathrm{f}, \mathrm{g})_{\mathrm{w}} \in \mathrm{Comp}(\mathrm{f}, \mathrm{g})$.

Exemple II - 3.1.

1. $\mathrm{X} = \{\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3\}$, $\mathrm{X}_1 \succ \mathrm{X}_2 \succ \mathrm{X}_3$, $\prec$ *: l'ordre lexicographique gradué,* $\mathbb{K} = \mathbb{Q}$
   $\mathrm{f} = \mathrm{X}_1\mathrm{X}_2 + \mathrm{X}_2^2 + \mathrm{X}_1\mathrm{X}_3^3,\ \mathrm{g} = \mathrm{X}_1 + \mathrm{X}_2 + \mathrm{X}_3^2$
   $\mathrm{LM}(\mathrm{f}) = \mathrm{X}_1\mathrm{X}_3^3,\ \mathrm{LM}(\mathrm{g}) = \mathrm{X}_3^2$
   $\mathrm{w} = \mathrm{X}_1\mathrm{X}_3^3 = \mathrm{LM}(\mathrm{f}) = \mathrm{X}_1\mathrm{LM}(\mathrm{g})\mathrm{X}_3.$
   On a alors $(\mathrm{f}, \mathrm{g})_{\mathrm{w}} = \mathrm{f} - \mathrm{X}_1\mathrm{g}\mathrm{X}_3$
   $= -\mathrm{X}_1^2\mathrm{X}_3 - \mathrm{X}_1\mathrm{X}_2\mathrm{X}_3 + \mathrm{X}_1\mathrm{X}_2 + \mathrm{X}_2^2$
   est une composition d'inclusion de f *et* g *relativement à* w.
2. $\mathrm{X} = \{\mathrm{X}_1, \mathrm{X}_2, \mathrm{X}_3\}$, $\mathrm{X}_1 \succ \mathrm{X}_2 \succ \mathrm{X}_3$, $\prec$ *: l'ordre lexicographique gradué,* $\mathbb{K} = \mathbb{Q}$
   $\mathrm{f} = \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 + \mathrm{X}_2\mathrm{X}_3,\ \mathrm{g} = \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2 + \mathrm{X}_3^2\mathrm{X}_1$
   $\mathrm{LM}(\mathrm{f}) = \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1,\ \mathrm{LM}(\mathrm{g}) = \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2$
   $\mathrm{w}_1 = \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2 = \mathrm{LM}(\mathrm{f})\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2 = \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{LM}(\mathrm{g})$
   $\deg(\mathrm{LM}(\mathrm{f})) = 6 > 4 = \deg(\mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3).$
   $\Rightarrow (\mathrm{f}, \mathrm{g})_{\mathrm{w}_1} = \mathrm{f}\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2 - \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{g}$
   $= \mathrm{X}_2\mathrm{X}_3^2\mathrm{X}_2\mathrm{X}_1^2 - \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3^3\mathrm{X}_1$
   $\mathrm{w}_2 = \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^3\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 = \mathrm{LM}(\mathrm{g})\mathrm{X}_1\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 = \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1\mathrm{LM}(\mathrm{f})$
   $\deg(\mathrm{LM}(\mathrm{g})) = 6 > 5 = \deg(\mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1)$
   $\Rightarrow (\mathrm{g}, \mathrm{f})_{\mathrm{w}_2} = \mathrm{g}\mathrm{X}_1\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 - \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1\mathrm{f}$
   $= \mathrm{X}_3^2\mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 - \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1\mathrm{X}_2\mathrm{X}_3$
   $\mathrm{w}_3 = \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 = \mathrm{LM}(\mathrm{g})\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 = \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{LM}(\mathrm{f})$
   $\deg(\mathrm{LM}(\mathrm{g})) = 6 > 4 = \deg(\mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2)$
   $\Rightarrow (\mathrm{g}, \mathrm{f})_{\mathrm{w}_3} = \mathrm{g}\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 - \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2\mathrm{f}$
   $= \mathrm{X}_3^2\mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2 - \mathrm{X}_2\mathrm{X}_1\mathrm{X}_3\mathrm{X}_2^2\mathrm{X}_3$
   $\mathrm{w}_4 = \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 = \mathrm{LM}(\mathrm{f})\mathrm{X}_1\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{X}_1 = \mathrm{X}_1^2\mathrm{X}_2\mathrm{X}_3\mathrm{X}_2\mathrm{LM}(\mathrm{f})$

$$\deg(\mathrm{LM}(\mathrm{f})) = 6 > 5\deg(\mathrm{X_1X_2X_3X_2X_1})$$
$$\Rightarrow (\mathrm{f},\mathrm{f})_{\mathrm{w_4}} = \mathrm{fX_1X_2X_3X_2X_1} - \mathrm{X_1^2X_2X_3X_2f}$$
$$= \mathrm{X_2X_3X_1X_2X_3X_2X_1} - \mathrm{X_1^2X_2X_3X_2^2X_3}$$

Le théorème suivant est l'équivalent du critère de Buchberger.

Théorème II.4 (Lemme de composition)**.** *Soient* $\mathrm{G} \subset \mathbb{K}\langle \mathrm{X}\rangle$ *et* $\prec$ *un ordre monomial. Les assertions suivantes sont équivalentes.*

1. G *est une base de Gröbner* $\langle \mathrm{G}\rangle$*.*
2. *Toutes les compositions définies dans* G *sont réduites à zéro modulo* G*.*

Démonstration. *Voir [7]*

Exemple II - 3.2. *Considérons l'ordre alphabétique* $\mathrm{X_1} \succ \mathrm{X_2} \succ \mathrm{X_3}$ *et l'ordre lexicographique gradué.*
Alors, $\mathrm{G} = \{\mathrm{g_1} = \mathrm{X_1^2X_3} + \mathrm{X_2X_1}, \mathrm{g_2} = \mathrm{X_3^3} - \mathrm{X_2^2}, \mathrm{g_3} = \mathrm{X_1^2X_2^2} + \mathrm{X_2X_1X_3^2}, \mathrm{g_4} = \mathrm{X_2^2X_3} - \mathrm{X_3X_2^2}\}$ *est une base de Gröbner de* $\mathcal{I} = \langle \mathrm{G}\rangle$*.*
En effet, les compositions possibles dans G *sont les suivantes :*
$(\mathrm{g_1},\mathrm{g_2})_{\mathrm{w_1}},\ (\mathrm{g_4},\mathrm{g_2})_{\mathrm{w_2}},\ (\mathrm{g_3},\mathrm{g_4})_{\mathrm{w_3}},\ (\mathrm{g_2},\mathrm{g_2})_{\mathrm{w_4}},\ (\mathrm{g_2},\mathrm{g_2})_{\mathrm{w_5}}$ *où*
$\mathrm{w_1} = \mathrm{LM}(\mathrm{g_1})\mathrm{X_3^2} = \mathrm{X_1^2LM}(\mathrm{g_2}) = \mathrm{X_1^2X_3^3},$
$\mathrm{w_2} = \mathrm{LM}(\mathrm{g_4})\mathrm{X_3^2} = \mathrm{X_2^2LM}(\mathrm{g_2}) = \mathrm{X_2^2X_3^3},$
$\mathrm{w_3} = \mathrm{LM}(\mathrm{g_3})\mathrm{X_3} = \mathrm{X_1^2LM}(\mathrm{g_4}) = \mathrm{X_1^2X_2^2X_3},$
$\mathrm{w_4} = \mathrm{LM}(\mathrm{g_2})\mathrm{X_3} = \mathrm{X_3LM}(\mathrm{g_2}) = \mathrm{X_3^4},$
$\mathrm{w_5} = \mathrm{LM}(\mathrm{g_2})\mathrm{X_3^2} = \mathrm{X_3^2LM}(\mathrm{g_2}) = \mathrm{X_3^5}.$

- $(\mathrm{g_1},\mathrm{g_2})_{\mathrm{w_1}} = \mathrm{g_1X_3^2} - \mathrm{X_1^2g_2}$
$= \mathrm{X_1^2X_3^3} + \mathrm{X_2X_1X_3^2} - \mathrm{X_1^2X_3^3} + \mathrm{X_1^2X_2^2}$
$= \mathrm{X_1^2X_2^2} + \mathrm{X_2X_1X_3^2} \xrightarrow{\mathrm{g_3}} \mathrm{X_1^2X_2^2} + \mathrm{X_2X_1X_3^2} - \mathrm{g_3} = 0.$

- $(\mathrm{g_4},\mathrm{g_2})_{\mathrm{w_2}} = \mathrm{g_4X_3^2} - \mathrm{X_2^2g_2}$
$= \mathrm{X_2^2X_3^3} - \mathrm{X_3X_2^2X_3^2} - \mathrm{X_2^2X_3^3} + \mathrm{X_2^4}$
$= \mathrm{X_2^4} - \mathrm{X_3X_2^2X_3^2} = \mathrm{f_0}$

$\mathrm{f_0} \xrightarrow{\mathrm{g_4}} \mathrm{X_2^4} - \mathrm{X_3X_2^2X_3^2} + \mathrm{X_3g_4X_3} = \mathrm{X_2^4} - \mathrm{X_3X_2^2X_3^2} + \mathrm{X_3X_2^2X_3^2} - \mathrm{X_3^2X_2^2X_3} = \mathrm{f_1}$

$f_1 \xrightarrow{g_4} X_2^4 - X_3X_2^2X_3^2 + X_3g_4X_3 = yX_2^4 - X_3^2X_2^2X_3 = f_2$
$f_2 \xrightarrow{g_4} X_2^4 - X_3^2X_2^2X_3 + X_3^2g_4 = X_2^4 - X_3^2X_2^2X_3 + X_3^2X_2^2X_3 - X_3^3X_2^2 = X_2^4 - X_3^3X_2^2 = f_3$
$f_3 \xrightarrow{g_2} X_2^4 - X_3^3X_2^2 + g_2X_2^2 = X_2^4 - X_3^3X_2^2 + X_3^3X_2^2 - X_2^4 = 0.$

- $(g_3, g_4)_{w_3} = g_3X_3 - X_1^2g_4$
$= X_1^2X_2^2X_3 + X_2X_1X_3^3 - X_1^2X_2^2X_3 + X_1^2X_3X_2^2$
$= X_1^2X_3X_2^2 + X_2X_1X_3^3 = h_1$

$h_1 \xrightarrow{g_1} X_1^2X_3X_2^2 + X_2X_1X_3^3 - g_1X_2^2 = X_2X_1X_3^3 - X_2X_1X_2^2 = h_2$
$h_2 \xrightarrow{g_2} X_2X_1X_3^3 - X_2X_1X_2^2 - X_2X_1g_2 = X_2X_1X_3^3 - X_2X_1X_2^2 - X_2X_1X_3^3 + X_2X_1X_2^2 = 0.$

- $(g_2, g_2)_{w_4} = g_2X_3 - X_3g_2$
$= X_3^4 - X_2^2X_3 - X_3^4 + X_3X_2^2$
$= X_3X_2^2 - X_2^2X_3 = p_1$

$p_1 \xrightarrow{g_4} X_3X_2^2 - X_2^2X_3 + g_4 = X_3X_2^2 - X_2^2X_3 + X_2^2X_3 - X_3X_2^2 = 0.$

- $(g_2, g_2)_{w_5} = g_2X_3^2 - X_3^2g_2$
$= X_3^5 - X_2^2X_3^2 - X_3^5 + X_3^2X_2^2$
$= X_3^2X_2^2 - X_2^2X_3^2 = q_1$

$q_1 \xrightarrow{g_4} X_3^2X_2^2 - X_2^2X_3^2 + g_4X_3 = X_3^2X_2^2 - X_3X_2^2X_3 = X_3^2X_2^2 - X_3X_2^2X_3 = q_2$
$q_2 \xrightarrow{g_4} X_3^2X_2^2 - X_3X_2^2X_3 + X_3g_4 = X_3^2X_2^2 - X_3X_2^2X_3 + X_3X_2^2X_3 - X_3^2X_2^2 = 0.$

Toutes les compositions sont réduites à zéro modulo G.

Proposition II - 3.1. *Tout idéal* $\mathcal{I}$ $\mathbb{K}[X]$ *admet une base Gröbner* (*finie ou non*).

L'idéal lui-même est une base de Gröbner. De plus, il existe une version non commutative de l'algorithme de Buchberger. Cependant, l'existence d'une partie génératrice finie (Théorème de la base de Hilbert) n'est pas toujours garantie. Ainsi, pour pouvoir utiliser cet algorithme, on se restreint aux idéaux admettant au moins une partie génératrice finie. Egalement, on verra avec un exemple classique, que l'existence d'une partie génératrice finie n'entraîne pas forcément l'existence d'une base de Gröbner finie. Autrement dit, l'algorithme de Buchberger ne se termine pas

toujours dans l'anneau $\mathbb{K}\langle X\rangle$ des polynômes non commutatifs.

Algorithme 6 : Algorithme de Buchberger

Entrée : $(G = \{g_1, ..., g_m\}, \prec)$

Sortie : G^{comp}

```
G^comp ← G;
Tant que il existe une nouvelle composition c dans G^comp Faire
    Si Réduction(c, G^comp, ≺) ≠ 0 Alors
        G^comp ← G^comp ∪ {Réduction(c, G^comp, ≺)};
Fin
Retourner G^comp
```

Exemple II - 3.3. *Soit* $G = \{g_1 = Z^3XZ + Y^2X,\ g_2 = YZXZ + X^2Y\}$.
Déterminons une base de Gröbner de l'idéal $\mathcal{I} = \langle G\rangle$ *pour l'ordre lexicographique gradué induit par* $Z \prec Y \prec X$.
Déroulement de l'algorithme :
$G^{comp} \leftarrow G$
Première itération :
$w_1 = YZXZ^3XZ = LM(g_2) = YZXLM(g_1)$
$(g_2, g_1)_{w_1} = g_2Z^2XZ - YZXg_1$
$= (YZXZ + X^2Y)Z^2XZ - YZX(Z^3XZ + Y^2X)$
$= X^2YZ^2XZ - YZXY^2X$ (*irréductible modulo* G^{comp})
$G^{comp} \leftarrow \{g_1,\ g_2,\ g_3 = X^2YZ^2XZ - YZXY^2X\}$

Deuxième itération :
$w_2 = Z^3XZ^3XZ = LM(g_1)Z^2XZ = Z^3XLM(g_1),\ \deg(LM(g_1)) = 5 > \deg(Z^3X) = 4$
$(g_1, g_1)_{w_2} = g_1Z^2XZ - Z^3Xg_1$
$= (Z^3XZ + Y^2X)Z^2XZ - Z^3X(Z^3XZ + Y^2X)$
$= Y^2XZ^2XZ - Z^3XY^2X$ (*irréductible modulo* G^{comp})
$G^{comp} \leftarrow \{g_1,\ g_2,\ g_3,\ g_4 = Y^2XZ^2XZ - Z^3XY^2X\}$

Troisième itération :

$w_3 = X^2YZ^2XZ^3XZ = LM(g_3)Z^2XZ = X^2YZ^2XLM(g_1)$,

$\deg(LM(g_3)) = 7 > \deg(X^2YZ^2) = 5$

$(g_3, g_1)_{w_3} = g_3Z^2XZ - X^2YZ^2Xg_1$

$= (X^2YZ^2XZ - YZXY^2X)Z^2XZ - X^2YZ(Z^3XZ + Y^2X)$

$= -YZXY^2XZ^2XZ - X^2YZ^2XY^2X \xrightarrow{g_4} -YZXZ^3XY^2X - X^2YZ^2XY^2X \xrightarrow{g_2} 0$

Quatrième itération :

$w_4 = Y^2XZ^2XZ^3XZ = LM(g_4)Z^2XZ = Y^2XZ^2XLM(g_1)$

$\deg(LM(g_4)) = 7 > \deg(Y^2XZ^2) = 5$

$(g_4, g_1)_{w_4} = g_4Z^2XZ - Y^2XZ^2Xg_1$

$= (Y^2XZ^2XZ - Z^3XY^2X)Z^2XZ - Y^2XZ^2X(Z^3XZ + Y^2X)$

$= -Z^3XY^2XZ^2XZ - Y^2XZ^2XY^2X \xrightarrow{g_4} -Z^3XZ^3XY^2X - Y^2XZ^2XY^2X \xrightarrow{g_1} 0$

G^{comp} *n'admet aucune nouvelle composition : la boucle s'arrête.*

Sortie : $G^{comp} = \{g_1,\ g_2,\ g_3,\ g_4\}$ *est une base de Gröbner* $\langle g_1, g_2\rangle$.

Exemple II - 3.4. *On considère l'ensemble* $G = \{g_1 = XYX - YX\}$ *et un ordre monomial quelconque.*

Déroulement de l'algorithme :

$G^{comp} \leftarrow G$

Première itération :

$w_1 = LM(g_1)YX = XYLM(g_1)),\ \deg(LM(g_1)) = 3 > 2 = \deg(XY)$

$(g_1, g_1)_{w_1} = g_1YX - XYg_1 = -YXYX + XY^2X \xrightarrow{g_1} XY^2X - Y^2X = g_2.$

$G^{comp} \leftarrow \{g_1, g_2\}$

Deuxième itération :

$w_2 = LM(g_1)Y^2X = XYLM(g_2)),\ \deg(LM(g_1)) = 3 > 2 = \deg(XY)$

$(g_1, g_2)_{w_2} = g_1Y^2X - XYg_2 = -YXY^2X + XY^3X \xrightarrow{g_2} XY^3X - Y^3X = g_3.$

$G^{comp} \leftarrow \{g_1, g_2, g_3\}$

Troisième itération :

$w_3 = LM(g_1)Y^3X = XYLM(g_3)),\ \deg(LM(g_1)) = 3 > 2 = \deg(XY)$

$(g_1, g_3)_{w_3} = g_1Y^3X - XYg_3 = -YXY^3X + XY^4X \xrightarrow{g_3} XY^4X - Y^4X = g_4.$

$G^{comp} \leftarrow \{g_1, g_2, g_3, g_4\}$
On constate que g_1 *est toujours composable avec l'élément* $g_n = XY^nX - Y^nX$ *généré lors de l'itération précédente.*
De plus, à la n^{ieme} *itération, on a toujours :*
$(g_1, g_n)_{w_n} = g_1Y^nX - XYg_n = -YXY^nX + XY^{n+1}X \xrightarrow{g_n} XY^{n+1}X - Y^{n+1}X = g_{n+1}$.
On en déduit que la boucle ne s'arrête jamais. Ainsi, la base de Gröbner en construction est infinie.

L'existence d'idéaux n'admettant aucune base de Gröbner finie est la principale différence entre lecas commutatif et le cas non commuatif.

II - 3 - b Bases de Gröbner réduites et bases de Gröbner minimales

Les définitions et propriétés des notions de bases de Gröbner minimales et bases de Gröbner réduites restent inchangées par rapport à la Section 1.

III Bases de Gröbner sur un anneau

Dans cette section, on généralise à nouveau la notion de base de Gröbner en remplaçant le corps $\mathbb{K}$ par un anneau $\mathbb{A}$. Ainsi, la plupart des concepts de base (degré, ordre monomial, plus petit commun multiple,...) restent les mêmes que celles des sections précédentes. On introduit la divisibilité entre termes qui généralise celle définie entre monômes. Puis, on reprend la notion de réduction. Dans cette section, $\mathcal{R}$ désigne l'anneau :

— $\mathbb{A}[X] = \mathbb{A}[X_1, X_2, ..., X_n]$ si la multiplication entre monômes est commutative ;
— $\mathbb{A}\langle X\rangle = \mathbb{A}\langle X_1, X_2, ..., X_n\rangle$ sinon.

III - 1 Concepts de base

Définition III - 1.1.

— *Les notions de degré, de divisibilité entre monômes restent les mêmes que celles des sections précédentes.*

— *Soient* $(\alpha, \beta) \in \mathbb{A} \times \mathbb{A}$, $(\mathrm{u}, \mathrm{v}) \in \mathbb{M} \times \mathbb{M}$. *Le terme* $\alpha\mathrm{u}$ *divise le terme* $\beta\mathrm{v}$ *si* α *divise* β *dans* $\mathbb{A}$ *et* u *divise* v *dans* $\mathbb{M}$*; c'est à dire s'il existe un terme* $(\gamma, \mathrm{w}) \in \mathbb{A} \times \mathbb{M}$ *tel que* $\beta = \gamma\alpha$ *et* $\mathrm{v} = \mathrm{wu}$.

— *Un polynôme* f *est dit réductible modulo un polynôme* g *si un terme de* f *est divisible par le terme dominant de* g.

Si le terme dominant de f *est divisible par celui de* g*, on dit que* f *est top-réductible modulo* g.

Les définitions de réduction modulo un ensemble et de réduction totale restent inchangées.

Dans ce qui suit, on donne la version non commutative de l'algorithme de réduction totale.

Algorithme 7 : Réduction totale

Entrée : $(\mathrm{f}, \mathrm{G}, \prec)$
Sortie : r : irréductible modulo G

```
r ← 0;
Tant que f ≠ 0 Faire
    Si LT(f) = αuLT(g)v, u, v ∈ M, α ∈ A, g ∈ G Alors
        f ← f − αugv
    Sinon
        r ← r + LT(f);
        f ← f − LT(f);
    FinSi
Fin
Retourner r
```

III - 2 Bases de Gröbner sur un anneau

Le théorème de caractérisation des bases de Gröbner (critère de Buchberger ou lemme de composition) s'énonce différemment selon les spécificités des anneaux. Dans certains anneaux, on trouve des éléments dont aucun ne divise l'autre. C'est par exemple le cas de l'anneau $\mathbb{Z}$ dans lequel 2 ne divise pas 3 et 3 non plus ne divise pas 2. Dans d'autres anneaux, on trouve des diviseurs de zéro qui nécessitent une attention et un traitement particuliers. C'est l'exemple de $\frac{\mathbb{Z}}{6\mathbb{Z}}$ où $2\times 3 = 0$. Sur chaque type d'anneau, on donne des définitions équivalentes des notions de S-polynôme et composition suivant les particularités. Alors, pour contourner le problème, les chercheurs ont introduit de nouvelles classifications aux bases de Gröbner sur les anneaux : les bases de Gröbner fortes et les bases de Gröbner faibles.

Définition III - 2.1. *Soit* G *une base de Gröbner d'un idéal* $\mathcal{I}$ *de* $\mathbb{A}[\mathrm{X}]$*, où* $\mathbb{A}$ *est un anneau.*

1. G *est une base de Gröbner faible si* $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(\mathcal{I})\rangle$.
2. G *est une base de Gröbner forte si le terme dominant de tout élément de* $\mathcal{I}$ *est divisible par celui d'un élément de* G.

Remarque III.1.

— *Toute base de Gröbner forte est faible.*

— *Si* $\mathbb{A}$ *est un corps alors toute base de Gröbner faible est forte. Ceci est la raison pour laquelle dans le cas des corps on parle tout simplement de bases de Gröbner (sans aucune distiction). Cependant, il n'est pas nécessaire que l'anneau de base soit un corps pour qu'il y ait équivalence entre base de Gröbner forte et base de Gröbner faible. Les bases de Gröbner sur les anneaux de valuation en sont des exemples. On les étudiera en détails dans le Chapitre* 3.

Définition III - 2.2. *Un anneau* $\mathbb{A}$ *est dit de valuation si pour tous* $\mathrm{a}, \mathrm{b} \in \mathbb{A}$*,* a *divise* b *ou* b *divise* a.

Exemple III - 2.1. *Pour tout nombre premier* p *et tout entier naturel* n*, l'anneau quotient* $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ *est un anneau de valuation.*

Proposition III - 2.1. *Si* $\mathbb{A}$ *est un anneau de valuation alors toute base de Gröbner faible est forte.*

Dans tout le reste de cette section, $\mathcal{R} = \mathbb{A}[\mathrm{X}]$**, où** $\mathbb{A}$ **est un anneau de valuation.**

Définition III - 2.3.

1. *On suppose que* $\mathcal{R}$ *est commutatif. Soient* $\mathrm{f}, \mathrm{g} \in \mathcal{R}$ *et* $\mathrm{X}^\gamma = \mathrm{LCM}(\mathrm{LM}(\mathrm{f}), \mathrm{LM}(\mathrm{g}))$. *Le* S-polynôme *de* f *et* g *est défini par :*

$$\mathrm{S}-\mathrm{pol}(\mathrm{f},\mathrm{g}) = \begin{cases} \frac{\mathrm{X}^\gamma}{\mathrm{LM(f)}}\mathrm{f} - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)}\frac{\mathrm{X}^\gamma}{\mathrm{LM(g)}}\mathrm{g} \ \textit{si} \ \mathrm{LC(g)} \ \textit{divise} \ \mathrm{LC(f)} \\ \frac{\mathrm{LC(g)}}{\mathrm{LC(f)}}\frac{\mathrm{X}^\gamma}{\mathrm{LM(f)}}\mathrm{f} - \frac{\mathrm{X}^\gamma}{\mathrm{LM(g)}}\mathrm{g} \ \textit{sinon} \end{cases}$$

2. *On suppose que* $\mathcal{R}$ *est non nécessairement commutatif. Soient* $\mathrm{f}, \mathrm{g} \in \mathcal{R}$.

   (a) *S'il existe* $\mathrm{u}, \mathrm{v} \in \mathbb{M}$ *tels que* $\mathrm{LM(f)u} = \mathrm{vLM(g)}$ *et* $\deg(\mathrm{LM(f)}) > \deg(\mathrm{v})$ *alors la* ***composition d'intersection*** *des polynômes* f *et* g *relativement à* $\mathrm{w} = \mathrm{LM(f)u} = \mathrm{vLM(g)}$ *est définie par :*

$$\mathcal{O}(\mathrm{f},\mathrm{g})_\mathrm{w} = \begin{cases} \mathrm{fu} - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}}vg \ \textit{si} \ \mathrm{LC(g)} \ \textit{divise} \ \mathrm{LC(f)} \\ \frac{\mathrm{LC(g)}}{\mathrm{LC(f)}}\mathrm{fu} - \mathrm{vg} \ \textit{sinon} \end{cases}$$

   (b) *S'il existe* $\mathrm{u}, \mathrm{v} \in \mathbb{M}$ *tels que* $\mathrm{LM(f)} = \mathrm{uLM(g)v}$ *alors la* ***composition d'inclusion*** *des polynômes* f *et* g *relativement à* $\mathrm{w} = \mathrm{LM}(f) = \mathrm{uLM(g)v}$ *est donnée par :*

$$\mathcal{O}(\mathrm{f},\mathrm{g})_\mathrm{w} = \begin{cases} \mathrm{f} - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}ugv} \ \textit{si} \ \mathrm{LC(g)} \ \textit{divise} \ \mathrm{LC(f)} \\ \frac{\mathrm{LC(g)}}{\mathrm{LC(f)}}\mathrm{f} - \mathrm{ugv} \ \textit{sinon} \end{cases}$$

L'exemple suivant montre que dans le cas d'un anneau de valuation admettant des diviseurs de zéro, les S-polynômes (ou de compositions) ne suffisent pas à eux seuls pour caractériser les bases de Gröbner.

Exemple III - 2.2. *On donne* $\mathrm{G} = \{\mathrm{g}_1 = 4\mathrm{X}^2 + 2, \mathrm{g}_2 = 2\mathrm{X} + 3\} \subset \frac{\mathbb{Z}}{8\mathbb{Z}}[X]$ *et un ordre monomial quelconque.*

$\text{S-pol}(g_1, g_2) = g_1 - 2Xg_2 = 4X^2 + 2 - 4X^2 - 6X = -6X + 2 = 2X + 2 \xrightarrow{g_2} 0.$
Or $\text{LT}(2g_1) = 4 \notin \langle 2X \rangle = \langle \text{LT}(G) \rangle$. *On en déduit que* G *n'est pas une base de gröbner même si l'unique* S-polynôme *défini dans* G *est réduit à zéro modulo* G.

D'où la nécessité d'introduire une nouvelle notion.

Définition III - 2.4. *Soit* $f \in \mathcal{R}\backslash\{0\}$. *On définit :*

1. $\text{a-pol}^1(f) = a_1 f$ *avec* $\langle a_1 \rangle = \text{Ann}(\text{LC}(f))$
   $\text{a-pol}^i(f) = \text{a-pol}(\text{a-pol}^{i-1}(f)) = a_i(\text{a-pol}^{i-1}(f))$ *où* $\langle a_i \rangle = \text{Ann}(\text{LC}(\text{a-pol}^{i-1}(f))$.
2. $\text{A-pol}(f) = \{\text{a-pol}^i(f)\}$
3. $\text{A-pol}(G) = \bigcup_{f \in G} \text{A-pol}(f)$

Une caractérisation des bases de Gröbner est obtenue en rajoutant les a-polynômes aux S-polynômes.

Théorème III.1 (Critère de Buchberger/Lemme de composition)**.**

1. *On suppose que* $\mathcal{R}$ *est commutatif. Alors, un sous-ensemble* G *est une base de Gröbner de* $\langle G \rangle$ *si et seulement si tous les* S-polynômes *et tous les* a-polynômes *sont réduits à zéro modulo* G.
2. *On suppose que* $\mathcal{R}$ *n'est pas commutatif. Alors, un sous-ensemble* G *est une base de Gröbner* $\langle G \rangle$ *si et seulement si toutes les compositions et tous les* a-polynômes *sont réduits à zéro modulo* G.

Dans le Chapitre 3, on verra une preuve du théorème précédent et une version de l'algorithme de Buchberger adaptée aux anneaux de valuation noethériens.

Chapitre 2

Sur la finitude des bases de Gröbner non commutatives sur un corps

L'idéal $\mathcal{J} = \langle XYX - YX \rangle$ de l'anneau non commutatif $\mathbb{K}\langle X, Y \rangle$ des polynômes à coefficients dans un corps $\mathbb{K}$ et à indéterminées dans $\{X, Y\}$ n'admet aucune base de Gröbner finie relativement à un ordre monomial. En effet, pour tout entier n, le polynôme $f_n = XY^nX - Y^nX \in \mathcal{J}$ et son monôme dominant $LM(f_n) = XY^nX$ n'est divisible par aucun monôme dominant d'un autre polynôme de $\mathcal{J}$. Ainsi, toute base de Gröbner de $\mathcal{J}$ doit contenir f_n. Il s'en suit que toute base de Gröbner de $\mathcal{J}$ est infinie. Se pose alors la question de distinguer les idéaux non commutatifs ayant des bases de Gröbner finies de ceux n'en qui ont aucune.

L'expérience a montré que les bases de Gröbner non commutatives sont généralement infinies ; d'où la problématique de leur utilisation pratique dans la résolution de problèmes tels que le problème de l'appartenance d'un polynôme à un idéal. De plus, il n'est pas montré que l'existence d'une base de Gröbner finie pour un idéal non commutatif quelconque est un problème de décision. Autrement dit, il n'existe pas de critères généraux permettant de dire si un idéal quelconque donné admet ou non une base de Gröbner finie. Egalement, dans la littérature, les papiers traitant les bases de Gröbner non commutatives finies sont rares. Dans l'article [27] publié en 1998, D. Eisenbud, I. Peeva et B. Strumfels ont prouvé l'existence de bases de Gröbner non commutatives finies relativement à un ordre monomial spécifique pour des idéaux particuliers. Leur preuve est basée sur des applications entre les anneaux non com-

mutatifs et commutatifs de polynômes. Plus précisément, ils ont construit un homomorphisme surjectif γ de l'anneau non nécessairement commutatif $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ vers l'anneau commutatif $\mathbb{K}[x_1, x_2, ..., x_n]$ et ont montré que pour tout idéal $\mathcal{I}$ de $\mathbb{K}[x_1, x_2, ..., x_n]$, l'idéal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ admet une base de Gröbner finie. Nous avons travaillé sur la réciproque de leur résultat. Nous avons alors montré que sous certaines conditions, tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ admettant une base de Gröbner finie s'écrit sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ où $\mathcal{I}$ est un idéal de $\mathbb{K}[x_1, x_2, ..., x_n]$. Ce travail a fait l'objet du papier [24] "Diop Y., Sow D. *On finite noncommutative Gröbner bases. Algebra Colloquium* 27 : 3(2020) 381 − 388".
Ce chapitre est un exposé de ces deux travaux. Dans la première section, nous présentons le travail de Eisenbud de façon détaillée et dans la seconde, nous donnerons notre contribution à l'étude des bases de Gröbner non commutatives finies. Toutefois, signalons que nos notations diffèrent de celles de [27].

Dans tout le Chapitre, $X = \{X_1, X_2, ..., X_n\}$ et $x = \{x_1, x_2, ..., x_n\}$ sont deux alphabets finis. $\mathbb{K}\langle X\rangle$ et $\mathbb{K}[x]$ désignent respectivement l'anneau des polynômes non commutatif à indéterminées dans X et l'anneau des polynômes commutatif à indéterminées dans x et à coefficients dans le corps commutatif $\mathbb{K}$.

I Construction d'idéaux non commutatifs admettant des bases de Gröbner finies

Rappelons que la problématique est celle de la classification des idéaux non commuatifs en deux classes :

— ceux admettant des bases de Gröbner finies ;

— ceux n'admettant pas de base de Gröbner finie.

Plus précisément, on s'intéresse à la question suivante : existe-t-il des critères de caractérisation des idéaux de $\mathbb{K}\langle X\rangle$ admettant des bases de Gröbner finies ?
Une réponse partielle à cette question est donnée par Eisenbud, Peeva et Strumfels dans [27]. En effet, en construisant un homomorphisme surjectif $\gamma : \mathbb{K}\langle X\rangle \longrightarrow \mathbb{K}[x]$, ils ont prouvé que pour tout idéal $\mathcal{I}$ de $\mathbb{K}[x]$, l'idéal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ de $\mathbb{K}\langle X\rangle$ admet

une base de Gröbner finie relativement à un ordre monomial spécifique.

I - 1 Préliminaires

Les applications γ et δ construites ci-après jouent un rôle prépondérant dans la suite. La plupart des preuves font appel à elles.

Proposition I - 1.1. *Soient* $\mathrm{X} = \{\mathrm{X}_1, \mathrm{X}_2, ..., \mathrm{X}_\mathrm{n}\}$ *et* $\mathrm{x} = \{\mathrm{x}_1, \mathrm{x}_2, ..., \mathrm{x}_\mathrm{n}\}$ *deux alphabets totalement ordonnés. Soient* $\mathbb{K}\langle \mathrm{X}\rangle = \mathbb{K}\langle \mathrm{X}_1, \mathrm{X}_2, ..., \mathrm{X}_\mathrm{n}\rangle$ *et* $\mathbb{K}[\mathrm{x}] = \mathbb{K}[\mathrm{x}_1, \mathrm{x}_2, ...\mathrm{x}_\mathrm{n}]$ *respectivement l'anneau non commutatif et l'anneau commutatif des ploynômes à* n *indéterminées et à coefficients dans* $\mathbb{K}$*. Les appliacations suivantes sont bien définies.*

- $\gamma : \mathbb{K}\langle \mathrm{X}\rangle \longrightarrow \mathbb{K}[\mathrm{x}]$ *qui remplace* $\mathrm{X_i}$ *par* $\mathrm{x_i}$ *;*
- $\delta : \mathbb{K}[\mathrm{x}] \longrightarrow \mathbb{K}\langle \mathrm{X}\rangle$ *qui remplace* $\mathrm{x_i}$ *par* $\mathrm{X_i}$ (*les indéterminées étant dans l'ordre croissant*).

Exemple I - 1.1. $\gamma(\mathrm{XYYXZ}) = \mathrm{x^2y^2z}$,
$\gamma(\mathrm{YXZ} - \mathrm{XYZ} + \mathrm{YZ} + \mathrm{X} - 1) = \mathrm{xyz} - \mathrm{xyz} + \mathrm{yz} + \mathrm{x} - 1 = \mathrm{yz} + \mathrm{x} - 1$

$$\delta(\mathrm{xy}) = \begin{cases} \mathrm{XY} \ si \ \mathrm{x} \prec \mathrm{y} \\ \mathrm{YX} \ si \ \mathrm{y} \prec \mathrm{x} \end{cases}$$

Proposition I - 1.2.

1. γ *est un homomorphisme surjectif.*
2. δ *est injectif.*

Démonstration. *La preuve est triviale.*

Proposition I - 1.3. *Soit* $\mathcal{I}$ *un idéal de* $\mathbb{K}[\mathrm{x}]$ *et* $\mathcal{J} = \gamma^{-1}(\mathcal{I}) = \{f \in \mathbb{K}\langle \mathrm{X}\rangle, \gamma(\mathrm{f}) \in \mathcal{I}\}$. *Alors :*

1. $\mathcal{J}$ *est un idéal de* $\mathbb{K}\langle \mathrm{X}\rangle$.
2. $\mathbb{K}\langle \mathrm{X}\rangle/\mathcal{J} \simeq \mathbb{K}[\mathrm{x}]/\mathcal{I}$.

Démonstration.

1. *On sait bien que l'image réciproque d'un idéal par un homorphisme d'anneaux est aussi un idéal.*

2. Soit $\gamma' : \mathbb{K}\langle X\rangle \longrightarrow \mathbb{K}[x]/\mathcal{I}$
$f \longmapsto \overline{\gamma(f)}.$
γ' *est surjectif et* $\ker(\gamma') = \mathcal{J}$. *Il s'en suit que* $\mathbb{K}\langle X\rangle/\mathcal{J} \simeq \mathbb{K}[x]/\mathcal{I}$.

□

Proposition I - 1.4. *Soit* $\prec$ *un ordre monomial sur* $\mathbb{K}[x]$. *L'ordre* $\ll$ *sur* $\mathbb{K}\langle X\rangle$ *défini par*

$$u \ll v \Leftrightarrow \begin{cases} \gamma(u) \prec \gamma(v) \\ ou \\ \gamma(u) = \gamma(v) \text{ et } u \prec_{lex} v \end{cases}$$

est un ordre monomial appelé extension lexicographique de $\prec$.

Démonstration. *On doit montrer que l'ordre* $\ll$ *est total, est un bon ordre et est compatible avec la multiplication.*
Il est clair que $\ll$ *est un ordre total.*
Soient $u, v, w, t \in \mathbb{M}$ *tels que* $u \ll v$. *Montrons que* $wut \prec wvt$.
Si $\gamma(u) \prec \gamma(v)$ *alors* $\gamma(w)\gamma(u)\gamma(t) \prec \gamma(w)\gamma(v)\gamma(t)$. *Ainsi* $\gamma(wut) \prec \gamma(wvt)$. *D'où* $wut \ll wvt$.
Sinon $\gamma(u) = \gamma(v)$ *et* $u \prec_{lex} v$. *Il s'en suit que* $wut \prec_{lex} wvt$. *D'où* $wut \ll wvt$.
Dans tous les cas $wut \ll wvt$.
Montrons que toute suite strictement décroissante de monômes dans $\mathbb{K}\langle X\rangle$ *est stationnaire.*
Soit $(u_i)_{i\in I}$ *une suite strictement décroissante de monômes dans* $\mathbb{K}\langle X\rangle$.
On définit sur $A = \{u_i, i \in I\}$ *la relation d'équivalence suivante :*
$u_i \sim u_j \Leftrightarrow \gamma(u_i) = \gamma(u_j)$.
La classe d'équivalence de tout $u \in A$ *est notée* $Cl(u)$.
Soit $(v_j)_{j\in J\subseteq I}$ *la suite strictement décroissante des représentants de classe et* $B = \{v_j, j \in J\}$.
Alors, la restriction γ_B *de* γ *dans* B *est injective. Ainsi* $\mathrm{card}(B) = \mathrm{card}(\{\gamma(v_j), j \in J\}$.
Or la suite $(\gamma(v_j))_{j\in J}$ *est strictement décroissante dans* $\mathbb{K}[x]$. *Donc elle est stationnaire. D'où* $\mathrm{card}(B)$ *est fini.*
Si u *et* v *sont dans la même classe alors* $\deg(u) = \deg(v)$ *et* $\mathrm{card}(Cl(u)) \leqslant (\deg(u))!$

est fini.
Il s'en suit que A *est une réunion finie d'ensembles finis. D'où* $\mathrm{card}(A) < \infty$. □

Exemple I - 1.2. *L'extension lexicographique de l'ordre lexicographique sur* $\mathbb{K}[x]$ *est l'ordre* $\ll_{lex}$ *défini sur* $\mathbb{K}\langle X\rangle$ *par*

$$u \ll_{lex} v \text{ } si \begin{cases} \gamma(u) \prec_{lex} \gamma(v) \\ ou \\ \gamma(u) = \gamma(v) \text{ } et \text{ } u \prec_{lex} v \end{cases}$$

Si $u = XZY$, $v = XZZZ$, $w = XYZ \in \mathbb{K}\langle X\rangle$ *et* $X \succ Y \succ Z$ *alors :*

1) $\gamma(u) = \gamma(XZY) = xyz$ *et* $\gamma(v) = \gamma(XZZZ) = xz^3$.
Comme $x \succ y \succ z$ *alors* $\gamma(v) \prec_{lex} \gamma(u)$. *Donc* $v \ll_{lex} u$.

2) $\gamma(w) = \gamma(XYZ) = xyz = \gamma(u)$. *Comme* $X \succ Y \succ Z$ *alors* $u \ll_{lex} w$.

Exemple I - 1.3. *L'extension lexicographique de l'ordre lexicographique gradué sur* $\mathbb{K}[x]$ *est l'ordre* $\ll_{grlex}$ *défini sur* $\mathbb{K}\langle X\rangle$ *par*

$$u \ll_{grlex} v \text{ } si \begin{cases} \gamma(u) \prec_{grlex} \gamma(v) \\ ou \\ \gamma(u) = \gamma(v) \text{ } et \text{ } u \prec_{lex} v \end{cases}$$

Si $u = XZY$, $v = XZZZ$, $w = XYZ \in \mathbb{K}\langle X\rangle$ *et* $X \succ Y \succ Z$ *alors :*

1) $\gamma(u) = \gamma(XZY) = xyz$ *et* $\gamma(v) = \gamma(XZZZ) = xz^3$.
$\deg(\gamma(u)) = 3 < \deg(\gamma(v)) = 4$. *Donc* $u \ll_{grlex} v$.

2) $\gamma(w) = \gamma(XYZ) = xyz = \gamma(u)$. *Comme* $X \succ Y \succ Z$ *alors* $u \ll_{lex} w$.

L'objectif est maintenant de montrer que tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ s'exprimant sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, $\mathcal{I}$ étant un idéal de $\mathbb{K}[x]$, admet une base de Gröbner finie relativement à toute extension lexicographique d'un ordre monomial sur $\mathbb{K}[x]$.
Le résultat suivant est un préliminaire à la caractérisation des éléments de l'idéal monomial de $\mathcal{J}$.

Proposition I - 1.5. *Soient* $u = X_{i_1}X_{i_2}...X_{i_t}$, $v = X_{j_1}X_{j_2}...X_{j_t} \in \mathbb{M}$ *tels que* $v \ll u$ *et* $\gamma(u) = \gamma(v)$. *Alors il existe* $k \in [1, t-1]$ *tel que* $X_{i_k} \succ X_{i_{k+1}}$.

Démonstration. *Soient* $u = X_{i_1}X_{i_2}...X_{i_t},\ v = X_{j_1}X_{j_2}...X_{j_t} \in \mathbb{M}$ *tels que* $v \ll u$ *et* $\gamma(u) = \gamma(v)$.
Supposons que pour tout $k \in [1, t-1]$ *on a* $X_{i_k} \preceq X_{i_{k+1}}$.
$v \ll u$ *et* $\gamma(u) = \gamma(v) \Rightarrow v \prec_{lex} u$. *Ainsi, il existe* $l \in [1, t-1]$ *tel que*
$X_{i_1} = X_{j_1},\ X_{i_2} = X_{j_2}, ..., X_{i_l} = X_{j_l}$ *et* $X_{j_{l+1}} \prec X_{i_{l+1}}$.
$\gamma(u) = \gamma(v) \Rightarrow \gamma(X_{i_{l+1}}...X_{i_t}) = \gamma(X_{j_{l+1}}...X_{j_t})$
$\Rightarrow \exists k \in [l+2, t]$ *tel que* $X_{j_{l+1}} = X_{i_k} \succeq X_{i_{l+1}}$
$\Rightarrow X_{j_{l+1}} \succeq X_{i_{l+1}}$ *; ce qui est absurde.*
Donc il existe $k \in [1, t-1]$ *tel que* $X_{i_k} \succ X_{i_{k+1}}$. □

Définition I - 1.1. *On appelle commutateur tout polynôme du type* $X_iX_j - X_jX_i$, *où* $X_i, X_j \in X$. *L'ensemble des commutateurs est noté* Com.

Proposition I - 1.6. *Soient* $\mathcal{I}$ *un idéal de* $\mathbb{K}[x]$ *et* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, $\prec$ *un ordre monomial sur* $\mathbb{K}[x]$ *et* $\ll$ *son extension lexicographique,* $u = X_{i_1}X_{i_2}...X_{i_t} \in \mathbb{M}$.
Les assertions suivantes sont équivalentes.

1. $u \in \langle LM_{\ll}(\mathcal{J})\rangle$.
2. $\gamma(u) \in \langle LM_{\prec}(\mathcal{I})\rangle$ *ou il existe* $k \in [1, t-1] : X_{i_k} \succ X_{i_{k+1}}$.

Démonstration.
1) $\Rightarrow$ 2) :
Si $u \in \langle LM_{\ll}(\mathcal{J})\rangle$ *alors il existe des monômes* v *et* w *et* $f = \alpha LM(f) + \sum_{i=1}^{n} \alpha_i f_i \in \mathcal{J}$ *tels que* $u = vLM(f)w$.
$LM(\gamma(f)) = \gamma(LM(f))$ *ou il existe* $i_0 \in [1, n] :\ \gamma(LM(f)) = \gamma(f_1) = ... = \gamma(f_{i_0})$ *et* $\alpha + \sum_{i=1}^{i_0} \alpha_i = 0$.
Dans le premier cas :

$$\begin{aligned} u = vLM(f)w \Rightarrow \gamma(u) &= \gamma(vLM(f)w) \\ &= \gamma(v)\gamma(LM(f))\gamma(w) \\ &= \gamma(v)LM(\gamma(f))\gamma(w) \end{aligned}$$

$$\begin{aligned} f \in \mathcal{J} &\Rightarrow \gamma(f) \in \mathcal{I} \\ &\Rightarrow LM(\gamma(f)) \in \langle LM_{\prec}(\mathcal{I})\rangle \\ &\Rightarrow \gamma(u) \in \langle LM_{\prec}(\mathcal{I})\rangle \end{aligned}$$

Dans le deuxième cas :
Posons $LM(f) = X_{i_1}X_{i_2}...X_{i_t}$.
Comme $f_{i_0} \ll f_{i_0-1} \ll ... \ll f_1 \ll LM(f)$ *et* $\gamma(LM(f)) = \gamma(f_1) = ... = \gamma(f_{i_0})$ *alors d'après la* ***Proposition I - 1.5****, il existe* $k \in [1, t-1]$ *tel que* $X_{i_k} \succ X_{i_{k+1}}$. *D'où le résultat.*
2) $\Rightarrow$ 1) :
Notons que $Com \subset \mathcal{J}$ *car pour tout* (i,j), $X_iX_j - X_jX_i \subset \gamma^{-1}(0) \subset \gamma^{-1}(\mathcal{I})$.
Ainsi, pour tous $i, j \in [1, n]$ *tel que* $X_j \prec X_i$, *on a* $X_iX_j = LM(X_iX_j - X_jX_i) \in \langle LM_{\ll}(\mathcal{J})\rangle$.
D'après ce qui précède, s'il existe $k \in [1, t-1]$ *tel que* $X_{i_k} \succ X_{i_{k+1}}$ *alors* $u \in \langle LM_{\ll}(\mathcal{J})\rangle$.
Si $\gamma(u) \in \langle LM_{\prec}(\mathcal{I})\rangle$ *et* $X_{i_k} \prec X_{i_{k+1}}$ $\forall k \in [1, t-1]$ *alors* $u = \delta(\gamma(u)) \in \langle LM_{\ll}(\mathcal{J})\rangle$. □

L'ensemble défini ci-dessous joue un rôle important dans la suite.

Notations I.1. *Soit* $\mathcal{L}$ *un idéal monomial de* $\mathbb{K}[x]$ *et* $m = x_{i_1}x_{i_2}...x_{i_r} \in \mathcal{L}$. *On note* $U_{\mathcal{L}}(m) = \{u \in k[x_{i_1+1}, ..., x_{i_r-1}] \cap \mathbb{M} : \ u\frac{m}{x_{i_1}} \notin \mathcal{L} \text{ et } u\frac{m}{x_{i_r}} \notin \mathcal{L}\}$.

Exemple I - 1.4. *Soit* $\mathcal{L} = \langle xyz, y^3\rangle$ *avec* $x \prec y \prec z$.
Alors : $U_{\mathcal{L}}(xyz) = \{u \in k[y] : uyz \notin \mathcal{L}, \ uxy \notin \mathcal{L}\} = \{1, y\}$
$U_{\mathcal{L}}(y^3) = \{1\}$.

Définition I - 1.2.

1. *Un monôme* m *d'un idéal* $\mathcal{I}$ *de* $\mathbb{K}[x]$ *est dit générateur minimal de* $\mathcal{I}$ *si* $\frac{m}{u} \notin \mathcal{I}$ *pour tout* u *diviseur de* m, $u \neq 1$.
2. *Un monôme* $m = X_{i_1}X_{i_2}...X_{i_t}$ *d'un idéal* $\mathcal{J}$ *de* $\mathbb{K}\langle X\rangle$ *est dit générateur minimal de* $\mathcal{J}$ *si* $X_{i_2}...X_{i_t} \notin \mathcal{J}$, $X_{i_1}...X_{i_{t-1}} \notin \mathcal{J}$.

Exemple I - 1.5.

1. y^2z *et* xy *sont des générateurs minimaux de l'idéal monomial* $\langle xy, x^2y, y^2z\rangle$ *de* $\mathbb{K}[x, y, z]$ *mais* x^2y *ne l'est pas.*
2. XZ, ZX, YZ *et* $YZZX$ *sont des générateurs minimaux de l'idéal monomial* $\langle XYZ, XZ, ZX, YZ, YZZX\rangle$ *de* $\mathbb{K}\langle X, Y, Z\rangle$ *mais* XYZ *ne l'est pas.*

Il est bien connu qu'un idéal non commutatif admet une base de Gröbner finie si et seulement si son idéal monomial admet une partie génératrice minimale finie. Ainsi, suivant l'objetif fixé, on doit caractériser la finitude de l'ensemble des générateurs minimaux de tout idéal $\mathcal{J}$ non commutatif s'exprimant sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, où $\mathcal{I}$ est un idéal commutatif. On a :

Proposition I - 1.7. *Soient $\mathcal{I}$ un idéal de $\mathbb{K}[\mathrm{x}]$, $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, $\prec$ un ordre monomial sur $\mathbb{K}[\mathrm{x}]$ et $\ll$ son extension lexicographique. Soient m un générateur minimal de $\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ et u un monôme de $\mathbb{K}\langle X\rangle$. Les assertions suivantes sont équivalentes.*

1. *$\delta(\mathrm{um})$ est un générateur minimal de $\langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle$;*
2. *$\mathrm{u} \in \mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})$.*

Démonstration. *Ecrivons :* $\mathrm{m} = \mathrm{x}_{\mathrm{i}_1}\mathrm{x}_{\mathrm{i}_2}...\mathrm{x}_{\mathrm{i}_r}$ *et* $\mathrm{u} = \mathrm{x}_{\mathrm{j}_1}\mathrm{x}_{\mathrm{j}_2}...\mathrm{x}_{\mathrm{j}_k}$ *avec* $\mathrm{x}_{\mathrm{i}_l} \preceq \mathrm{x}_{\mathrm{i}_{l+1}}$ *et* $\mathrm{x}_{\mathrm{j}_l} \preceq \mathrm{x}_{\mathrm{j}_{l+1}}$.
1) $\Rightarrow$ 2) : *Si* $\mathrm{x}_{\mathrm{j}_1} \preceq \mathrm{x}_{\mathrm{i}_1}$ *alors* $\delta(\mathrm{um}) = \delta(\mathrm{x}_{\mathrm{j}_1})\delta(\frac{\mathrm{u}}{\mathrm{x}_{\mathrm{j}_1}}\mathrm{m})$. *Il s'en suit que* $\delta(\frac{\mathrm{u}}{\mathrm{x}_{\mathrm{j}_1}}\mathrm{m}) \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle$ *car* $\delta(\mathrm{um})$ *est minimal. Donc* $\mathrm{x}_{\mathrm{j}_1} \succ \mathrm{x}_{\mathrm{i}_1}$. *De même,* $\mathrm{x}_{\mathrm{j}_k} \prec \mathrm{x}_{\mathrm{i}_r}$. *Donc* $\mathrm{u} \in \mathrm{k}\big[\mathrm{x}_{\mathrm{i}_1+1}, ..., \mathrm{x}_{\mathrm{i}_r-1}\big]$.
Si $\delta(\mathrm{um})$ *est un générateur minimal de* $\langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle$ *alors*

$$\delta(\mathrm{um}) = \delta(\mathrm{x}_{\mathrm{i}_1})\delta(\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_1}}) = \delta(\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}})\delta(\mathrm{x}_{\mathrm{i}_r}).$$

Il s'en suit que $\delta(\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_1}}) \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle$ *et* $\delta(\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}}) \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle$.
Par conséquent, $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_1}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *et* $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$. *D'où* $\mathrm{u} \in \mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})$.
2) $\Rightarrow$ 1) :
Si $\mathrm{u} \in \mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})$

$$\begin{aligned}
&\Rightarrow \mathrm{u}\tfrac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_1}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle \text{ et } \mathrm{u}\tfrac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle \\
&\Rightarrow \delta(\mathrm{u}\tfrac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_1}}) \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle \text{ et } \delta(\mathrm{u}\tfrac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}}) \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle \\
&\Rightarrow \tfrac{\delta(\mathrm{um})}{\delta(\mathrm{x}_{\mathrm{i}_1})} \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle \text{ et } \tfrac{\delta(\mathrm{um})}{\delta(\mathrm{x}_{\mathrm{i}_r})} \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle \\
&\Rightarrow \tfrac{\delta(\mathrm{um})}{\mathrm{X}_{\mathrm{i}_1}} \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle \text{ et } \tfrac{\delta(\mathrm{um})}{\mathrm{X}_{\mathrm{i}_r}} \notin \langle \mathrm{LM}_{\ll}(\mathcal{J})\rangle.
\end{aligned}$$

□

I - 2 Bases de Gröbner non commutatives finies

Les concepts et résultats de la section précédente permettent de construire une partie génératrice de l'idéal monomial de tout idéal s'exprimant sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$. Le théorème suivant est un résultat fondamental qui découle de ce qui précède.

Théorème I.1. *Si* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *et* $\ll$*, l'extension lexiographique de* $\prec$ *alors l'ensemble*

$$\{X_iX_j,\ i > j\} \cup \{\delta(um)|\ m \in \langle LM_{\prec}(\mathcal{I})\rangle,\ u \in U_{\langle LM_{\prec}(\mathcal{I})\rangle(m)}\}$$

est une partie génératrice de $\langle LM_{\ll}(\mathcal{J})\rangle$.

Démonstration. *On pose* $A = \{X_iX_j|\ i > j\}$ *et*
$B = \{\delta(um)|\ m \in \langle LM_{\prec}(\mathcal{I})\rangle,\ u \in U_{\langle LM_{\prec}(\mathcal{I})\rangle}(m)\}$. *Soit* $f \in \langle LM_{\ll}(\mathcal{J})\rangle$. *Alors* $f = f_1 + f_2$ *avec* $f_1 = \sum \alpha_i w_i$ *où* $w_i = w_{i_1}...w_{i_r}$ *est tel qu'il existe* $j \in [1, r-1]$ *tel que* $w_{i_j} > w_{i_{j+1}}$ *et* $f_2 = \sum \beta_j v_j$ *où* $v_j = v_{j_1}...v_{j_s}$ *est tel que* $v_{j_1} \preceq v_{j_2}... \preceq v_{j_s}$.
Alors f_1 *s'écrit sous la forme* $f_1 = \sum \alpha_i u_i g_i v_i$ *où* $g_i \in A$ *et* $u_i,\ v_i$ *sont des monômes de* $\mathbb{K}\langle X\rangle$. *D'où* $f \in \langle A\rangle$.
Soit t *un générateur minimal de* v_j *dans* $\langle LM_{\ll}(\mathcal{J})\rangle$. *Alors, il existe* v', v'' *des monômes de* $\mathbb{K}\langle X\rangle$ *tels que* $v_j = v'tv''$.
$v_j = \delta(\gamma(v_j)) = \delta(\gamma(v'))\delta(\gamma(t))\delta(\gamma(v'')) = v'\delta(um)v''$ *où* m *est un générateur minimal de* $\gamma(t)$ *dans* $\langle LM_{\prec}(\mathcal{I})\rangle$.
$t = \delta(um)$ *étant minimal alors* $u \in U_{\langle LM_{\prec}(\mathcal{I})\rangle}(m)$. *Il s'en suit que* $vv_j \in \langle B\rangle$. *D'où* $f_2 \in \langle B\rangle$. *On en déduit que* $f = f_1 + f_2 \in \langle A \cup B\rangle$. □

Du théorème précédent, découle l'un des résultats les plus importants de cette section. En effet, il nous permet d'obtenir une méthode de construction d'une base de Gröbner minimale de tout idéal non commutatif $\mathcal{J}$ qui s'écrit $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ pour un idéal commutatif $\mathcal{I}$.

Corollaire I.1. *Soit* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *et* $\ll$ *l'extension lexicographique de* $\prec$. *Soit* G *une base de Gröbner minimale de* $\mathcal{I}$ *relativement à* $\prec$ *alors*

$$T = \{X_iX_j - X_jX_i|\ i > j,\ X_i, X_j \notin \langle LM_{\prec}(\mathcal{I})\rangle\} \cup \{\delta(uf)|\ f \in G,\ u \in U_{\langle LM_{\prec}(\mathcal{I})\rangle}(LM_{\prec}(f))\}$$

est une base de Gröbner minimale de $\mathcal{J}$ *relativement à* $\ll$.

Démonstration. *Soit* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *et* $\ll$ *l'extension lexiographique de* $\prec$. *Soit* G *une base de Gröbner minimale de* $\mathcal{I}$ *relativement à* $\prec$. *D'après le Théorème* I.1. *et la propositon* I.1.7.,

$$\{X_iX_j|\ i > j,\ X_i, X_j \notin \langle LM_\prec(\mathcal{I})\rangle\} \cup \{\delta(uLM_\prec(f))|\ f \in G,\ u \in U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))\}$$

est une partie génératrice minimale de $\langle LM_\ll(\mathcal{J})\rangle$. *Il s'en suit que pour tout* $g \in \mathcal{J}$, *il existe* $a, b \in \mathbb{M},\ h \in T$ *tels que* $LM_\ll(g) = aLM_\ll(h)b$ (i).
Soit $g \in \mathcal{J}$ *et* $g' =$ Réduction Totale(g, Com).
Alors $g' \in \{\delta(uf)|\ f \in G,\ u \in U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))\}$. *D'où* $g \in \langle T\rangle$ (ii).
(i) *et* (ii) *impliquent que* T *est une base de Gröbner de* $\mathcal{J}$ *relativement à* $\ll$. □

Dans tout le reste de ce Chapitre, T désigne une base de Gröbner obtenue à partir de la méthode donnée par le Corollaire I.1.

Pour tout idéal commutatif $\mathcal{I}$, on dispose dorénavant d'un outil de construction d'une base de Gröbner de $\gamma^{-1}(\mathcal{I})$. Cependant, la base de Gröbner calculée avec la méthode précédemment indiquée n'est pas forcément finie.
Sachant que $\{X_iX_j - X_jX_i|\ i > j,\ X_i, X_j \notin \langle LM_\prec(\mathcal{I})\rangle\}$ est fini alors les conditions suivantes sont équivalentes

1. $\{X_iX_j - X_jX_i|\ i > j,\ X_i, X_j \notin \langle LM_\prec(\mathcal{I})\rangle\} \cup \{\delta(uf)|\ f \in G,\ u \in U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))\}$ est fini.
2. $\{\delta(uf)|\ f \in G,\ u \in U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))\}$ est fini.
3. $U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))$ est fini pour tout $f \in G$.

Ainsi, on va chercher des conditions de finitude des sous-ensembles $U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))$ pour obtenir une base de Gröbner finie. Pour cela, on introduit la notion de Borel fixe qui nous donnera des conditions suffisantes.
On a d'abord la définition suivante.

Définition I - 2.1. *Soit* p *un nombre premier.* $a = \sum_i a_i p^i$ *et* $b = \sum_i b_i p^i$ *deux entiers naturels exprimés dans la base* p. *On dit que* $a \leqslant_p b$ *si* $a_i \leqslant b_i\ \forall i$. $\leqslant_p$ *est un ordre partiel sur les entiers naturels.*

Exemple I - 2.1.

1. $10 \leqslant_2 15$ *car :*
   $15 = 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$ *et*
   $10 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$
2. 10 *et* 15 *ne sont pas comparables sous* $\leqslant_3$ *car :*
   $15 = 1 \times 3^2 + 2 \times 3^1 + 0 \times 3^0$ *et*
   $10 = 1 \times 3^2 + 0 \times 3^1 + 1 \times 3^0$

Définition I - 2.2.

— *Un idéal monomial* $\mathcal{I}$ *est dit* 0*-Borel fixe si* $x_j \frac{m}{x_i} \in \mathcal{I}$ *pour tout générateur* m *de* $\mathcal{I}$*, tout* x_i *diviseur de* m *et* $x_j \prec x_i$.

— *Soit* p *un nombre premier. Un idéal monomial est dit* p*-Borel fixe si la condition suivante est satisfaite : pour tout monôme* m *générateur de* $\mathcal{I}$*, si* ${x_i}^t$ *divise* m *et* ${x_i}^{t+1}$ *ne divise pas* m *alors* $(\frac{x_j}{x_i})^s m \in \mathcal{I}$ *pour tout* $x_j \prec x_i$ *et* $s \leqslant_p t$.

Exemple I - 2.2.

1. *L'idéal monomial* $\mathcal{I} = \langle x, y \rangle$ *de* $\mathbb{K}[x, y]$ *est* 0*-Borel fixe et* p*-Borel fixe pour tout nombre premier* p.
2. *L'idéal* $\mathcal{I} = \langle x^4y, y^3 \rangle$, $y \prec x$, *est* 2*-Borel fixe et non* 0*-Borel fixe. En effet,* x^4y *est divisible par* x^4 *et non par* x^5 *et* 0 *et* 4 *sont les seuls entiers inférieurs à* 4 *suivant l'ordre* $\leqslant_2$. *Or* $(\frac{y}{x})^0 x^4y = x^4y \in \mathcal{I}$ *et* $(\frac{y}{x})^4 x^4y = y^5 \in \mathcal{I}$.
   Par contre, $\frac{y}{x} x^4y = x^3y^2 \notin \mathcal{I}$

Remarque I.1. *Aucun idéal monomial principal n'est* 0*-Borel fixe ou* p*-Borel fixe pour un nombre premier* p.

Dans ce qui suit, on montre qu'il suffit que $\langle \mathrm{LM}_\prec(\mathcal{I}) \rangle$ soit 0-Borel fixe ou p-Borel fixe pour que la finitude de $\mathrm{U}_{\langle \mathrm{LM}_\prec(\mathcal{I}) \rangle}(\mathrm{LM}_\prec(f))$, où G est une base de Gröbner de $\mathcal{I}$ et $f \in G$, soit garantie.

Proposition I - 2.1. *Si* $\langle \mathrm{LM}_\prec(\mathcal{I}) \rangle$ *est* 0*-Borel fixe alors* $\mathrm{U}_{\langle \mathrm{LM}_\prec(\mathcal{I}) \rangle}(m) = \{1\}$ *pour tout monôme* m *générateur de* $\mathcal{I}$.

Démonstration. *Supposons que* $\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *est* 0*-Borel fixe. Soit* $\mathrm{m} = \mathrm{x}_{\mathrm{i}_1}\mathrm{x}_{\mathrm{i}_2}...\mathrm{x}_{\mathrm{i}_r}$ *un générateur de* $\mathcal{I}$ *et* $\mathrm{u} \in \mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})$.
Si $\mathrm{u} \neq 1$ *alors* $\mathrm{u} = \mathrm{x}_{\mathrm{j}_1}\mathrm{x}_{\mathrm{j}_2}...\mathrm{x}_{\mathrm{j}_k} \in \mathrm{k}[\mathrm{x}_{\mathrm{i}_1+1}, ..., \mathrm{x}_{\mathrm{i}_r-1}]$ *et* $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_1}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$, $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$.
Or, pour tout $\mathrm{l} \in [1; \mathrm{k}]$, $\mathrm{x}_{\mathrm{j}_l} \prec \mathrm{x}_{\mathrm{i}_r}$. *Donc* $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} = \frac{\mathrm{u}}{\mathrm{x}_{\mathrm{j}_l}}\mathrm{x}_{\mathrm{j}_l}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} \in \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *; ce qui est absurde. On en déduit que* $\mathrm{u} = 1$. □

Proposition I - 2.2. *Soit* p *un nombre premier. Si* $\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *est* p*-Borel fixe alors pour tout monôme m générateur de* $\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$, $\mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})$ *contient un nombre fini d'éléments.*

Démonstration. *Supposons que* $\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *est* p*-Borel fixe. Soit* $\mathrm{m} = \mathrm{x}_{\mathrm{i}_1}\mathrm{x}_{\mathrm{i}_2}...\mathrm{x}_{\mathrm{i}_r}$ *un générateur de* $\mathcal{I}$ *et* $\mathrm{t} = \deg_{\mathrm{m}}(\mathrm{x}_{\mathrm{i}_r})$ *le degré partiel de l'indéterminée* $\mathrm{x}_{\mathrm{i}_r}$ *dans* m.
Soit $\mathrm{u} = \mathrm{x}_{\mathrm{j}_1}\mathrm{x}_{\mathrm{j}_2}...\mathrm{x}_{\mathrm{j}_k} \in \mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})$. *Alors,* $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$.
Soit $\mathrm{x}_{\mathrm{j}} \prec \mathrm{x}_{\mathrm{i}_r}$. *Si* $\deg_{\mathrm{u}}(\mathrm{x}_{\mathrm{j}}) \geqslant \mathrm{t}$ *alors* $\mathrm{u}\frac{\mathrm{m}}{\mathrm{x}_{\mathrm{i}_r}} = \frac{\mathrm{u}}{\mathrm{x}_{\mathrm{j}}^{\mathrm{t}}}\mathrm{x}_{\mathrm{i}_r}^{\mathrm{t}-1}(\frac{\mathrm{x}_{\mathrm{j}}}{\mathrm{x}_{\mathrm{i}r}})^{\mathrm{t}}\mathrm{m} \in \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *; ce qui est absurde. D'où* $\deg_{\mathrm{u}}(\mathrm{x}_{\mathrm{j}}) < \mathrm{t}$ *pour tout* $\mathrm{x}_{\mathrm{j}} \prec \mathrm{x}_{\mathrm{i}_r}$.
Comme $\mathrm{u} \in \mathrm{k}[\mathrm{x}_{\mathrm{i}_1+1}, ..., \mathrm{x}_{\mathrm{i}_r-1}]$ *alors on peut l'écrire sous la forme :* $\mathrm{u} = \mathrm{x}_{\mathrm{i}_1+1}^{\alpha_{\mathrm{i}_1+1}}\mathrm{x}_{\mathrm{i}_1+2}^{\alpha_{\mathrm{i}_1+2}}...\mathrm{x}_{\mathrm{i}_r-1}^{\alpha_{\mathrm{i}_r-1}}$ *avec* $\alpha_{\mathrm{i}} < \mathrm{t}$ $\forall \mathrm{i} \in [\mathrm{i}_1 + 1; \mathrm{i}_r - 1]$. *Ainsi,* $\deg(\mathrm{u}) = \mathrm{k} < \mathrm{t} \times (\mathrm{i}_r - \mathrm{i}_1 - 1)$.
Par suite,

$$\mathrm{card}(\mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{m})) < \sum_{\mathrm{s}=1}^{\mathrm{t}\times(\mathrm{i}_r-\mathrm{i}_1-1)} (\mathrm{i}_r - \mathrm{i}_1 - 1)^{\mathrm{s}} < \infty$$

. □

Remarque I.2. *On peut remarquer que les conditions données dans la Proposition I - 2.1 et dans la Proposition I - 2.2 sont suffisantes mais non nécessaires. En effet, l'idéal monomial* $\mathcal{I} = \langle \mathrm{xyz}, \mathrm{y}^3\rangle$ *de* $\mathbb{K}[\mathrm{x}, \mathrm{y}, \mathrm{z}]$ *n'est ni* 0*-Borel fixe ni* p*-Borel fixe pour un nombre premier* p *et pourtant* $\mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{xyz}) = \{1, \mathrm{y}, \mathrm{y}^2\}$ *et* $\mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{y}^3) = \{1\}$ *sont bien finis.*

Alors, on reprend le *Corollaire* I.1 en y rajoutant ces nouvelles conditions. Cela donne :

Corollaire I.2. *Soient* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *et* $\ll$*, l'extension lexiographique de* $\prec$ *et* G *une base de Gröbner minimale de* $\mathcal{I}$ *relativement à* $\prec$. *Si* $\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle$ *est* 0*-Borel fixe ou* p*-Borel fixe pour un nombre premier* p *alors*

$$\{\mathrm{X_iX_j} - \mathrm{X_jX_i} |\ \mathrm{i} > \mathrm{j},\ \mathrm{X_i}, \mathrm{X_j} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle\} \cup \{\delta(\mathrm{uf}) |\ \mathrm{f} \in \mathrm{G},\ \mathrm{u} \in \mathrm{U}_{\langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle}(\mathrm{LM}_{\prec}(\mathrm{f}))\}$$

est une base de Gröbner minimale finie de $\mathcal{J}$ *relativement à* $\ll$.

Exemple I - 2.3.

1. *On considère l'idéal* $\mathcal{I} = \langle x - 1, y - 1\rangle$ *de* $\mathbb{K}[x, y]$, $x \succ y$. *Son idéal monomial* $\langle LM_{\prec}(\mathcal{I})\rangle$ *est* 0*-Borel fixe pour tout ordre monomial* $\prec$ *sur* $\mathbb{K}[x, y]$.
   Donc $\{\delta(x - 1),\ \delta(y - 1)\} = \{X - 1,\ Y - 1\}$ *est une base de Gröbner minimale de l'idéal* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *relativement à toute extension lexicographique de tout ordre monomial sur* $\mathbb{K}[x, y]$.

2. *Une base de Gröbner minimale de l'idéal* $\mathcal{I} = \langle x^4y + 2x^2, y^3 + y^2]$ *relativement à l'ordre lexicographique induit par* $y \prec x$ *est* $G = \{y^3 + y^2, x^2y + x^2, x^4 - 2x^2\}$.
   De plus, $\langle LM_{\prec}(\mathcal{I})\rangle = \langle y^3, x^2y, x^4\rangle$ *est* 2*-Borel fixe et*

$$U_{\langle LM_{\prec}(\mathcal{I})\rangle}(y^3) = U_{\langle LM_{\prec}(\mathcal{I})\rangle}(x^2y) = U_{\langle LM_{\prec}(\mathcal{I})\rangle}(x^4) = \{1\}.$$

   Ainsi, une base de Gröbner minimale de l'idéal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *relativement à l'extension lexicographique de l'ordre lexicographique est* $T = \{Y^3 + Y^2, YX^2 + X^2, X^4 - 2X$

3. *On considère un ordre monomial* $\prec$, *où* $z \prec y \prec x$, *sur* $\mathbb{K}[x, y, z]$ *et* $\ll$ *son extension lexicographique sur* $\mathbb{K}\langle X, Y, Z\rangle$.
   L'idéal monomial $\mathcal{I} = \langle f_1 = x^4yz^2, f_2 = y^5z^2, f_3 = yz^6, f_4 = x^4z^3, f_5 = y^4z^3, f_6 = z^7\rangle$ *est* 2*-Borel fixe. On a :* $U_{\langle LM_{\prec}(\mathcal{I})\rangle}(LM_{\prec}(f_1)) = \{1, y, y^2, y^3\}$ *et pour tout* $i \in \{2, 3, 4, 5, 6\}$, $U_{\langle LM_{\prec}(\mathcal{I})\rangle}(LM_{\prec}(f_i)) = \{1\}$. *Ainsi, une base de Gröbner de l'idéal* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *est*
   $T = \{XY - YX, XZ - ZX, YZ - ZY, Z^2YX^4, Z^2Y^2X^4, Z^2Y^3X^4, Z^2Y^4X^4, Z^2Y^5,$
   $Z^6Y, Z^3X^4, Z^3Y^4, Z^7\}$

La question revient alors de savoir à quelles conditions un idéal monomial est-il 0-Borel fixe ou p-Borel fixe pour un nombre premier p. Là encore, c'est une réponse partielle qui existe.

Théorème I.2 (Galligo-Bayer-Stillman)**.** *Si* $\mathbb{K}$ *est de caractéristique zéro alors après un changement linéaire d'indéterminées,* $\langle LM_{\prec}(\mathcal{I})\rangle$ *est* p*-Borel fixe pour tout* p *premier ou nul et tout ordre monomial* $\prec$.

En somme, on conclut que :

Corollaire I.3. *Si* $\mathbb{K}$ *est de caractéristique zéro alors tout idéal* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *de* $\mathbb{K}\langle X\rangle$ *admet une base de Gröbner finie relativement à toute extension lexicographique d'un ordre monomial sur* $\mathbb{K}[x]$.

Dans les exemples précédents, ni le corps de base $\mathbb{K}$ ni sa caractéristique ne sont spécifiés. En effet, ces exemples marchent indépendamment du corps. Par contre, dans [27], il est montré que si $\mathbb{K}$ est de caractéristique p non nulle et $\mathcal{I} \subset \mathbb{K}[x, y, z]$, l'idéal principal engendré par le produit des formes linéaires, $\mathcal{L} = (\langle x, y, z\rangle^3)^{[p]} \subset k[x, y, z]$, la p-ième puissance de Frobenius du cube de l'idéal maximal en trois indéterminées, alors les idéaux non commutatifs $\gamma^{-1}(\mathcal{I})$ et $\gamma^{-1}(\mathcal{L})$ n'admettent aucune base de Gröbner finie.

Dans toute la suite de ce chapitre, le corps $\mathbb{K}$ considéré est de caractéristique nulle.

II Caractérisation d'idéaux non commutatifs admettant une base de Gröbner finie

Dans la première section, on a montré que tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ s'exprimant sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, $\mathcal{I}$ étant un idéal de $\mathbb{K}[x]$, admet une base de Gröbner finie. La question naturelle est alors de savoir si tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ admettant une base de Gröbner finie relativement à une extension lexicographique d'un ordre monomial sur $\mathbb{K}[x]$ s'écrit nécessairement de la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ pour un idéal $\mathcal{I}$ de $\mathbb{K}[x]$.
Il est clair que la réponse n'est pas nécessairement affirmative. Une condition nécessaire à cela est que l'idéal $\mathcal{J}$ contienne tous les commutateurs.
Dans toute la suite, tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ considéré contient tous les commutateurs.
Remarquons d'abord que la réponse à la question posée est affirmative pour l'exemple suivant.

Exemple II - 0.1. *On considère l'idéal* $\mathcal{J}$ *de* $\mathbb{K}\langle X\rangle$ *engendré par*
$T = \{ZX - XZ, ZY - YZ, YX - XY\} \cup \{XYZ - Y, XZ - 1, XY^2Z - Y^2, Y^3\}$
avec $X \prec Y \prec Z$.

T *est une base de Gröbner minimale de* $\mathcal{J}$ *relativement à tout ordre monomial sur* $\mathbb{K}\langle X\rangle$. *En appliquant la procédure de construction décrite dans [27] à l'idéal* $\mathcal{I}$ *engendré par* $\{xz-1, y^3\}$, *on obtient :*
$T' = \{ZX - XZ, ZY - YZ, YX - XY\} \cup \{XYZ - Y, XZ - 1, XY^2Z - Y^2, Y^3\}$.
En remarquant que $T' = T$, *on conclut que* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$. *Donc, pour cet exemple, la réponse est affirmative.*

Nous allons montrer que pour tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ contenant les commutateurs et admettant une base de Gröbner finie, il existe un idéal $\mathcal{I}$ de $\mathbb{K}[x]$ tel que
$\mathcal{J} = \gamma^{-1}(\mathcal{I})$.
Nous adoptons la démarche suivante :

- nous allons d'abord énumérer deux propriétés caractéristiques de la base de Gröbner construite avec la méthode décrite par le Corollaire I.1 ;
- puis, nous allons montrer que tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ contenant les commutateurs et admettant une base de Gröbner finie ayant ces deux propriétés s'exprime sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$, pour un idéal $\mathcal{I}$ de $\mathbb{K}[x]$;
- enfin, on prouvera que si $\mathcal{J}$ contient tous les commutateurs, de toute base de Gröbner finie, on peut extraire une base de Gröbner finie ayant ces deux propriétés.

De façon générale, si la réponse est affirmative ; c'est à dire s'il existe un idéal $\mathcal{I}$ de $\mathbb{K}[x]$ tel que $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ alors $\mathcal{I}$ admet une base de Gröbner minimale à partir de laquelle on peut retrouver une base de Gröbner T de $\mathcal{J}$ par la méthode donnée au Corollaire I.1.
Notre question est donc équivalente à la suivante : existe-t-il une base de Gröbner minimale G d'un idéal $\mathcal{I}$ vérifiant :
$T = \{X_iX_j - X_jX_i \mid i > j, x_i, x_j \notin \langle LM_\prec(\mathcal{I})\rangle\} \cup \{\delta(uf) \mid f \in G, u \in U_{\langle LM_\prec(\mathcal{I})\rangle}(LM_\prec(f))\}$?
Ci-dessous, nous énumérons deux propriétés P_1 et P_2 satisfaites par la base de Gröbner minimale T construite avec la méthode proposée dans [27].

1. P_1 : Soit $g_i \in T$. Si g_i n'est pas un commutateur alors les indéterminées de chaque monôme de g_i sont dans l'ordre croissant.
2. P_2 : Soit $g_i \in T \backslash Com$ tel que $LM_\prec(\gamma(g_i))$ est un générateur minimal de $\langle LM_\prec(\gamma(T))\rangle$

et u_j un monôme de $\mathbb{K}[x]$. Il existe $g_j \in T$ tel que $LM_{\prec}(\gamma(g_j)) = u_j LM_{\prec}(\gamma(g_i))$ si et seulement si $u_j \in U_{\langle LM_{\prec}(\gamma(T))\rangle}(LM_{\prec}(\gamma(g_i)))$.

Dans ce qui suit, on prouve que la réponse à la question posée est positive si l'idéal $\mathcal{J}$ contient tous les commutateurs et admet une base de Gröbner finie ayant les propriétés P_1 et P_2.
Sous l'hypothèse que $\mathcal{J}$ contient tous les commutateurs, nous prouvons d'abord le résultat suivant.

Proposition II - 0.1. *Soit $\mathcal{J}$ un idéal de $\mathbb{K}\langle X\rangle$ admettant une base de Gröbner finie. Si $\mathcal{J}$ contient tous les commutateurs alors $\mathcal{J}$ admet une base de Gröbner finie vérifiant la propriété P_1.*

Démonstration. *Soit* T *une base Gröbner finie de* $\mathcal{J}$ *et* $T' =$ Réduction Totale$(T, Com, \ll)$ T' *est obtenu en réduisant totalement chaque élément de* T *par les commutateurs.*
Alors, on montre que $\mathcal{J} = \langle T\rangle = \langle T' \cup Com\rangle$.
• $\mathcal{J} \subseteq \langle T' \cup Com\rangle$:
Soit $f \in \mathcal{J}$. *alors* f *s'écrit sous la forme :* $f = \sum_i p_i t_i q_i,\ p_i, q_i \in \mathbb{K}\langle X\rangle,\ t_i \in T$.
Par une réduction totale de t_i *par les commutateurs, on a :*

$$t_i = \sum_{k,j} p_{k,j}(X_k X_j - X_j X_k) q_{k,j} + r_i,\ p_{k,j}, q_{k,j} \in \mathbb{K}\langle X\rangle,\ r_i \in T'$$

$$f = \sum_i p_i \Big(\sum_{k,j} p_{k,j}(X_k X_j - X_j X_k) q_{k,j} + r_i\Big) q_i,\ p_i, q_i \in \mathbb{K}\langle X\rangle,\ t_i \in T.$$
$$= \sum_i p_i \Big(\sum_{k,j} p_{k,j}(X_k X_j - X_j X_k) q_{k,j}\Big) q_i + \sum_i p_i r_i q_i \in \langle Com\rangle + \langle T'\rangle = \langle Com \cup T'\rangle$$

Donc $\mathcal{J} \subseteq \langle Com \cup T'\rangle$.
• *L'autre inclusion est triviale puisque* $Com \subseteq \mathcal{J}$ *et* $T' \subseteq \mathcal{J}$.
Ainsi $\mathcal{J} = \langle Com \cup T'\rangle$.
• *Nous devons maintenant prouver que* $Com \cup T'$ *est une base de Gröbner de* $\mathcal{J}$.
Soit $f \in \mathcal{J}$. *Alors, il existe* $g_i \in T$ *tel que* $LM_{\ll}(g_i)$ *divise* $LM_{\ll}(f)$.
Soit $r_i =$ Réduction Totale$(g_i, Com, \ll)$.
$LM_{\ll}(g_i) \neq LM_{\ll}(r_i)$ *si et seulement si* $LM_{\ll}(X_k X_l - X_l X_k)$ *divise* $LM_{\ll}(g_i)$ *pour un commutateur* $X_k X_l - X_l X_k$.

Dans chaque cas, le monôme dominant d'un élément de $\mathrm{Com} \cup \mathrm{T}'$ *divise* $\mathrm{LM}_{\ll}(\mathrm{f})$. *En rendant minimale* $\mathrm{Com} \cup \mathrm{T}'$, *on obtient une base de Gröbner* $\{\mathrm{X_iX_j} - \mathrm{X_jX_i} \mid \mathrm{i} > \mathrm{j}, \mathrm{x_i}, \mathrm{x_j} \notin \langle \mathrm{LM}_{\prec}(\mathcal{I})\rangle\} \cup \mathrm{T}''$ *satisfaisant* P_1. □

Dans ce qui suit, on montre qu'à partir d'un idéal $\mathcal{J}$ de $\mathbb{K}\langle \mathrm{X}\rangle$ admettant une base de Gröbner finie, on peut construire un sous-ensmeble G de $\mathbb{K}[\mathrm{x}]$ qui est une base de Gröbner de l'idéal $\mathcal{I}$ qu'il engendre tel que $\mathcal{J} = \gamma^{-1}(\mathcal{I})$.

Proposition II - 0.2. *Soit* $\mathcal{J}$ *un idéal de* $\mathbb{K}\langle \mathrm{X}\rangle$ *contenant tous les commutateurs et admettant une base de Gröbner finie* T *qui vérifie la propriété* P_1 *relativement à une extension lexicographique d'un ordre monomial sur* $\mathbb{K}[\mathrm{x}]$.
On définit l'ensemble $\mathcal{R} = \{\mathrm{g} \in \mathrm{T} \mid \mathrm{LM}_{\prec}(\gamma(\mathrm{g}))$ *est minimal dans* $\mathrm{LM}_{\prec}(\gamma(\mathrm{T}))\}$.
L'ensemble $\mathrm{G} = \{\gamma(\mathrm{g}) \mid \mathrm{g} \in \mathcal{R}\}$ *est une base de Gröbner minimale relativement à l'ordre sur* $\mathbb{K}[\mathrm{x}]$ *dont on a considéré l'extension lexicographique sur* $\mathbb{K}\langle \mathrm{X}\rangle$.

Démonstration. *Soit* $\mathcal{I} = \langle \mathrm{G}\rangle$ *et* $\mathrm{f} \in \mathcal{I}$. *Alors* f *s'exprime* $\mathrm{f} = \sum_{\mathrm{i}} \mathrm{h_i}\gamma(\mathrm{g_i})$.
L'application γ *étant surjective, alors il existe* $p_i, q_i \in \mathbb{K}[\mathrm{x}]$ *tel que* $\mathrm{h_i} = \gamma(\mathrm{p_i})$ *et* $1 = \gamma(\mathrm{q_i})$.
Ainsi $\mathrm{f} = \sum_{\mathrm{i}} \gamma(\mathrm{p_i})\gamma(\mathrm{g_i})\gamma(\mathrm{q_i}) = \sum_{\mathrm{i}} \gamma(\mathrm{p_ig_iq_i}) = \gamma(\sum_{\mathrm{i}} \mathrm{p_ig_iq_i})$.
D'où l'existence d'un $\mathrm{g} \in \mathcal{J}$ *tel que* $\mathrm{f} = \gamma(\mathrm{g})$. *En réduisant totalement ce* g *par les commutateurs, on a :* $\mathrm{g} = \sum_{\mathrm{i,j,k}} \mathrm{p_k}(\mathrm{X_iX_j} - \mathrm{X_jX_i})\mathrm{q_k} + \mathrm{r}$ *où aucun monôme de* r *n'est divisible par le monôme dominant d'un commutateur.*
Donc, $\mathrm{f} = \gamma(\mathrm{g}) = \gamma(\mathrm{r})$. *De même,* $\mathrm{r} = \mathrm{g} - \sum_{\mathrm{i,j,k}} \mathrm{p_k}(\mathrm{X_iX_j} - \mathrm{X_jX_i})\mathrm{q_k} \in \mathcal{J}$. *Ainsi, il existe* $\mathrm{g_i}$ *tel que* $\mathrm{LM}_{\prec}(\mathrm{r}) = \mathrm{u_i}\mathrm{LM}_{\prec}(\mathrm{g_i})\mathrm{v_i}$. *Puisque les indéterminées de chaque monôme de r sont dans l'ordre croissant, on a :*

$$\begin{aligned}
\mathrm{LM}_{\prec}(\mathrm{f}) &= \mathrm{LM}_{\prec}(\gamma(\mathrm{r})) \\
&= \gamma(\mathrm{LM}_{\prec}(\mathrm{r})) \\
&= \gamma(\mathrm{u_i}\mathrm{LM}_{\prec}(\mathrm{g_i})\mathrm{v_i}) \\
&= \gamma(\mathrm{u_i})\gamma(\mathrm{LM}_{\prec}(\mathrm{g_i}))\gamma(\mathrm{v_i}) \\
&= \gamma(\mathrm{u_i})\gamma(\mathrm{u_j}\mathrm{LM}_{\prec}(\mathrm{g_{i_j}}))\gamma(\mathrm{v_i})
\end{aligned}$$

avec g_{i_j} *étant le représentant du sous-ensemble contenant* g_i.
Finalement, $LM_{\prec}(f) = \gamma(u_i)\gamma(u_j)\gamma(LM_{\prec}(g_{i_j}))\gamma(v_i)$ *est divisible par le monôme dominant d'un élément de* G. *On en conclut que* G *est une base de Gröbner de* $\mathcal{I} = \langle G\rangle$. *De plus,* G *est minimal.* □

L'ensemble $\mathcal{R}$ des représentants de T joue un rôle important dans la suite du travail. Il permet d'obtenir un idéal $\mathcal{I} \subset \mathbb{K}[x]$ dont l'image réciproque par γ est l'idéal $\mathcal{J} \subset \mathbb{K}\langle X\rangle$ engendré par T.

Proposition II - 0.3. *Soit* $\mathcal{J}$ *un idéal de* $\mathbb{K}\langle X\rangle$ *contenant tous les commutateurs et admettant une base de Gröbner finie* T, *qui vérifie la propriété* P_1, *relativement à l'extension lexicographique d'un ordre monomial sur* $\mathbb{K}[x]$, $\mathcal{R}$ *l'ensemble des représentants de* T, $G = \{\gamma(g) \mid g \in \mathcal{R}\}$ *et* $\mathcal{I} = \gamma(\mathcal{J})$. *Alors* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ *et* G *est une base de Gröbner minimale de* $\mathcal{I}$.

Démonstration.
$\mathcal{I} = \gamma(\mathcal{J}) \Rightarrow \mathcal{J} \subseteq \gamma^{-1}(\mathcal{I})$ (i_1). *Notons que* $\mathcal{I} = \gamma(\mathcal{J}) = \gamma(\langle T\rangle) = \langle\gamma(T)\rangle = \langle G\rangle$.
Soit $\mathcal{J}' = \gamma^{-1}(\mathcal{I})$. *Alors, il existe une base de Gröbner minimale* T′ *de* $\mathcal{J}'$ *vérifiant*
$T' = \{X_iX_j - X_jX_i \mid i > j, x_i, x_j \notin \langle LM_{\prec}(\mathcal{I})\rangle\} \cup \{\delta(uf) \mid f \in G, u \in U_{\langle LM_{\prec}(\mathcal{I})\rangle}(LM_{\prec}(f))\}$.
Soit $h \in T'\backslash Com$. *Alors* $h = \delta(uf)$, $f \in G$ *et* $u \in U_{\langle LM_{\prec}(\mathcal{I})\rangle}(in_{\prec}(f))$.
$f \in G \Rightarrow \exists g \in \mathcal{R} \subseteq T$ *tel que* $f = \gamma(g)$. *Alors* $h = \delta(u\gamma(g))$.
Donc $\gamma(h) = u\gamma(g) \in \langle\gamma(T)\rangle$. *Ainsi,* $h = \delta(\gamma(h)) \in \delta(\langle\gamma(T)\rangle) \subset \langle T\rangle$.
Il s'en suit que $\langle T'\rangle \subseteq \langle T\rangle$ (i_2).
(i_1) *et* (i_2) *impliquent que* $\mathcal{J} = \mathcal{J}'$. □

Le résultat suivant découle assez naturellement de la *Proposition* II - 0.3.

Théorème II.1. *Soient* $\mathbb{K}$ *un corps,* $\mathbb{K}\langle X\rangle$ *et* $\mathbb{K}[x]$, *respectivement, l'anneau non commutatif et l'anneau commutatif des polynômes à indéterminées dans* $X = \{X_1, X_2, ..., X_n$ *respectivement, dans* $x = \{x_1, x_2, ..., x_n\}$. *Soit* $\mathcal{J}$ *un idéal de* $\mathbb{K}\langle X\rangle$. *Si* $\mathcal{J}$ *contient tous les commutateurs et admet une base de Gröbner finie alors il existe un idéal* $\mathcal{I}$ *de* $\mathbb{K}[x]$ *tel que* $\mathcal{J} = \gamma^{-1}(\mathcal{I})$.

De ce théorème, on déduit :

Remarque II.1. *Tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X\rangle$ contenant les commutateurs et admettant une base de Gröbner finie admet une base de Gröbner vérifiant* P_2.

En combinant le théorème précédent et le Théorème 2.1 dans [27], on obtient le résultat final suivant.

Théorème II.2. *Soit $\mathcal{J}$ un idéal de $\mathbb{K}\langle \mathrm{X}\rangle$ contenant tous les commutateurs et « l'extension lexicographique d'un ordre monomial sur $\mathbb{K}[\mathrm{x}]$. Alors $\mathcal{J}$ admet une base de Gröbner finie relativement à « si et seulement s'il existe un idéal $\mathcal{I}$ de $\mathbb{K}[\mathrm{x}]$ tel que $\mathcal{J} = \gamma^{-1}(\mathcal{I})$.*

Ce chapitre donne une caractérisation complète de la classe des idéaux non commutatifs contenant tous les commutateurs et admettant une base de Gröbner finie. Par le **Théorème** II.2, on sait qu'un idéal $\mathcal{J}$ appartenant à cette classe s'écrit nécessairement $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ où $\mathcal{I}$ est un idéal de $\mathbb{K}[\mathrm{x}]$. Egalement, si $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ alors une base de Gröbner de chacun des deux idéaux peut être déterminée à partir d'une base de Gröbner de l'autre.
Néanmoins, du travail reste à faire dans la caractérisation des idéaux non commutatifs ayant des bases de Gröbner finies.

1. Tout d'abord, dans le **Théorème** II.2, il est bien précisé que le corps de base $\mathbb{K}$ est de caractéristique nulle ; $\mathbb{K}$ est infini. Il reste donc à trouver les critères de finitude des bases de Gröber des idéaux s'exprimant sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ pour un idéal $\mathcal{I}$ commutatif au cas où $\mathbb{K}$ est fini. Résoudre ce problème pourrait permettre de généraliser le travail présenté dans ce chapitre. Cela est d'autant plus important que dans les applications pratiques notamment en cryptologie et en théorie des codes, les corps finis sont plus présents que les corps infinis. Et pour espérer utiliser convenablement les idéaux non commutatifs dans ces domaines, on doit préalablement s'assurer de la finitude des algorithmes utilisés, en particulier de l'algorithme de Buchberger. Autrement dit, on doit s'assurer de l'existence d'une base de Gröbner finie.
2. On sait également qu'il existe des idéaux non commutatifs admettant des bases de Gröbner finies mais ne s'exprimant pas sous la forme $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ pour un

idéal $\mathcal{I}$ commutatif. C'est donc un challenge de passer de la classe des idéaux étudiés dans ce chapitre à une autre classe la contenant et ainsi de suite afin de trouver les critères de reconnaissance de l'existence d'une base de Gröbner finie d'un idéal non commutatif.

3. Du point de vue mathématique, généraliser (adapter) le travail dèjà accompli aux anneaux (remplacer le corps $\mathbb{K}$ par un anneau) peut être intéressant.

Chapitre 3

Bases de Gröbner-Shirshov sur un anneau de valution noethérien

Dans ce chapitre, nous présentons une généralisation des bases de Gröbner portant à la fois sur la structure algébrique des coefficients et sur celle des monômes :

1. l'ensemble des coefficients est un anneau de valuation noté $\mathbb{V}$;
2. l'ensemble des monômes est un semi-anneau au lieu d'un monoïde (voir [9]).

Ce travail a fait l'objet du papier [23] présenté lors de la "troisième rencontre maroco-andalouse sur les algèbres et leurs applications" qui s'est tenue à Chefchaouen du 12 au 14 avril 2018.
Le chapitre est organisé comme suit :

— dans la section 1, on donne les notions et notations qu'on utlisera dans la suite ;
— dans la section 2, on définit les bases de Gröbner-Shirshov sur un anneau de valuation puis on les caractérise en donnant et prouvant le lemme de Composition correspondant.

I Concepts de base

Dans cette section, on donne les notions de base nécessaires à la définition et à la caractérisatoin des bases de Gröbner. Cette section contient également les notations qu'on utlisera dans les parties suivantes. Se réfèrer à [9] pour plus de détails.

I - 1 Anneau de valuation

La définition d'anneau de valuation est donnée à la page 29. Dans le cas des bases de Gröbner sur un anneau de valuation $\mathbb{V}$, on verra comment la relation de division garantie entre deux éléments non nuls permet de contourner certaines difficultés liées aux coefficients.

I - 2 Semi-anneau des monômes

Proposition I - 2.1. *Soit* $X = \{X_1, X_2, ..., X_n\}$ *un alphabet,* $\mathbb{M} = \{X_{i_1}X_{i_2}...X_{i_s}, X_i \in X\}$, $\mathrm{Rig}\langle X\rangle = \{u_1 \circ u_2 \circ ... \circ u_t, u_i \in \mathbb{M}\}$, *où* $\circ$ *est une loi de composition vérifiant* $u_i \circ u_j = u_j \circ u_i$ *pour tout* i, j.

1. $(\mathrm{Rig}\langle X\rangle, \circ)$ *est un monoïde commutatif d'élément neutre noté* θ.
2. *On étend la concaténation sur* $\mathbb{M}$ *à une opération "." sur* $\mathrm{Rig}\langle X\rangle$ *qui est distributive à gauche et à droite par rapport à* $\circ$. *Alors,* $(\mathrm{Rig}\langle X\rangle, ., \circ)$ *est un semi-anneau. On l'appelle le semi-anneau libre engendré par* $\mathbb{M}$ *et on le note simplement par* $Rig\langle X\rangle$.

Définition I - 2.1. *Soit* $\mathbb{V}$ *un anneau de valuation et* $\mathbb{V}\mathrm{Rig}\langle X\rangle$ *le* $\mathbb{V}$*-semimodule ayant pour base* $\mathrm{Rig}\langle X\rangle$ *et pour produits multilinéaires* $\omega \in \{., \circ\}$ *étendus par linéarité de* $\mathrm{Rig}\langle X\rangle$ *à* $\mathbb{V}\mathrm{Rig}\langle X\rangle$.
Nous appelons respectivement monôme et polynôme tout élément u *de* $\mathrm{Rig}\langle X\rangle$ *et tout élément* f *de* $\mathbb{V}\mathrm{Rig}\langle X\rangle$. *Tout idéal de* $\mathbb{V}\mathrm{Rig}\langle X\rangle$ *est appelé un* Ω*-idéal où* $\Omega = \{., \circ\}$.
Un monôme u *s'exprime sous la forme* $u = u_1 \circ u_2 \circ ... \circ u_t$ *où* $u_i = u_{i_1}u_{i_2}...u_{i_s} \in \mathbb{M}$.
Pour tout monôme $u = u_1 \circ u_2 \circ ... \circ u_t \in \mathrm{Rig}\langle X\rangle$, *l'entier naturel* t *sera appelé longueur de* u *relativement à* $\circ$. *On notera* $|u|_\circ = t$. *Si* $u_i = u_j$ *pour tout* $i, j \in [1, t]$ *alors* $u = u_1 \circ u_2 \circ ... \circ u_t$ *sera noté* $u = w^{|t|_\circ}$ *où* $w = u_1$. *Par convention* $u = \theta$ *si et seulement si* $t = 0$.
Un polynôme f *s'exprime :*

$$f = \sum_{i=1}^{n} \alpha_i u_i, \ \alpha_i \in \mathbb{V}, \ u_i \in \mathrm{Rig}\langle X\rangle$$

Exemple I - 2.1. *On donne* $X = \{x, y, z\}$, $\mathrm{Rig}\langle X\rangle = (\mathbb{M}, \cdot, \circ)$, $\mathbb{V} = \frac{\mathbb{Z}}{8\mathbb{Z}}$.
Alors $x \circ xz$, $zxy \circ xz \circ yx \circ z \circ y$, $y^{|3|_\circ}$, $z^{|4|_\circ} yz^{|2|_\circ}$, z *sont des monômes et* $f = 2x \circ xz + zxy \circ xz \circ yx \circ z \circ y + 3y^{|3|_\circ} + z^{|4|_\circ} yz^{|2|_\circ} + 3z$ *est un polynôme.*

I - 3 Ordre admissible et ordre monomial

Définition I - 3.1. *Un ordre total sur* $\mathbb{M}$ *est dit admissible s'il est compatible avec la multiplication ; c'est à dire si pour* $u, v, w, t \in \mathbb{M}$, $u \preceq v$ *implique que* $wut \preceq wvt$.

Exemple I - 3.1. *L'ordre du degré lexicographique défini par*

$$u \prec v \Leftrightarrow \begin{cases} \deg(u) < \deg(v) \\ ou \\ \deg(u) = \deg(v) \text{ et } u \prec_{\mathrm{lex}} v \end{cases}$$

est un ordre admissible sur $\mathbb{M}$.

Remarque I.1. *Si un ordre admissile est fixé sur* $\mathbb{M}$ *alors tout élément* $u \in \mathrm{Rig}\langle X\rangle$ *s'exprime de façon unique sous la forme* $u = u_1 \circ u_2 \circ ... \circ u_l$, *où* $u_i \in \mathbb{M}$ *et* $u_i \preceq u_{i+1}$ *pour tout* $i = 1, ..., l-1$.

Définition I - 3.2. *Un ordre* $\prec$ *sur* $\mathrm{Rig}\langle X\rangle$ *est dit monomial si :*

1. *il est un ordre total ;*
2. *il est un bon ordre ;*
3. *il est compatible avec la structure du semi-anneau, c'est à dire si pour tout* $u, v, w \in \mathrm{Rig}\langle X\rangle$, $t', w' \in \mathbb{M}$, *on a :*

$$u \prec v \Rightarrow \begin{cases} u \circ w \prec v \circ w \\ t'uw' \prec t'vw' \end{cases}$$

Exemple I - 3.2. *Soit* $u = u_1 \circ u_2 \circ ... \circ u_n \in \mathrm{Rig}\langle X\rangle$ *avec* $u_i \preceq u_{i+1}$, *on définit* $\mathrm{vect}(u)$ *par* $\mathrm{vect}(u) = (u_1, u_2, ..., u_n)$. *Pour comparer deux monômes* u *et* v *lexicographiquement, on compare* $\mathrm{vect}(u)$ *et* $\mathrm{vect}(v)$ *lexicographiquement en utilisant un ordre admissible sur* $\mathbb{M}$.

L'ordre de la longueur lexicographique défini par

$$u \prec_{ll} v \Leftrightarrow \begin{cases} |u|_\circ < |v|_\circ \\ ou \\ |u|_\circ = |v|_\circ \text{ et } u \prec_{lex} v \end{cases}$$

est un ordre monomial sur $\mathrm{Rig}\langle X\rangle$.

Un ordre monomial étant fixé sur $\mathbb{V}\mathrm{Rig}\langle X\rangle$, les notions et notations de monôme dominant, coefficient dominant et terme dominant restent identiques à celles des chapitres précédents.

Exemple I - 3.3. *On donne* $\mathbb{V} = \frac{\mathbb{Z}}{8\mathbb{Z}}$, $f = 4yy \circ zyzx \circ zyyx + 2z \circ xy + y \circ x + 1 \in \mathbb{V}\mathrm{Rig}\langle X\rangle$. *Considérons l'ordre de la longueur lexicographique sur* $\mathrm{Rig}\langle X\rangle$.
Alors : $\mathrm{LM}(f) = yy \circ zyzx \circ zyyx$, $\mathrm{LC}(f) = 4$, $\mathrm{LT}(f) = 4yy \circ zyzx \circ zyyx$.

Définition I - 3.3. *Soient* $u = w_1 \circ w_2 \circ ... \circ w_m \circ u_{m+1} \circ ... \circ u_n$,
$v = w_1 \circ w_2 \circ ... \circ w_m \circ v_{m+1} \circ ... \circ v_t$ *deux monômes tels que* $u_i \neq v_j$ *pour tout* $(i, j) \in [m+1, n] \times [m+1, t]$. *Alors* $d = w_1 \circ w_2 \circ ... \circ w_m \circ u_{m+1} \circ ... \circ u_n \circ v_{m+1} \circ ... \circ v_t$ *et* $w = w_1 \circ w_2 \circ ... \circ w_m$ *sont respectivement appelés plus petit commun multiple et plus grand commun diviseur de* u *et* v *relativement à* $\circ$. *On les notera* $d = \mathrm{LCM}_\circ(u, v)$ *et* $w = \gcd_\circ(u, v)$.

Exemple I - 3.4. *Si* $u = x^{|4|_\circ} \circ yz \circ zxy \circ y$ *et* $v = x \circ yz \circ z^{|2|_\circ} \circ yx \circ zx \circ y^{|3|_\circ}$ *alors*

$$\begin{aligned} \mathrm{LCM}_\circ(u, v) &= x^{|4|_\circ} \circ yz \circ zxy \circ z^{|2|_\circ} \circ yx \circ zx \circ y^{|3|_\circ} \\ &= u \circ z^{|2|_\circ} \circ yx \circ zx \circ y^{|2|_\circ} \\ &= v \circ x^{|3|_\circ} \circ zxy \end{aligned}$$

$\gcd_\circ(u, v) = x \circ y \circ yz$.

Proposition I - 3.1. *Soit* $\prec$ *un ordre monomial sur* $\mathrm{Rig}\langle X\rangle$. *Alors pour tout* $u, v, w \in \mathrm{Rig}\langle X\rangle$, *on a :*

1. $u \circ w = u \circ v \Rightarrow v = w$.
2. $u \circ v = \theta \Rightarrow u = v = \theta$.

Démonstration. *Soient* $\prec$ *un ordre monomial sur* $\mathrm{Rig}\langle X\rangle$, $u, v, w \in \mathrm{Rig}\langle X\rangle$.

1. *Supposons que* $u \circ v = u \circ w$.
   Comme $\prec$ *est un ordre monomial il est total. Donc, si* $v \neq w$ *alors* $v \prec w$ *ou* $w \prec v$. *De plus* $\prec$ *est compatible avec la structure du semi-anneau.*
   Ainsi, si $v \prec w$ *alors* $u \circ v \prec u \circ w$. *Finalement, si* $v \prec w$ *alors* $u \circ v \neq u \circ w$ *; ce qui est absurde. Donc,* $u \circ v = u \circ w \Rightarrow v = w$.
2. *Si* $u \neq \theta$ *et* $v \neq \theta$ *alors* $\theta \prec u$ *et* $\theta \prec v$. *Ainsi,* $\theta = \theta \circ \theta \prec u \circ v$. *Donc, si* $u \circ v = \theta$ *alors* $u = \theta$ *ou* $v = \theta$.
   Si $u = \theta$ *alors* $v = u \circ v = \theta$. *De même, si* $v = \theta$ *alors* $u = \theta$.

□

I - 4 Algorithme de réduction

Définition I - 4.1. *Soit* $f = \alpha_1 m_1 + \alpha_2 m_2 + ... + \alpha_t m_t, \alpha_i \in \mathbb{V}, m_i \in \mathrm{Rig}\langle X\rangle, g \in \mathbb{V}\mathrm{Rig}\langle X\rangle$ *et* $G \subset \mathbb{V}\mathrm{Rig}\langle X\rangle$.

1. *On dira que* f *est réductible modulo* g *s'il existe* $i \in [1, n]$, $a, b \in \mathbb{M}$, $u \in \mathrm{Rig}\langle X\rangle$ *tels que* $\alpha_i m_i = \alpha a \mathrm{LT}(g) b \circ u$. *Dans ce cas, le polynôme* $h = f - \alpha a g b \circ u$ *est appelé un réduit de* f *modulo* g. *On note* $f \xrightarrow{g} h$ *ou* $h = \mathrm{Red}(f, g)$.
   Sinon, f *est dit irréductible modulo* g.
2. *On dira que* f *est top-réductible modulo* g *s'il existe* $a, b \in \mathbb{M}$, $u \in \mathrm{Rig}\langle X\rangle$ *tels que* $\mathrm{LT}(f) = \alpha a \mathrm{LT}(g) b \circ u$. *Dans ce cas* $\mathrm{Red}(f, g)$ *est noté* $\mathrm{TopRed}(f, g)$.
3. *On étend cette réduction à une réduction d'un polynôme modulo un ensemble de polynômes. Le polynôme* f *est dit réductible modulo* G *s'il existe un polynôme* $g \in G$ *tel que* f *soit réductible modulo* g.
4. *On dira que* f *est totalement réduit à* g *modulo* G *s'il une séquence de réductions :* $f \xrightarrow{G} f_1 \xrightarrow{G} f_2 ... \ f_{n-1} \xrightarrow{G} f_n = g$, *où* g *est irréductible modulo* G. *On note* $\mathrm{TotRed}(f, G) = g$. *Le polynôme* f *est irréductible modulo* G *si* $\mathrm{TotRed}(f, G) = f$.

L'algorithme suivant permet de réduire totalement un polynôme f modulo un ensemble G relativement à un ordre monomial fixé sur $\mathrm{Rig}\langle X\rangle$.

Proposition I - 4.1. *L'algorithme de réduction se termine.*

Algorithme 8 : Réduction Totale

Entrée : $(f, G, \prec)$

Sortie : r : irréductible modulo G

```
1 r ← 0;
2 Tant que f ≠ 0 Faire
3     Si LT(f) = αaLT(g)b ∘ u, g ∈ G, u ∈ Rig⟨X⟩ Alors
4         f ⟵ f − αagb ∘ u
5     Sinon
6         r ← r + LT(f);
7         f ← f − LT(f);
8 return r
```

La preuve de cette proposition est analogue à celle du **Théorème I.1**.

Exemple I - 4.1. *On donne* $\mathbb{V} = \frac{\mathbb{Z}}{8\mathbb{Z}}$, $f = 4yy \circ zyzx \circ zyyx + 2z \circ xy + y \circ x + 1 \in \mathbb{V}Rig\langle X\rangle$,
$G = \{g_1 = 2zx \circ yx + 3x \circ y, g_2 = 5zy \circ y + y \circ 1, g_3 = xy + 2\} \subset \mathbb{V}Rig\langle X\rangle$. *On veut réduire* f *par* G *en utilisant l'ordre de la longueur lexicographique sur* $Rig\langle X\rangle$.
Première étape ; initialisation : r := 0
$LT(f) = 4yy \circ zyzx \circ zyyx = 2zyLT(g_1) \circ yy$. *Donc* f *est réductible par* g_1 *et on a :*
$f \xrightarrow{g_1} f_1 = f - 2zyg_1 \circ yy = 2zyx \circ zyy \circ yy + y \circ x + 2z \circ xy + 1$
$LT(f_1) = 2zyx \circ zyy \circ yy = 2LT(g_2)y \circ zyx$. *Donc* f_1 *est réductible par* g_2 *et on a :*
$f_1 \xrightarrow{g_2} f_2 = f_1 - 2g_2y \circ zyx = 6y \circ yy \circ zyx + y \circ x + 2z \circ xy + 1$
$LT(f_2) = 6y \circ yy \circ zyx$ *qui n'est divisible par aucun* $LT(g_i)$ *pour tout* $i \in \{1, 2, 3\}$.
Donc r := $6y \circ yy \circ zyx$ *et* $f_3 = f_2 - LT(f_2) = y \circ x + 2z \circ xy + 1$
$LT(f_3) = y \circ x$ *qui n'est divisible par aucun* $LT(g_i)$ *pour tout* $i \in \{1, 2, 3\}$.
Donc r := $6y \circ yy \circ zyx + y \circ x$ *et* $f_4 = f_3 - LT(f_3) = 2z \circ xy + 1$
$LT(f_4) = 2z \circ xy = 2z \circ LT(g_3)$. *Donc* f_4 *est réductible modulo* g_3 *et on a :*
$f_4 \xrightarrow{g_3} f_5 = f_4 - 2z \circ g_3 = 4z \circ 1 + 1$
$LT(f_5) = 4z \circ 1$ *qui n'est divisible par aucun* $LT(g_i)$ *pour tout* $i \in \{1, 2, 3\}$.
Donc r := $6yy \circ y \circ zyx + 4z \circ 1$ *et* $f_6 = f_5 - LT(f_5) = 1$
$LT(f_6) = 1$ *qui n'est divisible par aucun* $LT(g_i)$ *pour tout* $i \in \{1, 2, 3\}$.
Donc r := $6yy \circ y \circ zyx + 4z \circ 1 + 1$ *et* $f_7 = f_6 - LT(f_6) = 0$.

Alors, l'algorithme s'arrête.
$\mathrm{r} := 6\mathrm{yy} \circ \mathrm{y} \circ \mathrm{zyx} + 4\mathrm{z} \circ 1 + 1$ *est un réduit* f *modulo* G.

II Bases de Gröbner-Shirshov sur un anneau de valuation noethérien

II - 1 Bases de Gröbner fortes et bases de Gröbner faibles

L'absence de relation de division entre deux éléments quelconques non nuls dans certains anneaux entraîne la définition de deux types de bases de Gröbner sur les anneaux : les bases de Gröbner fortes et les bases de Gröbner faibles.

Définition II - 1.1. *Soit* $\mathbb{V}$ *un anneau,* $\mathrm{G} \subset \mathbb{V}Rig\langle X\rangle$, $\mathcal{I}$ *l'idéal de* $\mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle$ *engendré par* G *et* " $\preceq$ " *un ordre monomial sur* $\mathrm{Rig}\langle \mathrm{X}\rangle$.

1. G *est une base de Gröbner-Shirshov faible (Weak-GS) de* $\mathcal{I}$ *relativement à* $\preceq$ *si* $\langle \mathrm{LT(G)}\rangle = \langle \mathrm{LT}(\mathcal{I})\rangle$.
2. G *est une base de Gröbner-Shirshov forte (Strong-GS) de* $\mathcal{I}$ *relativement à* $\preceq$ *si pour tout* $\mathrm{f} \in \mathcal{I}$ *il existe* $\mathrm{g} \in \mathrm{G},\ \mathrm{a}, \mathrm{b} \in \mathbb{M},\ \mathrm{u} \in \mathrm{Rig}\langle \mathrm{X}\rangle,\ \alpha \in \mathbb{V}$ *tels que* $\mathrm{LT(f)} = \alpha \mathrm{aLT(g)b} \circ \mathrm{u}$.

Exemple II - 1.1.

1. *Si* G *est un ensemble de termes alors* G *est une base de Gröbner-Shirshov forte relativement à tout ordre monomial.*
2. $\mathrm{G} = \{\mathrm{g}_1 = 2\mathrm{z} \circ \mathrm{x} \circ \mathrm{xy} \circ \mathrm{y} + 3\mathrm{x} \circ \mathrm{z} \circ 1,\ \mathrm{g}_2 = 3\mathrm{x} \circ \mathrm{z} \circ 1\} \subseteq \frac{\mathbb{Z}}{4\mathbb{Z}}\mathrm{Rig}\langle \mathrm{X}\rangle$ *est une base de Gröbner-Shirshov forte de* $\langle G\rangle$ *relativement à l'ordre de la longueur lexicographique.*
   Soit $\mathrm{G}' = \{\mathrm{g}'_1 = \mathrm{g}_1 - \mathrm{g}_2,\ \mathrm{g}_2\}$. *On peut facilement vérifier que* $\langle \mathrm{G}\rangle = \langle \mathrm{G}'\rangle$ *et* $\mathrm{LT(G)} = \mathrm{LT(G}')$. *Puisque* G′ *est une base de Gröbner-Shirshov forte, pour tout* $\mathrm{f} \in \langle \mathrm{G}\rangle$ *il existe* $\mathrm{g}' \in \mathrm{G}',\ \mathrm{a}, \mathrm{b} \in \mathbb{M},\ \mathrm{u} \in \mathrm{Rig}\langle \mathrm{X}\rangle,\ \alpha \in \mathbb{V}$ *tel que* $\mathrm{LT(f)} = \alpha \mathrm{aLT(g')b} \circ \mathrm{u}$. *De façon équivalente, il existe* $\mathrm{g} \in \mathrm{G},\ \mathrm{a}, \mathrm{b} \in \mathbb{M},\ \mathrm{u} \in \mathrm{Rig}\langle \mathrm{X}\rangle,\ \alpha \in \mathbb{V}$ *tel que* $\mathrm{LT(f)} = \alpha \mathrm{aLT(g)b} \circ \mathrm{u}$.

Proposition II - 1.1. *Soit* $\mathbb{V}$ *un anneau et* $\mathbb{V}Rig\langle X\rangle$ *l'anneau des polynômes à coefficients dans* $\mathbb{V}$. *Alors*

1. *toute base de Gröbner-Shirshov forte* $\mathbb{V}Rig\langle X\rangle$ *est faible de ;*
2. *si* $\mathbb{V}$ *est un anneau de valuation alors toute base de Gröbner-Shirshov faible est aussi forte.*

Démonstration.

1. *Soit* G *une base de Gröbner-Shirshov forte et* $f \in \mathcal{I}$. *Alors il existe* $g \in G$, $a, b \in \mathbb{M}$, $u \in \mathrm{Rig}\langle X\rangle$ *tels que* $LT(f) = \alpha a Lt(g) b \circ u$. *Ainsi* $LT(f) \in \langle LT(G)\rangle$. *Donc* $\langle LT(\mathcal{I})\rangle \subseteq \langle LT(G)\rangle$. *Il s'en suit que* $\langle LT(\mathcal{I})\rangle = \langle LT(G)\rangle$.
2. *Soit* $\mathbb{V}$ *un anneau de valuation,* G *une base de Gröbner-Shirshov faible et* $f \in \mathcal{I}$. *Comme* $f \in \mathcal{I}$, *on a* $LT(f) \in LT(\mathcal{I}) \subset \langle LT(\mathcal{I})\rangle = \langle LT(G)\rangle$.
Ainsi : $LT(f) = \sum_{i,j} \alpha_{i,j} a_{i,j} LT(g_i) b_{i,j} \circ u_{i,j}$, $\alpha_{i,j} \in V, a_{i,j}, b_{i,j} \in \mathbb{M}, u_{i,j} \in \mathrm{Rig}\langle X\rangle, g_i \in G$.
Il est possible de choisir l'expression de $LT(f)$ *de telle sorte que* $a_{i,j} LM(g_i) b_{i,j} \circ u_{i,j} = LM(f)$ *pour tout* (i, j).
Soit (i_0, j_0) *tel que*

$$LM(f) = a_{i_0,j_0} LM(g_{i_0}) b_{i_0,j_0} \circ u_{i_0,j_0} = a_{i,j} LM(g_i) b_{i,j} \circ u_{i,j}$$

et $LC(g_{i_0})$ *divise* $LC(g_i)$ $\forall (i, j)$. *Ainsi, pour tout* i *il existe* $\beta_i \in \mathbb{V}$ *tel que* $LC(g_i) = \beta_i LC(g_{i_0})$. *Il s'en suit que :*

$$\begin{aligned}
LT(f) &= \sum_{i,j} \alpha_{i,j} a_{i,j} LT(g_i) b_{i,j} \circ u_{i,j} \\
&= \sum_{i,j} \alpha_{i,j} LC(g_i) a_{i,j} LM(g_i) b_{i,j} \circ u_{i,j} \\
&= \sum_{i,j} \alpha_{i,j} \beta_i LC(g_{i_0}) a_{i,j} LM(g_i) b_{i,j} \circ u_{i,j} \\
&= \sum_{i,j} \alpha_{i,j} \beta_i LC(g_{i_0}) a_{i_0,j_0} LM(g_{i_0}) b_{i_0,j_0} \circ u_{i_0,j_0} \\
&= (\sum_{i,j} \alpha_{i,j} \beta_i) a_{i_0,j_0} LT(g_{i_0}) b_{i_0,j_0} \circ u_{i_0,j_0} \\
&= \alpha a_{i_0,j_0} LT(g_{i_0}) b_{i_0,j_0} \circ u_{i_0,j_0} \text{ with } \alpha = \sum_{i,j} \alpha_{i,j} \beta_i
\end{aligned}$$

Donc, G *est une base de Gröbner-Shirshov forte.*

□

Remarque II.1. *Sachant que tout anneau noethérien est de chaîne finie, on peut se réfèrer à [49] pour une autre démonstration de la proposition précédente.*

II - 2 Caractérisation des bases de Gröbner-Shirshov sur un anneau de valuation

Dans la suite, $\mathbb{V}$ désigne toujours un anneau de valuation. Ainsi, base de Gröbner-Shirshov forte et base de Gröbner faible sont identiques. La notion de composition est très importante pour la théorie des bases de Gröbner. Elle permet de vérifier si un ensemble donné de polynômes est une base de Gröbner relativement à un ordre monomial fixé ou non. Dans ce qui suit, on la définit dans les cas commutatif et non commutatif tenant compte du semi-anneau (ensemble des monômes) et un anneau de valuation (ensemble des coefficients).

Définition II - 2.1.

1. *Cas commutatif : on suppose que* $\mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle$ *est un semi-anneau commutatif.*
   Soient $\mathrm{f}, \mathrm{g} \in \mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle,\ \mathrm{a}, \mathrm{c} \in \mathbb{M}$. *Il existe* $\mathrm{u}, \mathrm{v} \in \mathrm{Rig}\langle \mathrm{X}\rangle$ *tels que :*
   $\mathrm{LCM}_{\circ}(\mathrm{aLM(f)}, \mathrm{cLM(g)}) = \mathrm{aLM(f)} \circ \mathrm{u} = \mathrm{cLM(g)} \circ \mathrm{v}$. *Le polynôme*

$$\mathcal{O}(\mathrm{f}, \mathrm{g}, \mathrm{a}, \mathrm{c}, \mathrm{u}, \mathrm{v}) = \begin{cases} \mathrm{af} \circ \mathrm{u} - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}} \mathrm{cg} \circ \mathrm{v} \ \textit{si}\ \mathrm{LC(g)}\ \textit{divise}\ \mathrm{LC(f)} \\ \frac{\mathrm{LC(g)}}{\mathrm{LC(f)}} \mathrm{af} \circ \mathrm{u} - \mathrm{cg} \circ \mathrm{v}\ \textit{sinon} \end{cases}$$

   est appelé composition de f *et* g *relativement à* $\mathrm{w} = \mathrm{LCM}_{\circ}(\mathrm{aLM(f)}, c\mathrm{LM(g)})$.

2. *Cas non commutatif : on suppose que* $\mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle$ *est un semi-anneau non commutatif.*
   Soient $\mathrm{f}, \mathrm{g} \in \mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle,\ \mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d} \in \mathbb{M}$. *Il existe* $\mathrm{u}, \mathrm{v} \in \mathrm{Rig}\langle \mathrm{X}\rangle$ *tels que :*
   $\mathrm{LCM}_{\circ}(\mathrm{aLM(f)b}, \mathrm{cLM(g)d}) = \mathrm{aLM(f)b} \circ \mathrm{u} = \mathrm{cLM(g)d} \circ \mathrm{v}$. *Le polynôme*

$$\mathcal{O}(\mathrm{f}, \mathrm{g}, \mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{u}, \mathrm{v}) = \begin{cases} \mathrm{afb} \circ \mathrm{u} - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}} \mathrm{cgd} \circ \mathrm{v} \ \textit{si}\ \mathrm{LC(g)}\ \textit{divise}\ \mathrm{LC(f)} \\ \frac{\mathrm{LC(g)}}{\mathrm{LC(f)}} \mathrm{afb} \circ \mathrm{u} - \mathrm{cgd} \circ \mathrm{v}\ \textit{sinon} \end{cases}$$

est appelé composition de f *et* g *relativement à* $\mathrm{w} = \mathrm{LCM}_\circ(\mathrm{aLM(f)b}, \mathrm{cLM(g)d})$. *L'ensemble de toutes les compositions entre* f *et* g *est noté* $\mathcal{O}(\mathrm{f},\mathrm{g})$ *et* $\mathcal{O}(\mathrm{G})$ *l'ensemble de toutes les compositions définies dans* G.

Remarque II.2.

1. *Pour tout* $\mathrm{f},\mathrm{g} \in \mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle$, $\mathcal{O}(\mathrm{f},\mathrm{g}) \neq \varnothing$.
2. *Soit* $\mathrm{f},\mathrm{g} \in \mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle$ *tel que* $\mathrm{LM(f)} = \mathrm{LM(g)}$. *Alors* $\mathcal{O}(\mathrm{f},\mathrm{g},1,1,1,1,\theta,\theta) \in \mathcal{O}(\mathrm{f},\mathrm{g})$. *On l'appelle composition simple de* f *et* g *et on la note* $\widetilde{\mathcal{O}}(\mathrm{f},\mathrm{g})$.
3. *La définition que nous avons donnée généralise celle donnée dans [9, p.5, def 3.1]. Par exemple, dans le cas non commutatif, il suffit de prendre respectivement* $(\mathrm{a},\mathrm{d}) = (1,1)$ *et* $(\mathrm{a},\mathrm{b}) = (1,1)$ *pour obtenir la composition d'intersection et la composition d'inclusion telles que dans [9]. Cependant, dans [9], les auteurs considèrent uniquement les compositions qui vérifient* $|\mathrm{LCM}_\circ(\mathrm{aLM(f)b}, \mathrm{cLM(g)d})|_\circ < |\mathrm{aLM(f)b}|_\circ + |\mathrm{cLM(g)d}|_\circ$.
Cette restriction est dûe au fait que l'ensemble de coefficients considéré dans [9] est un corps. Ainsi, si $|\mathrm{LCM}_\circ(\mathrm{aLM(f)b}, \mathrm{cLM(g)d})|_\circ = |\mathrm{aLM(f)b}|_\circ + |\mathrm{cLM(g)d}|_\circ$ *ou de façon équivalente,* $\mathrm{gcd}_\circ(\mathrm{aLM(f)b}, \mathrm{cLM(g)d}) = \theta$ *alors* $\mathcal{O}(\mathrm{f},\mathrm{g},\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{d},\mathrm{u},\mathrm{v})$ *est toujours réduit à zéro modulo* $\{\mathrm{f},\mathrm{g}\}$. *En général, tel n'est pas le cas dans un anneau de valuation.*

Exemple II - 2.1.

On donne $\mathrm{f} = 5\mathrm{yz}\circ\mathrm{zx}\circ\mathrm{x}\circ 1 + 2\mathrm{xy}\circ\mathrm{z} + \mathrm{z}\circ 1, \mathrm{g} = 2\mathrm{xy}\circ\mathrm{y}\circ\mathrm{z}\circ 1 + 3\mathrm{x}\circ\mathrm{z}\circ 1 \in \frac{\mathbb{Z}}{8\mathbb{Z}}\mathrm{Rig}\langle \mathrm{X}\rangle$ *et l'ordre de la longueur lexicographique. On suppose que* $\mathbb{V}\mathrm{Rig}\langle \mathrm{X}\rangle$ *n'est pas commutatif. Alors* $\mathrm{LM(f)} = \mathrm{yz}\circ\mathrm{zx}\circ\mathrm{x}\circ 1,\ \mathrm{LM(g)} = \mathrm{xy}\circ\mathrm{y}\circ\mathrm{z}\circ 1$.

1. *On donne* $(\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{d}) = (\mathrm{xy},\mathrm{z},1,\mathrm{xz})$.

$$\begin{aligned}\mathrm{LCM}_\circ(\mathrm{xyLM(f)z}, \mathrm{LM(g)xz}) &= \mathrm{xyyzz}\circ\mathrm{xyzxz}\circ\mathrm{xyz}\circ\mathrm{xyxz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}\\ &= \mathrm{xyLM(f)z}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}\\ &= \mathrm{LM(g)xz}\circ\mathrm{xyyzz}\circ\mathrm{xyzxz}\circ\mathrm{xyz}\end{aligned}$$

$$\begin{aligned}\mathcal{O}(\mathrm{f},\mathrm{g},\mathrm{xy},\mathrm{z},1,\mathrm{xz},\mathrm{u},\mathrm{v}) &= 2\mathrm{xyfz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz} - \mathrm{gxz}\circ\mathrm{xyyzz}\circ\mathrm{xyzxz}\circ\mathrm{xyz}\\ &= 2\mathrm{xyyzz}\circ\mathrm{xyzxz}\circ\mathrm{xyz}\circ\mathrm{xyxz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}\\ &\quad +4\mathrm{xyxyz}\circ\mathrm{xyzz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}\end{aligned}$$

$$
\begin{aligned}
&+2\mathrm{xyzz}\circ\mathrm{xyz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}\\
&-2\mathrm{xyyzz}\circ\mathrm{xyzxz}\circ\mathrm{xyz}\circ\mathrm{xyxz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}\\
&-3\mathrm{xxz}\circ\mathrm{zxz}\circ\mathrm{xz}\circ\mathrm{xyyzz}\circ\mathrm{xyzxz}\circ\mathrm{xyz}\\
&=4\mathrm{xyxyz}\circ\mathrm{xyzz}\circ\mathrm{yxz}\circ\mathrm{zxz}\circ\mathrm{xz}+2\mathrm{xyzz}\circ\mathrm{xyz}\circ\mathrm{yxz}
\end{aligned}
$$

2. *On donne* $(\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{d})=(\mathrm{zx},\mathrm{xy},\mathrm{z},\mathrm{xy})$.

$$
\begin{aligned}
\mathrm{LCM}_\circ(\mathrm{zxLM(g)xy},\mathrm{zLM(g)xy}) &= \mathrm{zxxyxy}\circ\mathrm{zxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&= \mathrm{zxLM(g)xy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&= \mathrm{zLM(g)xy}\circ\mathrm{zxxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\\
\mathcal{O}(\mathrm{g},\mathrm{g},\mathrm{zx},\mathrm{xy},\mathrm{z},\mathrm{xy},\mathrm{u},\mathrm{v}) &= \mathrm{zxgxy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&\quad -\mathrm{zgxy}\circ\mathrm{zxxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\\
&= 2\mathrm{zxxyxy}\circ\mathrm{zxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&\quad +3\mathrm{zxxxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&\quad -2\mathrm{zxxyxy}\circ\mathrm{zxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&\quad -3\mathrm{zxxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\circ\mathrm{zxxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\\
&= 3\mathrm{zxxxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}\circ\mathrm{zyxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\\
&\quad +5\mathrm{zxxy}\circ\mathrm{zzxy}\circ\mathrm{zxy}\circ\mathrm{zxxyxy}\circ\mathrm{zxzxy}\circ\mathrm{zxxy}
\end{aligned}
$$

Dans tout ce qui reste, on suppose que $\mathbb{V}\mathrm{Rig}\langle\mathrm{X}\rangle$ n'est pas nécessairement commutatif.

Jusqu'ici, le célèbre critère de Buchberger dépendait exclusivement des S-polynômes. Cependant, si la structure algébrique des coefficients est un anneau contenant des diviseurs de zéro, le fait que tous les S-polynômes soient réduits à zéro n'entraînent pas forcément que l'ensemble considéré est une base de Gröbner-Shirshov. Autrement dit, les S-polynômes ne suffisent pas à eux seuls pour caractériser les bases de Gröbner-Shirshov. Cela se voit dans l'exemple suivant.

Exemple II - 2.2.
Soient $\mathrm{X}=\{\mathrm{x}\}$, $\mathrm{G}=\{\mathrm{f}=2\mathrm{x}\circ\mathrm{x}-1\circ 1,\mathrm{x}^{\mathrm{m}}\circ\mathrm{x}^{\mathrm{m}}-\mathrm{x}^{\mathrm{n}}\circ\mathrm{x}^{\mathrm{n}},\ \mathrm{m}>\mathrm{n}\in\mathbb{N}^*\}\subseteq\frac{\mathbb{Z}}{4\mathbb{Z}}\mathrm{Rig}\langle\mathrm{X}\rangle$. *Considérons l'ordre de la longueur lexicographique sur* $\mathrm{Rig}\langle\mathrm{X}\rangle$. *Dans ce qui suit, on vérifie que toutes les compositions définies dans* G *sont réduites à zéro modulo* G.

1. *Compsitions entre* f *et lui-même : Soit* $\mathcal{O}(f, f, x^k, x^l, u, v) \in \mathcal{O}(f, f)$.

$$x^k LM(f) \circ u = x^l LM(f) \circ v \Rightarrow x^{k+1} \circ x^{k+1} \circ u = x^{l+1} \circ x^{l+1} \circ v \ (\star)$$
$$\Rightarrow |u|_\circ = |v|_\circ$$
$$\Rightarrow u = x^{m_1} \circ x^{m_2} \circ ... \circ x^{m_r},\ v = x^{n_1} \circ x^{n_2} \circ ... \circ x^{n_r}$$

Alors

$$\begin{aligned}\mathcal{O}(f, f, x^k, x^l, u, v) &= x^k f \circ u - x^l f \circ v \\ &= x^k(2x \circ x - 1 \circ 1) \circ u - x^l(2x \circ x + 1 \circ 1) \circ v \\ &= 2x^{k+1} \circ x^{k+1} \circ u - x^k \circ x^k \circ u - 2x^{l+1} \circ x^{l+1} \circ v \\ &\quad + x^l \circ x^l \circ v = x^l \circ x^l \circ v - x^k \circ x^k \circ u\end{aligned}$$

Si $k = l$ *alors* $u = v$ *et* $\mathcal{O}(f, f, x^k, x^l, u, v) = 0$.
Sinon, il existe $i, j, i', j' \in [1, r]$ *tels que* $k + 1 = n_{i'} = n_{j'}$ *et* $l + 1 = m_i = m_j$.
Sans perte de généralité, on peut supposer que $i = i' = 1$ *et* $j = j' = 2$.
Donc, on obtient $x^{m_1} \circ x^{m_2} \circ ... \circ x^{m_r} = x^{l+1} \circ x^{l+1} \circ x^{m_3} \circ ... \circ x^{m_r}$
et $v = x^{n_1} \circ x^{n_2} \circ ... \circ x^{n_r} = x^{k+1} \circ x^{k+1} \circ x^{n_3} \circ ... \circ x^{n_r}$
Donc, la relation $(\star)$ *devient :*

$$x^{k+1} \circ x^{k+1} \circ x^{l+1} \circ x^{l+1} \circ x^{m_3} \circ ... \circ x^{m_r} = x^{l+1} \circ x^{l+1} \circ x^{k+1} \circ x^{k+1} \circ x^{n_3} \circ ... \circ x^{n_r}$$

Ainsi, $\gcd_\circ(u, v) = x^{m_3} \circ ... \circ x^{m_r} = x^{n_3} \circ ... \circ x^{n_r} = t$

$$\begin{aligned}\mathcal{O}(f, f, x^k, x^l, u, v) &= x^l \circ x^l \circ v - x^k \circ x^k \circ u \\ &= x^l \circ x^l \circ x^{k+1} \circ x^{k+1} \circ t - x^k \circ x^k \circ x^{l+1} \circ x^{l+1} \circ t\end{aligned}$$

Soit $\gamma = \max\{l + 1, k + 1\}$, $\gamma' = \min\{l + 1, k + 1\}$. *Sans perte de généralité, on peut supposer que* $\gamma = k + 1$ *et* $\gamma' = l + 1$.
On note également $x_\gamma = x^\gamma \circ x^\gamma - x^{\gamma-1} \circ x^{\gamma-1}$ *et* $x_{\gamma'} = x^{\gamma'} \circ x^{\gamma'} - x^{\gamma'-1} \circ x^{\gamma'-1}$.
Alors

$$\begin{aligned}\mathcal{O}(f, f, x^k, x^l, u, v) &= x^\gamma \circ x^\gamma \circ x^{\gamma'-1} \circ x^{\gamma'-1} \circ t - x^{\gamma-1} \circ x^{\gamma-1} \circ x^{\gamma'} \circ x^{\gamma'} \circ t \\ &\xrightarrow{x_\gamma} x^{\gamma-1} \circ x^{\gamma-1} \circ x^{\gamma'-1} \circ x^{\gamma'-1} \circ t - x^{\gamma-1} \circ x^{\gamma-1} \circ x^{\gamma'} \circ x^{\gamma'} \circ t \\ &\xrightarrow{x_{\gamma'}} 0\end{aligned}$$

Soient $g_i = x^{m_i} \circ x^{m_i} - x^{n_i} \circ x^{n_i}$ *et* $g_j = x^{m_j} \circ x^{m_j} - x^{n_j} \circ x^{n_j}$, $m_i, n_i, m_j, n_j \in \mathbb{N}^*$ *tels que* $m_i > n_i$ *et* $m_j > n_j$.
Les mêmes arguments que précédemment permettent de conclure que les autres compositions données ci-après sont toutes réduites à zéro.

2. *Composition entre* g_i , $g_j \in G$ *:*

$$\begin{aligned}\mathcal{O}(g_i, g_j, x^k, x^l, u, v) &= x^k g_i \circ u - x^l g_j \circ v \\ &= x^{k+m_i} \circ x^{k+m_i} \circ u - x^{k+n_i} \circ x^{k+n_i} \circ u \\ &- x^{l+m_j} \circ x^{l+m_j} \circ v + x^{l+n_j} \circ x^{l+n_j} \circ v \\ &= x^{l+n_j} \circ x^{l+n_j} \circ v - x^{k+n_i} \circ x^{k+n_i} \circ u\end{aligned}$$

3. *Composition entre* f *et* $g_i \in G$ *:*

$$\begin{aligned}\mathcal{O}(f, g_i, x^k, x^l, u, v) &= x^k f \circ u - 2x^l g_i \circ v \\ &= 2x^{k+1} \circ x^{k+1} \circ u - x^k \circ x^k \circ u - 2x^{l+m_i} \circ x^{l+m_i} \\ &+ 2x^{l+n_i} \circ x^{l+n_i} \circ v \\ &= 2x^{l+n_i} \circ x^{l+n_i} \circ v - x^k \circ x^k \circ u\end{aligned}$$

Mais $LT(2f) = LT(2(2x \circ x - 1 \circ 1)) = 2(1 \circ 1) \notin \langle LT(G) \rangle$. *Donc* G *n'est pas une base de Gröbner-Shirshov de* $\langle G \rangle$ *mêmes si toutes les compositions sont réduites à zéro modulo* G.

Dans le cas d'un anneau de valuation noethérien, en adjoignant la notion de a-*polynôme* à celle de S-polynôme, on obtient une caractérisation complète des bases de Gröbner-Shirshov. En d'autres termes, on obtient une version du critère de Buchberger.

Définition II - 2.2. *Soit* $\mathbb{V}$ *un anneau et* $a \in \mathbb{V}$. *On appelle annulateur de* a *l'ensemble noté* $\mathrm{Ann}(a)$ *et donné par* $\mathrm{Ann}(a) = \{b \in \mathbb{V} : ab = 0\}$.

Définition II - 2.3. *Soit* $\mathbb{V}$ *un anneau de valuation noethérien et* $0 \neq f \in \mathbb{V}\mathrm{Rig}\langle X\rangle$. *On définit :*

1. $a\text{-pol}^1(f) = a_1 f$ *où* $\langle a_1\rangle = \mathrm{Ann}(\mathrm{LC}(f))$
   $a\text{-pol}^i(f) = a\text{-pol}(a\text{-pol}^{i-1}(f)) = a_i(a\text{-pol}^{i-1}(f))$ *où* $\langle a_i\rangle = \mathrm{Ann}(\mathrm{LC}(a\text{-pol}^{i-1}(f))$.
2. $A\text{-pol}(f) = \bigcup_{i=1}^{m}\{a - \mathrm{pol}^i(f)\}$, *où* $m = \max\{i \in \mathbb{N} : a - \mathrm{pol}^i(f) \neq 0\}$
3. $A\text{-pol}(G) = \bigcup_{f\in G} A\text{-pol}(f)$.

Exemple II - 2.3.
Soit $f = 6xy \circ z \circ 1 \circ 1 + 4zz \circ x \circ y + 5x \circ x \circ 1 + 1 \circ 1 + 2y \in \frac{\mathbb{Z}}{9\mathbb{Z}}\mathrm{Rig}\langle X\rangle$ *et* $\prec_{ll}$ *l'ordre de la longueur lexicographique. Alors :*
$a\text{-pol}^1(f) = 3f = 3zz \circ x \circ y + 6x \circ x \circ 1 + 3(1 \circ 1) + 6y$
$a\text{-pol}^2(f) = 3a\text{-pol}^1(f) = 0$
$A\text{-pol}(f) = \{3zz \circ x \circ y + 6x \circ x \circ 1 + 3(1 \circ 1) + 6y, 0\}$

Remarque II.3. *Remarquons que si* $a\text{-pol}^i(f) = 0$ *alors* $a\text{-pol}^j(f) = 0$ *pour tout* $j > i$.

Lemme II.1. *Soit* $g \in G$ *tel que tout élément de* $A\text{-pol}(g)$ *soit réduit à zéro modulo* G. *Alors pour tout* $\alpha \in \mathbb{V}$ *tel que* $\alpha g \neq 0$, *il existe* $\beta_i \in \mathbb{V}, a_i, b_i \in \mathbb{M}, u_i \in \mathrm{Rig}\langle X\rangle, g_i \in G$ *tels que*
$\alpha g = \sum_i \beta_i a_i g_i b_i \circ u_i,\ \beta_i \mathrm{LC}(g_i) \neq 0\ \forall i$ *et* $\mathrm{LM}(\alpha g) = \max\{\mathrm{LM}(\beta_i a_i g_i b_i \circ u_i)\}$.

Démonstration. *Soit* $g \in G$ *tel que tout élément de* $A\text{-pol}(g)$ *soit réduit à zéro modulo* G *et* $\alpha \in \mathbb{V}$.
Si $\alpha\mathrm{LC}(g) \neq 0$ *alors l'expression* αg *convient.*
Sinon $\alpha g \in A\text{-pol}(g)$. *Donc, il existe* $h_1 \in G$ *tel que* $\mathrm{LT}(\alpha g) = \beta_1 a_1 \mathrm{LT}(h_1) b_1 \circ u_1$ *avec* $\beta_1 \in \mathbb{V}, a_1, b_1 \in \mathbb{M}, u_1 \in \mathrm{Rig}\langle X\rangle$. *Donc* $\beta_1\mathrm{LC}(h_1) \neq 0$.
On réduit αg *par* h_1. *On obtient :* $g_1 = \alpha g - \beta_1 a_1 h_1 b_1 \circ u_1$.
$\alpha g = \beta_1 a_1 h_1 b_1 \circ u_1 + g_1$ $(\star)$
Si $g_1 = 0$ *alors* $\alpha g = \beta_1 a_1 h_1 b_1 \circ u_1$.

Si $g_1 \neq 0$ *alors* $\mathrm{LM}(g_1) \prec \mathrm{LM}(\alpha g) = \mathrm{LM}(\beta_1 a_1 h_1 b_1 \circ u_1) = a_1 \mathrm{LM}(h_1) b_1 \circ u_1$.
De même, il existe $h_2 \in G$ *tel que* $\mathrm{LT}(g_1) = \beta_2 a_2 \mathrm{LT}(h_2) b_2 \circ u_2$. *En réduisant* g_1 *par* h_2, *on a :* $g_2 = g_1 - \beta_2 a_2 h_2 b_2 \circ u_2$ *satisfaisant* $\mathrm{LM}(g_2) \prec \mathrm{LM}(g_1)$.
La relation $(\star)$ *devient :* $\alpha g = \beta_1 a_1 h_1 b_1 \circ u_1 + \beta_2 a_2 \mathrm{LT}(h_2) b_2 \circ u_2 + g_2$.
Quand la réduction se termine, on obtient :
$\alpha g = \sum_i \beta_i a_i g_i b_i \circ u_i,\ \beta_i \in V, a_i, b_i \in \mathbb{M}, u_i \in \mathrm{Rig}\langle X\rangle, g_i \in G.$ □

Lemme II.2. *Soit* G *un ensemble de polynômes tel que tout a-polynôme défini dans* G *soit réduit à zéro modulo* G. *Alors*

$$f = \sum_{i,j} \alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j},\ \alpha_{i,j} \in V,\ a_{i,j}, b_{i,j} \in \mathbb{M},\ g_i \in G\ , u_{i,j} \in \mathrm{Rig}\langle X\rangle$$

peut être réécrit :

$$f = \sum_{k,l} \lambda_{k,l} c_{k,l} g_k d_{k,l} \circ v_{k,l},\ \lambda_{k,l} \in V,\ c_{k,l}, d_{k,l} \in \mathbb{M},\ g_k \in G\ , v_{k,l} \in \mathrm{Rig}\langle X\rangle$$

satisfaisant $\lambda_{k,l}\mathrm{LC}(g_k) \neq 0$ *et*
$\max\{\mathrm{LM}(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j})\} = \max\{\mathrm{LM}(\lambda_{k,l} c_{k,l} g_k d_{k,l} \circ v_{k,l})\}$

Démonstration.
Soit $f = \sum_{i,j} \alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j},\ \alpha_{i,j} \in \mathbb{V},\ a_{i,j}, b_{i,j} \in \mathbb{M},\ g_i \in G\ , u_{i,j} \in \mathrm{Rig}\langle X\rangle$,
$\gamma = \max\{\mathrm{LM}(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j})\}$, $\Gamma = \{(i,j) : \mathrm{LM}(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}) = \gamma\}$
Soit $(i,j) \in \Gamma$ *tel que* $\alpha_{i,j}\mathrm{LC}(g_i) = 0$.
$\alpha_{i,j}\mathrm{LC}(g_i) = 0 \Rightarrow \alpha_{i,j} g_i \in$ A-pol(g_i). *Puisque tout* a-polynôme *est réduit à zéro modulo* G, *le lemme précédent implique :* $\alpha_{i,j} g_i = \sum_{k,l} \beta_{k,l} c_{k,l} g_k b_{k,l} \circ v_{k,l}$ *avec* $\beta_{k,l}\mathrm{LC}(g_k) \neq 0$ *et*
$\mathrm{LM}(\beta_{k,l} c_{k,l} g_k b_{k,l} \circ v_{k,l}) = \mathrm{LM}(c_{k,l} g_k b_{k,l} \circ v_{k,l}) \preceq \mathrm{LM}(\alpha_{i,j} g_i)$.
Donc $\mathrm{LM}(\beta_{k,l} a_{i,j} c_{k,l} g_k b_{k,l} b_{i,j} \circ a_{i,j} v_{k,l} b_{i,j} \circ u_{i,j}) = \mathrm{LM}(a_{i,j} c_{k,l} g_k b_{k,l} b_{i,j} \circ a_{i,j} v_{k,l} b_{i,j} \circ u_{i,j})$
Or $\mathrm{LM}(a_{i,j} c_{k,l} g_k b_{k,l} b_{i,j} \circ a_{i,j} v_{k,l} b_{i,j} \circ u_{i,j}) \preceq \mathrm{LM}(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}) = \gamma$.
Ainsi, $\mathrm{LM}(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}) = \gamma = \max\{\mathrm{LM}(\beta_{k,l} a_{i,j} c_{k,l} g_k b_{k,l} b_{i,j} \circ a_{i,j} v_{k,l} b_{i,j} \circ u_{i,j})\}$.
Finalement, l'expression :
$\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j} = \sum_{k,l} \beta_{k,l} a_{i,j} c_{k,l} g_k b_{k,l} b_{i,j} \circ a_{i,j} v_{k,l} b_{i,j} \circ u_{i,j}$ *satisfait* $\beta_{k,l}\mathrm{LC}(g_k) \neq 0$ *et*
$\mathrm{LM}(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}) = \gamma = \max\{\mathrm{LM}(\beta_{k,l} a_{i,j} c_{k,l} g_k b_{k,l} b_{i,j} \circ a_{i,j} v_{k,l} b_{i,j} \circ u_{i,j})\}$.

En appliquant cette procédure à tout $(i,j) \in \Gamma$ *tel que* $\alpha_{i,j}LC(g_i) = 0$ *on obtient une expression de* f *satisfaisant la condition recherchée.* □

Définition II - 2.4. *Soit* $f \in G$ *Une expression de* f *:*

$$f = \sum_{i,j} \alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j},\ \alpha_{i,j} \in V,\ a_{i,j}, b_{i,j} \in \mathbb{M},\ g_i \in G\ , u_{i,j} \in Rig\langle X\rangle$$

satisfaisant $LM(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}) \preceq LM(f)$ *est appelée expression standard de* f *dans* G.

Théorème II.1. *Soit* $G \subseteq \mathbb{V}Rig\langle X\rangle$ *tel que tout a-polynôme défini dans* G *soit réduit à zéro modulo* G. *Les assertions suivantes sont équivalentes.*

1. G *est une base de Gröbner-Shirshov* $\langle G\rangle$.
2. *Tout élément* f *de* $\langle G\rangle$ *admet une expression standard.*

Démonstration.

1) $\Rightarrow$ 2) :

Supposons que G *est une base Gröbner-Shirshov. Alors il existe* $g_1 \in G$ *tel que* $LT(f) = \alpha_1 a_1 LT(g_1) b_1 \circ u_1$ *avec* $a_1, b_1 \in \mathbb{M},\ u_1 \in Rig\langle X\rangle,\ \alpha_1 \in \mathbb{V}$. *On réduit* f *par* g_1. *On obtient* $f_1 = f - \alpha_1 a_1 g_1 b_1 \circ u_1$.

$f_1 \in \langle G\rangle$ *et* $LM(f_1) \prec LM(f)$. *Si* $f_1 \neq 0$ *alors on répète le procédé en remplaçant* f *par* f_1. *En réduisant* f_1, *on obtient* $f_2 = f_1 - \alpha_2 a_2 g_2 b_2 \circ u_2$.

On a $f = f_1 + \alpha a_1 g_1 b_1 \circ u_1 = \alpha a_1 g_1 b_1 \circ u_1 + \alpha_2 a_2 g_2 b_2 \circ u_2 + f_2$.

De même $LM(f_2) \prec LM(f_1) = LM(\alpha_2 a_2 g_2 b_2 \circ u_2) \prec LM(f) = LM(\alpha agb \circ u)$.

Comme f *se réduit à zéro, à la dernière étape, on a :*

$f = \alpha_1 a_1 g_1 b_1 \circ u_1 + \alpha_2 a_2 g_2 b_2 \circ u_2 + ... + \alpha_n a_n g_n b_n \circ u_n$. *On obtient une expression de* f *comme voulue.*

2) $\Rightarrow$ 1) :

Supposons que 2) *est satisfaite. En vertu du Lemme II.2, on choisit l'expression* $f = \sum_{i,j} \alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}$ *telle que* $\alpha_{i,j} LC(g_i) \neq 0$ *pour tout* $(i,j) \in \Gamma$ *défini précédemment.*

Donc $LM(f) = \gamma = \max\{LM(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j}),\ (i,j) \in \Gamma\}$

Alors $\mathrm{LT(f)} = \sum_{(\mathrm{i,j})\in\Gamma} \alpha_{\mathrm{i,j}}\mathrm{LC}(\mathrm{g_i})\mathrm{a_{i,j}}\mathrm{LM}(\mathrm{g_i})\mathrm{b_{i,j}} \circ \mathrm{u_{i,j}}$ (1).
Puisque $\mathbb{V}$ *est un anneau de valuation, il existe* $(\mathrm{i_0,j_0}) \in \Gamma$ *tel que* $\alpha_{\mathrm{i_0,j_0}}\mathrm{LC}(\mathrm{g_{i_0}})$ *divise* $\alpha_{\mathrm{i,j}}\mathrm{LC}(\mathrm{g_i})$ *pour tout* $(\mathrm{i,j}) \in \Gamma$.
Donc l'équation (1) *devient :* $\mathrm{LT(f)} = \alpha\mathrm{a_{i_0}}\mathrm{LT}(\mathrm{g_{i_0}})\mathrm{b_{i_0}} \circ \mathrm{u_{i_0}} \in \langle \mathrm{LT(G)} \rangle$. □

Les lemmes suivants sont très importants pour la preuve du théorème fondamental.

Lemme II.3. *Soit* $\mathrm{f_1},\ \mathrm{f_2}, ..., \mathrm{f_n} \in \mathbb{V}\mathrm{Rig}\langle \mathrm{X} \rangle$ *tel que* $\mathrm{LM(f_i)} = \mathrm{LM(f_j)} = \gamma\ \forall \mathrm{i,j}$.
S'il existe $\alpha_1,\ \alpha_2, ..., \alpha_\mathrm{n} \in \mathbb{V}$ *tel que* $\mathrm{LM}(\sum_{\mathrm{i=1}}^{\mathrm{n}} \alpha_\mathrm{i}\mathrm{f_i}) \prec \gamma$ *alors* $\sum_{\mathrm{i=1}}^{\mathrm{n}} \alpha_\mathrm{i}\mathrm{f_i}$ *est une combinaison linéaire de compositions simples de* $\mathrm{f_i}$ *à laquelle s'ajoute un élément de* $\mathrm{A\text{-}pol(f_{i_0})}$ *avec* $\mathrm{i_0} \in \{1, 2, ..., \mathrm{n}\}$.

Démonstration. *Cette preuve est similaire à celle donnée dans [62, p. 121]. Pour plus de comodité, nous la reprenons dans ce qui suit en l'adaptant aux semi-anneaux.*
Puisque $\mathbb{V}$ *est un anneau de valuation, on peut supposer que* $\mathrm{LC(f_n)|LC(f_{n-1})|\ldots|LC(f_1)}$.
Comme $\mathrm{LM(f_i)} = \mathrm{LM(f_j)}$ *pour tout* $\mathrm{i} < \mathrm{j}$ *alors* $\widetilde{\mathcal{O}}(\mathrm{f_i}, f_j) = \mathrm{f_i} - \frac{\mathrm{LC(f_i)}}{\mathrm{LC(f_j)}}\mathrm{f_j}$.

$$\begin{aligned}\sum_{i=1}^{n} \alpha_i\mathrm{f_i} &= \alpha_1(\mathrm{f_1} - \frac{\mathrm{LC(f_1)}}{\mathrm{LC(f_2)}}\mathrm{f_2}) + (\alpha_2 + \frac{\mathrm{LC(f_1)}}{\mathrm{LC(f_2)}}\alpha_1)(\mathrm{f_2} - \frac{\mathrm{LC(f_2)}}{\mathrm{LC(f_3)}}\mathrm{f_3}) \\ &+ \ldots + (\alpha_{\mathrm{n-1}} + \frac{\mathrm{LC(f_{n-2})}}{\mathrm{LC(f_{n-1})}}\alpha_{\mathrm{n-2}} + \ldots + \frac{\mathrm{LC(f_1)}}{\mathrm{LC(f_{n-1})}}\alpha_1)(\mathrm{f_{n-1}} - \frac{\mathrm{LC(f_{n-1})}}{\mathrm{LC(f_n)}}\mathrm{f_n}) \\ &+ (\alpha_\mathrm{n} + \frac{\mathrm{LC(f_{n-1})}}{\mathrm{LC(f_n)}}\alpha_{\mathrm{n-1}} + \ldots + \frac{\mathrm{LC(f_1)}}{\mathrm{LC(f_n)}}\alpha_1)\mathrm{f_n}\end{aligned}$$

Soit $\beta_\mathrm{i} = \sum_{j=1}^{i} \frac{\mathrm{LC(f_j)}}{\mathrm{LC(f_i)}}\alpha_\mathrm{j},\ \mathrm{i} = 1, 2, \ldots, \mathrm{n}$
Puisque $\mathrm{LM}(\sum_{i=1}^{n} \alpha_i\mathrm{f_i} =) \prec \gamma$ *on obtient* $\beta_n\mathrm{LC(f_n)} = 0$. *Ainsi* $\beta_\mathrm{n}\mathrm{f_n} \in \mathrm{A\text{-}pol(f_n)}$

$$\sum_{i=1}^{n} \alpha_i\mathrm{f_i} = \sum_{1=1}^{n-1} \beta_i\widetilde{\mathcal{O}}(\mathrm{f_i}, f_{i+1}) + \beta_n\mathrm{f_n}.$$ □

Lemme II.4.
Soit $\mathrm{f,g} \in \mathbb{V}\mathrm{Rig}\langle \mathrm{X} \rangle,\ \mathrm{a,b,c,d} \in \mathbb{M},\ \mathrm{u,v} \in \mathrm{Rig}\langle \mathrm{X} \rangle$ *tel que* $\mathrm{aLM(f)b} \circ \mathrm{u} = \mathrm{cLM(g)d} \circ \mathrm{v}$ *et* $\mathrm{LC(g)}$ *divise* $\mathrm{LC(f)}$. *Alors il existe* $\mathrm{t} \in \mathrm{Rig}\langle \mathrm{X} \rangle$ *telle que la composition simple :* $\widetilde{\mathcal{O}}(\mathrm{afb} \circ \mathrm{u}, \mathrm{cgd} \circ \mathrm{v}) = \mathcal{O}(\mathrm{f,g,a,b,c,d,u_1,v_1}) \circ \mathrm{t}$ *avec* $\mathrm{u_1,v_1} \in \mathrm{Rig}\langle \mathrm{X} \rangle$.

Démonstration. *Supposons que* $\mathrm{aLM(f)b} \circ \mathrm{u} = \mathrm{cLM(g)d} \circ \mathrm{v}$ *et* $\mathrm{LC(g)}$ *divise* $\mathrm{LC(f)}$.
Soit $\mathrm{t} = \mathrm{gcd}_\circ(\mathrm{u}, \mathrm{v})$. *Donc* $\mathrm{u} = \mathrm{u}_1 \circ \mathrm{t}$, $\mathrm{v} = \mathrm{v}_1 \circ \mathrm{t}$ *où* $\mathrm{u}_1, \mathrm{v}_1 \in \mathrm{Rig}\langle \mathrm{X} \rangle$.
Alors :

$$\begin{aligned}\widetilde{\mathcal{O}}(\mathrm{afb} \circ \mathrm{u}, \mathrm{cgd} \circ \mathrm{v}) &= \mathrm{afb} \circ \mathrm{u} - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}}\mathrm{cgd} \circ \mathrm{v} \\ &= \mathrm{afb} \circ \mathrm{u}_1 \circ \mathrm{t} - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}}\mathrm{cgd} \circ \mathrm{v}_1 \circ \mathrm{t} \\ &= (\mathrm{afb} \circ \mathrm{u}_1 - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}}\mathrm{cgd} \circ \mathrm{v}_1) \circ \mathrm{t}\end{aligned}$$

Maintenant, on doit prouver que

$$\mathrm{LCM}_\circ(\mathrm{aLM(f)b}, \mathrm{cLM(g)d}) = \mathrm{aLM(f)} \circ \mathrm{u}_1 = \mathrm{cLM(g)} \circ \mathrm{v}_1.$$

Soit $\mathrm{u}', \mathrm{v}' \in \mathrm{Rig}\langle \mathrm{X} \rangle$ *tels que*

$$\mathrm{LCM}_\circ(\mathrm{aLM(f)b}, \mathrm{cLM(g)d}) = \mathrm{aLM(f)b} \circ \mathrm{u}' = \mathrm{cLM(g)d} \circ \mathrm{v}'.$$

On va montrer que $\mathrm{u} = \mathrm{u}'$ *et* $\mathrm{v} = \mathrm{v}'$.
Remarquons que $\mathrm{gcd}_\circ(\mathrm{u}_1, \mathrm{v}_1) = \mathrm{gcd}_\circ(\mathrm{u}', \mathrm{v}') = \theta$.

$$\begin{aligned}\mathrm{aLM(f)b} \circ \mathrm{u}_1 = \mathrm{cLM(g)d} \circ \mathrm{v}_1 &\Rightarrow \mathrm{aLM(f)b} \circ \mathrm{u}_1 \circ \mathrm{u}' = \mathrm{cLM(g)d} \circ \mathrm{v}_1 \circ \mathrm{u}' \\ &\Rightarrow (\mathrm{aLM(f)b} \circ \mathrm{u}') \circ \mathrm{u}_1 = \mathrm{cLM(g)d} \circ \mathrm{v}_1 \circ \mathrm{u}' \\ &\Rightarrow \mathrm{cLM(g)d} \circ \mathrm{v}' \circ \mathrm{u}_1 = \mathrm{cLM(g)d} \circ \mathrm{v}_1 \circ \mathrm{u}' \\ &\Rightarrow \mathrm{v}' \circ \mathrm{u}_1 = \mathrm{u}' \circ \mathrm{v}_1\end{aligned}$$

$\mathrm{gcd}_\circ(\mathrm{u}', \mathrm{v}') = \theta \Rightarrow \exists \mathrm{w}_1, \mathrm{w}_2 \in \mathrm{Rig}\langle \mathrm{X} \rangle$ *tels que* $\mathrm{u}_1 = \mathrm{u}' \circ \mathrm{w}_1$ *et* $\mathrm{v}_1 = \mathrm{v}' \circ \mathrm{w}_2$ (i).
$\mathrm{gcd}_\circ(\mathrm{u}_1, \mathrm{v}_1) = \theta \Rightarrow \exists \mathrm{w}'_1, \mathrm{w}'_2 \in \mathrm{Rig}\langle \mathrm{X} \rangle$ *tels que* $\mathrm{u}' = \mathrm{u}_1 \circ \mathrm{w}'_1$ *et* $\mathrm{v}' = \mathrm{v}_1 \circ \mathrm{w}'_2$ (ii).
(i) *et* (ii) *impliquent* $\begin{cases} \mathrm{u}_1 = \mathrm{u}' \circ \mathrm{w}_1 = \mathrm{u}_1 \circ \mathrm{w}'_1 \circ \mathrm{w}_1 \ (iii) \\ \mathrm{v}_1 = \mathrm{v}' \circ \mathrm{w}_2 = \mathrm{v}_1 \circ \mathrm{w}'_2 \circ \mathrm{w}_2 \ (iv) \end{cases}$
$(3i) \Rightarrow \mathrm{w}'_1 \circ \mathrm{w}_1 = \theta$. *La Proposition 2.1,* $\mathrm{w}'_1 = \mathrm{w}_1 = \theta$
$(4i) \Rightarrow \mathrm{w}'_2 \circ \mathrm{w}_2 = \theta$. *Ainsi* $\mathrm{w}'_2 = \mathrm{w}_2 = \theta$. *Il s'en suit que* $\mathrm{u}_1 = \mathrm{u}'_1$ *et* $\mathrm{v}_1 = \mathrm{v}'_1$.
On conclut que $\mathrm{LCM}_\circ(\mathrm{aLM(f)b}, c\mathrm{LM(g)d}) = \mathrm{aLM(f)b} \circ \mathrm{u}_1 = \mathrm{cLM(g)d} \circ \mathrm{v}_1$
$\widetilde{\mathcal{O}}(\mathrm{afb} \circ \mathrm{u}, \mathrm{cgd} \circ \mathrm{v}) = (\mathrm{afb} \circ \mathrm{u}_1 - \frac{\mathrm{LC(f)}}{\mathrm{LC(g)}}\mathrm{cgd} \circ \mathrm{v}_1) \circ \mathrm{t}$
$= \mathcal{O}(\mathrm{f}, \mathrm{g}, \mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{u}_1, \mathrm{v}_1) \circ \mathrm{t}.$ □

Le théorème suivant communément appelé Critère de Buchberger ou Lemme de Composition est fondamental dans la théorie des bases de Gröbner. Il donne une caractérisation complète des bases de Gröbner-Shirshov. On l'utilise pour :

— vérifier si un ensemble de polynômes donné est une base de Gröbner-Shirshov relativement à un ordre monomial ;

— compléter un ensemble en une base de Gröbner-Shirshov.

Théorème II.2. *Soit* $G \subseteq \mathbb{V}\mathrm{Rig}\langle X\rangle$. *Les assertions suivantes sont équivalentes.*

1. G *est une base de Gröbner-Shirshov de* $\langle G\rangle$.
2. *Tout élément de* $\mathcal{O}(G)\bigcup A\text{-pol}(G)$ *est réduit à zéro modulo* G.

Démonstration.

1) $\Rightarrow$ 2) : *On sait que toutes les compositions et tous les* a-polynôes *sont dans* $\langle G\rangle$. *Alors ils sont tous réduits à zéro modulo* G.

2 $\Rightarrow$ 1) : *On va montrer que* f *admet une expression standard dans* G.

Soit $f = \sum_{i,j} \alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j},\ \alpha_{i,j} \in V,\ a_{i,j}, b_{i,j} \in \mathbb{M},\ g_i \in G\ , u_{i,j} \in \mathrm{Rig}\langle X\rangle$

Parmi toutes les expressions de f *sous cette forme, il en existe au moins une qui minimise* $\gamma = \max\{LM(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j})\}$ *et* $\alpha_{i,j} LC(g_i) \neq 0$.

Soit $f = \sum_{i,j} \alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j},\ \alpha_{i,j} \in V,\ a_{i,j}, b_{i,j} \in \mathbb{M},\ g_i \in G\ , u_{i,j} \in \mathrm{Rig}\langle X\rangle$ *tel que* $\max\{LM(\alpha_{i,j} a_{i,j} g_i b_{i,j} \circ u_{i,j})\} = \gamma,\ \alpha_{i,j} LC(g_i) \neq 0$.

Soit $h_{i,j} = a_{i,j} g_i b_{i,j} \circ u_{i,j}\ \forall (i,j),\ \Gamma = \{(i,j) :\ LM(\alpha_{i,j} h_{i,j}) = \gamma\}$

Si $\gamma \succ LM(f)$ *alors* $LM(\sum_{(i,j)\in\Gamma} \alpha_{i,j} h_{i,j}) \prec \gamma$. *Alors en vertu du Lemme II.3, on peut écrire :*

$$\sum_{(i,j)\in\Gamma} \alpha_{i,j} h_{i,j} = \sum_{(k,l),(m,n)\in\Gamma} \beta_{k,l,m,n} \widetilde{\mathcal{O}}(h_{k,l}, h_{m,n}) + h \text{ avec } h \in A\text{-pol}(h_{i_0,j_0}),\ (i_0,j_0) \in \Gamma.$$

Pour tout $(k,l),\ (m,n) \in \Gamma$, *on a :*

$$\gamma_{k,l,m,n} = LM(\widetilde{\mathcal{O}}(h_{k,l}, h_{m,n})) \prec \gamma.$$

D'après le Lemme II.4, on a : pour tout $(k,l),\ (m,n) \in \Gamma$ *il existe* $u'_{k,l},\ v'_{k,l},\ t_{k,l,m,n}$ *tels que*

$$\begin{aligned}\widetilde{\mathcal{O}}(h_{k,l}, h_{m,n}) &= \widetilde{\mathcal{O}}(a_{k,l}g_k b_{k,l} \circ u_{k,l}, a_{m,n}g_m b_{m,n} \circ u_{m,n}) \\ &= \mathcal{O}(g_k, g_m, a_{k,l}, b_{k,l}, a_{m,n}, b_{m,n}, u'_{k,l}, v'_{m,n}) \circ t_{k,l,m,n}\end{aligned}$$

Puisque $\mathcal{O}(g_k, g_m, a_{k,l}, b_{k,l}, a_{m,n}, b_{m,n}, , u'_{k,l}, v'_{m,n})$ *et* h *sont réduits à zéro modulo* G, *on a :*

$\mathcal{O}(g_k, g_m, a_{k,l}, b_{k,l}, a_{m,n}, b_{m,n}, u'_{k,l}, v'_{m,n}) = \sum_{s,t} \lambda_{s,t} c_{s,t} g_s d_{s,t} \circ v_{s,t}$ *et* $h = \sum_{p,q} \gamma_{p,q} c'_{p,q} g_p d'_{p,q} \circ v'_{p,q}$

avec $LM(\lambda_{s,t} c_{s,t} g_s d_{s,t} \circ v_{s,t}) \preceq LM(\mathcal{O}(g_k, g_l, a_{k,l}, b_{k,l}, a_{m,n}, b_{m,n}, u'_{k,l}, v'_{m,n}))$.

Donc

$$\begin{aligned}\sum_{(i,j)\in\Gamma} \alpha_{i,j} h_{i,j} &= \sum_{(k,l),(m,n)} \beta_{k,l,m,n} \Big(\sum_{s,t} \lambda_{s,t} c_{s,t} g_s d_{s,t} \circ v_{s,t}\Big) \circ t_{k,l,m,n} + \sum_{p,q} \gamma_{p,q} c'_{p,q} g_p d'_{p,q} \circ v'_{p,q} \\ &= \sum_{(k,l),(m,n)} \sum_{s,t} \lambda_{k,l,m,n} \beta_{s,t} c_{s,t} g_s d_{s,t} \circ v_{s,t} \circ t_{k,l,m,n} + \sum_{p,q} \gamma_{p,q} c'_{p,q} g_p d'_{p,q} \circ v'_{p,q}\end{aligned}$$

Ainsi

$LM(\lambda_{s,t} c_{s,t} g_s d_{s,t} \circ v_{s,t}) \circ t_{k,l,m,n} \preceq LM(\mathcal{O}(g_k, g_l, a_{k,l}, b_{k,l}, a_{m,n}, b_{m,n}, u'_{k,l}, v'_{m,n})) \circ t_{k,l,m,n}$

Or $LM(\mathcal{O}(g_k, g_l, a_{k,l}, b_{k,l}, a_{m,n}, b_{m,n}, u'_{k,l}, v'_{m,n})) \circ t_{k,l,m,n} = \gamma_{k,l,m,n} \prec \gamma$.

Aussi : $LM(\gamma_{p,q} c'_{p,q} g_p d'_{p,q} \circ v'_{p,q}) \prec LM(h_{i_0,j_0}) = \gamma$. *Alors*

$$\begin{aligned}\sum_{(i,j)\in\Gamma} \alpha_{i,j} h_{i,j} &= \sum_{(k,l),(m,n)} \sum_{s,t} \lambda_{k,l,m,n} \beta_{s,t} c_{s,t} g_s d_{s,t} \circ v_{s,t} \circ t_{k,l,m,n} + \sum_{p,q} \gamma_{p,q} c'_{p,q} g_p d'_{p,q} \circ v'_{p,q} \\ &= \sum_{(x,y)} \alpha'_{x,y} a'_{x,y} g_{x,y} b'_{x,y} \circ w_{x,y}\end{aligned}$$

Cette expression satisfait $LM(\alpha'_{x,y} a'_{x,y} g_{x,y} b'_{x,y} \circ w_{x,y}) \prec \gamma = LM(\alpha_{i,j} h_{i,j}),\ (i,j) \in \Gamma$.
Ceci contredit la minimalité de γ. *On conclut que* $\gamma = \max\{LM(\alpha_{i,j} h_{i,j})\} \preceq LM(f)$.□

Le théorème précédent conduit à la version suivante de l'algorithme de Buchberger. Dans les deux exemples suivants, on exécute l'algorithme en discutant des compositions et des réductions. Dans le premier exemple, on obtient une base de Gröbner-Shirshov finie et dans le second, on montre que l'algorithme ne se termine pas. Dans les deux cas, on considère l'ordre de la longueur lexicographique.

Exemple II - 2.4. *Soit* $G = \{g_1 = 2xy \circ x \circ z \circ 1 + 3x \circ z \circ 1\} \subseteq \frac{\mathbb{Z}}{4\mathbb{Z}} Rig\langle X\rangle$.
Alors $a\text{-pol}^1(g_1) = 2g_1 = 2x \circ z \circ 1 = g_2$
$Red(g_2, G) = g_2 \Rightarrow G \longleftarrow G \cup \{g_2\} = \{g_1, g_2\}$

Algorithme 9 : Algorithme de Buchberger

Entrée : $(G, \prec)$

Sortie : *base de Gröbner-Shirshov* si l'algorithme termine

$\mathcal{O}' \leftarrow \varnothing$;
Calculer et réduire A-pol(G);
$G \leftarrow G \cup (\text{Red}(\text{A-pol}(G)\backslash\{0\})$;
Tant que $\mathcal{O}\backslash\mathcal{O}' \neq \varnothing$ **Faire**
    choisir un élément $\mathcal{O}(f, g, a, b, c, d) \in \mathcal{O}\backslash\mathcal{O}'$;
    $G \leftarrow G \cup (\text{Red}(\{f,\ \text{A-pol}(f)\}, G)\backslash\{0\})$;
    $\mathcal{O}' \leftarrow \mathcal{O}' \cup \mathcal{O}(f, g, a, b, c, d)$
return G

$\text{LCM}_\circ(\text{LM}(g_1), \text{LM}(g_2)) = xy \circ x \circ z \circ 1 = \text{LM}(g_1) = \text{LM}(g_2) \circ xy$. *La composition correspondante est :*
$\mathcal{O}(g_1, g_2, 1, 1, 1, 1, 1, xy) = g_1 - g_2 \circ xy = 3x \circ z \circ 1$
$\text{Red}(g_3, G) = g_3 \Rightarrow G \longleftarrow G \cup \{g_3\} = \{g_1, g_2, g_3\}$
Pour $(a, b, c, d) \neq (1, 1, 1, 1)$, $u, v \in \text{Rig}\langle X\rangle$ *tels que*
$\text{LCM}_\circ(a\text{LM}(g_1)b, c\text{LM}(g_2)d) = a\text{LM}(g_1)b \circ u = c\text{LM}(g_2) \circ v$, *la composition correspondante est :* $\mathcal{O}(g_1, g_2, b, c, d, u, v) = ag_1b \circ u - cg_2d \circ v = 3a(x \circ z \circ 1)b \circ v \xrightarrow{g_3} 0$
Pour (a, b, c, d), $u, v \in \text{Rig}\langle X\rangle$ *tels que*
$\text{LCM}_\circ(a\text{LM}(g_1)b, c\text{LM}(g_3)d) = a\text{LM}(g_1)b \circ u = c\text{LM}(g_3) \circ v$, *la composition correspondante est :* $\mathcal{O}(g_1, g_3, b, c, d, u, v) = ag_1b \circ u - 2cg_3d \circ v = 3a(x \circ z \circ 1)b \circ v \xrightarrow{g_3} 0$
Pour (a, b, c, d), $u, v \in \text{Rig}\langle X\rangle$ *tels que*
$\text{LCM}_\circ(a\text{LM}(g_1)b, c\text{LM}(g_1)d) = a\text{LM}(g_1)b \circ u = c\text{LM}(g_1) \circ v$, *la composition correspondante est :*
$\mathcal{O}(g_1, g_1, b, c, d, u, v) = ag_1b \circ u - cg_1d \circ v = 3a(x \circ z \circ 1)b \circ u - 3c(x \circ z \circ 1)d \circ v \xrightarrow{g_3} 0$
$\mathcal{O}(g_2, g_3) = \mathcal{O}(g_2, g_2) = \mathcal{O}(g_3, g_3) = \{0\}$
$\{g_1, g_2, g_3\}$ *est ue base de Gröbner-Shirshov de* $\langle g_1\rangle$.

Exemple II - 2.5. *Soit* $G = \{g_1 = 2xy \circ x \circ z \circ y + 3x \circ z \circ 1\} \subseteq \frac{\mathbb{Z}}{4\mathbb{Z}}\text{Rig}\langle X\rangle$.
Alors $\text{a-pol}^1(g_1) = 2g_1 = 2x \circ z \circ 1 = g_2$
$\text{Red}(g_2, G) = g_2 \Rightarrow G \longleftarrow G \cup \{g_2\} = \{g_1, g_2\}$
Pour $(a, b) = (1, 1)$ *et* $u \in \mathbb{M}$, *on peut déterminer* $c, d \in \mathbb{M}$, $v \in \text{Rig}\langle X\rangle$ *tels que* $\text{LCM}_\circ(\text{LM}(g_1$

La composition correspondante est $\mathcal{O}(g_1, g_2, 1, 1, c, d, u, v) = g_1 \circ u - cg_2d \circ v = 3x \circ z \circ 1 \circ u$
Supposons que g_u *est réductible modulo une composition*
$\mathcal{O}(g_1, g_2, a', b', c', d', u', v') = a'g_1b' \circ u' - c'g_2d' \circ v' = 3a'(x \circ z \circ 1)b' \circ u'$.
Alors $g_u = x \circ z \circ 1 \circ u = a_1(a'(x \circ z \circ 1)b' \circ u')b_1$ *où* $a_1, b_1 \in \mathbb{M}$.

$$x \circ z \circ 1 \circ u = a_1(a'(x \circ z \circ 1)b' \circ u')b_1 \Rightarrow a_1 = b_1 = 1$$
$$\Rightarrow x \circ z \circ 1 \circ u = a'(x \circ z \circ 1)b' \circ u'$$
$$\Rightarrow \mathcal{O}(g_1, g_2, a', b', c', d', u', v') = g_u$$

En d'autres termes, g_u *est uniquement réductible par lui-même. Donc, pour tout* $u \in \mathbb{M}$, *on doit déterminer* g_u *et l'ajouter à* $\mathbb{G}$. *Puisque* $\mathbb{M}$ *est infini, l' algorithme ne se termine pas.*

Discussion sur l'algorithme

Deux faits ont motivé le démarrage de l'exécution de l'algorithme par le calcul des a-polynômes :

1. l'ensemble des a-polynômes est fini ;
2. durant la réduction d'une composition, il peut être très avantageux d'avoir les monômes des réducteurs aussi petits que possibles.

Malheureusement, dans notre cas (l'ensemble des monômes est un semi-anneau), l'algorithme de Buchbegrer s'exécute difficilement. Ceci est dû au fait que pour tout $(a, b, c, d) \in \mathbb{M}$, on doit toujours calculer la composition correspondante. Puisque, $\mathbb{M}$ est infini, $\mathcal{O}(f, g)$ est difficile à calculer en pratique. Ainsi, pour la plupart du temps, on se restreint à utiliser le critère de Buchberger pour vérifier si un ensemble donné est une base de Gröbner-Shirshov ou non. Donc, la théorie des bases de Gröbner ne nous permettra pas toujours de résoudre le problème d'appartenance d'un polynôme à un idéal.

Conclusion et perspectives

Dans cette thèse, nous avons présenté deux résultats fondamentaux : le premier porte sur la caractérisation d'idéaux admettant des bases de Gröbner non commutatives finies et le second, sur la généralisation des bases de Gröner-Shirshov sur les anneaux de valuation.
Chacun de ces résultats a son importance. En guise d'exemple, sachant que la manipulation des anneaux de polynômes commutatifs est généralement plus simple, tout travail sur un idéal non commutatif $\mathcal{J}$ admettant une base de Gröbner finie ayant les propriétés P_1 et P_2 peut se ramener à celui de l'idéal commutitif $\mathcal{I}$ tel que $\mathcal{J} = \gamma^{-1}(\mathcal{I})$.
De même, nous avons vu que les bases de Gröbner-Shirshov peuvent être adaptées à certains types d'anneaux tels que les anneaux de valuation.

Cette recherche sur les bases de Gröbner est motivée par les applications de plus en plus nombreuses qu'offre cette théorie. Ces applications font de la théorie des bases de Gröbner l'une des inventions mathématiques les plus importantes du XX^e siècle.
A terme, nous avons plusieurs objectifs parmi lesquels on peut citer les trois ci-dessous.

1. Faire une étude sur l'adaptation du résultat sur les bases de Gröbner non commutatives finies aux anneax : notre résultat et celui de Eisenbud *et al.* ne concernent que les anneaux de polynômes à coefficient dans un corps de caractéristique nulle. Nous comptons faire une investigation afin de généraliser ces résultats aux corps de caractéristique non nulle et aux anneaux de façon générale.

2. Mener des recherches pour la réduction du temps de calcul : l'importance manifeste des bases de Gröbner contraste avec la difficulté de leur utilisation. Dans la théorie, l'existence d'une base de Gröbner d'un idéal donné est établie par Buchberger dans [13]. Mais sa détermination est difficile. En effet, l'algorithme de Buchberger qui est le principal outil de calcul des bases de Gröbner est très coûteux (en temps et en espace). Alors, des recherches allant dans le sens de l'optimisation de cet algorithme et/ou la mise sur pied d'autres algorithmes ont été entreprises. Très peu nombreux, les algorithmes obtenus de ces recherches peuvent être classés en deux catégories :
   — les algorithmes de changement d'ordre tels que FGLM [31] qui permettent de transformer une base de Gröbner relativemnt à un ordre en une base de Gröbner relativement à un autre ordre ;
   — les algorithmes de calcul directs tels que F_4 [29], F_5 [30], F_5C,... qui peuvent être considèrés comme des versions optimisées de l'algorithme de Buchberger.

   Comparés à l'algorithme de Buchberger, ces nouveaux algorithmes diminuent considérablement le temps de calcul mais pas assez convenablement pour les usages voulus des bases de Gröbner. Ainsi, nous comptons faire des recherches afin d'optimiser certains des algorithmes dèjà existants et/ou de mettre sur pied de nouveaux algorithmes plus rapides permettant d'accélérer les calculs.
3. Mener des recherches pour la détermination de Polly Cracker sûrs et rapides : L'hypothèse selon laquelle l'avènement de la machine quantique entrainera la disparition des cryptosystèmes actuels a orienté les recherches pour la mise sur pied de cryptosystèmes post-quantiques. Les cryptosystèmes basés sur les bases de Gröbner, communément appelés Polly Cracker, sont de la catégorie des cryptosystèmes post-quantiques. Mais jusqu'ici, tous les Polly Cracker conçus ont des vulnérabilités qui rendent impossible leur utlisation. Ainsi, la question "Why You Cannot Even Hope to use Gröbner bases in Public Key Cryptography ?" posée par B. Barkee, D. C. Can, J. Ecks, T. Moriarty, et R. F. Ree dans [4] reste d'actualité. Et comme le disait C. Traverso dans son exposé intitulé "Gröbner Bases In Public Key Cryptography : Hope Never Dies"

(travail en collaboration avec M. Caboara, F. Caruso) lors de l'Eurocrypt 2008 à Istanbul : "c'est notre tour d'essayer au risque d'échouer". Alors, nous comptons nous investir sur la recherche de Polly Crackers sûrs et rapides pour des usages pratiques et efficients.

4. Faire des investigations sur la théorie des représentations et la combinatoire en lien avec les bases de Gröbner.

Bibliographie

[1] Aoki S., Takemura A., Yoshida R. *Indispensable monomials of toric ideals and Markov bases, Germany J. Symbolic Computation* 43(2008) , 490 – 507

[2] Autord M. *Aspects algorithmiques du retournement de mots, Thèse de doctorat soutenue le 7 mai 2009, Université de Caen*

[3] Bardet M., Faugère J., Salvy B. *On the complexity of the F5 Gröbner basis algorithm, J. Symbolic Computation* 70 (2015) 49 – 70

[4] Barkee B., Can D. C., Ecks J., Moriarty T., and Ree R. F. *Why You Cannot Even Hope to Use Gröbner Bases in Public-Key Cryptography ? An Open Letter to a Scientist Who Failed and a Challenge to Those Who Have Not Yet Failed, J. Symbolic computations* 18(6)497 – 501, 1994

[5] Bergman G. M. *The diamond lemma for ring theory, Adv. Math.* 29 (1978), 178 – 218.

[6] Bokut L. A. *Imbedding into simple associative algebras, Algebra Logic* 15(1976) 117 – 142.

[7] Bokut L. A., Chen Y. *Gröbner-Shirshov bases and their calculations, Bull. Math. Sci.* (2014) 4 : 325 – 395

[8] Bokut L. A., Chen Y. *Gröbner-Shirshov bases for Lie algebras : after A. I. Shirshov, Southeast Asian Bulletin of Mathematics* (2007) 31 : 1057 – 1076

[9] Bokut L. A., Chen Y., and MO Q. *Gröbner-Shirshov bases for semirings, Journal of Algebra 385* (2013) 47 – 63

[10] Bouesso A. S. E. M. *Gröbner bases over a dual valuation ring, International Journal of Algebra, Vol.* 7, 2013, *no.* 11, 539 – 548

[11] Bouesso A. S. E. M. *Généralisation des bases de Gröbner commutatives et non commutatives sur certains types d'anneaux, Thèse de doctorat soutenue soutenue le* 28 *février* 2014 *à l'Université Cheikh Anta Diop de Dakar*

[12] Bouesso A. S. E. M., Sow D. *Non-Commutative Gröbner Bases over rings, Communications in Algebra.* 2010

[13] Bucherger B. *Bruno Buchber's PhD thesis* 1965 *: An algorithm for finding the basis elements of the residue class of a zero dimensional ideal, Journal of Symbolic Computation* 41(2006) 475 – 511

[14] Buchmann J., Pyshkin A., Weinmann R. *A Zero-Dimensional Groebner basis for AES-128, Technische Universitat Darmstadt, Fachbereich Informatik, Hochschulstr. 10, D-64289 Darmstadt, Germany J. Symbolic Computation* (1988) 7, 55 – 69

[15] Buchmann J, Pyshkin A., Weinmann R. *Block ciphers sensitive to Groebner Basis Attacks, Technische Universitat Darmstadt, Fachbereich Informatik, Hochschulstr. 10, D-64289 Darmstadt, Germany J. Symbolic Computation* (1988) 7, 55 – 69

[16] Bulygin S., Pellikaan R. *Bounded distance decoding of linear error-correcting codes with Gröbner bases, Journal of Symbolic Computation* 44(2009), 1626 – 1643

[17] Caboara M., Caruzo F., Traverso C. *Gröbner Bases for Public Key Cryptography*

[18] Ceria M., Mora T. *Buchberger-Weispfenning Theory for Effective Associative Rings, J. Symb. Comp., special issue for ISSAC* 2015, 83, *pp.* 112 – 146.

[19] Ceria M., Mora T. *Buchberger-Zacharias Theory of Multivariate Ore Extensions, Journal of Pure and Applied Algebra Volume* 221, *Issue* 12, *December* 2017, *Pages* 2974 – 3026

[20] Cox D., Little J., O'Shea D. *Ideals, Varieties and Algorithms An Introduction to Computational Algebraic Geometry and Commuative Algebra. Second edition* 1997 *Springer*

[21] De Alba Casillas H. *Nombre de Betti d'idéaux monomiaux, Thèse de doctorat soutenue le* 10 *octobre* 2012

[22] Diarra N. *Fonctions de hachage sur les courbes (Hyper)Elliptiques et Bases de Gröbner sur les D-A-anneaux, Thèse de doctorat soutenue le* 12 *aout* 2017 *à l'Université Cheikh Anta Diop de Dakar*

[23] Diop Y., Mesmoudi L., Sow D. *Semi-ring based Gröbner-Shirshov over a noetherian valuation ring. Associative and Non-associative Algebras and Applications. Springer Proceedings in Mathematics & Statistics, vol* 311(2020), *pp* 183 – 198. *Springer, Cham*

[24] Diop Y., Sow D. *On finite noncommutative Gröbner bases. Algebra Colloquium* 27 : 3(2020) 381 – 388 (to appear in september 2020)

[25] Eder C., Faugère J., *A survey on signature-based algorithms for computing Gröbner basis computations. Journal of Symbolic Computation, Elsevier,* 2016, *pp*.1 – 75. 10.1016/*j.jsc*.2016.07.031. *hal* – 00974810*v*2

[26] Eisenbud D. *Commutative algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics. 150. Berlin : Springer-Verlag*

[27] Eisenbud D., Peeva I., and Sturmfels B. *Noncommutative Gröbner bases for commutative algebras, Proceedings of the American Mathematical Society, Volume* 126, *Number* 3, *March* 1998, *Pages* 687−691 *S*0002−9939(98)04229−4

[28] El-Sherbiny A., Elhosseini M. A., Haikal A. Y. *A comparative study of soft computing methods to solve inverse kinematics problem, Germany J. Symbolic Computation* 43(2008) , 6455 – 658

[29] Faugère J. *A new efficient algorithm for computing Gröbner bases, Journal of Pure and Applied Algebra* 139 (1999) 61 – 88

[30] Faugère J. *A new efficient algorithm for computing Gröbner bases without reduction to zero, In Proceedings of the* 2002 *International Symposium on Symbolic and Algebraic Computation* (*ISSAC*), *pages* 75 – 83, *Lille, France, July* 2002

[31] Faugère J., Gianni P., Lazard D., Mora T. *Efficient computation of zero-dimensionl Gröbner bases by changing of ordering, Journal of Symbolic Computation* (1993)16, $329-344$

[32] Francisco C. A., Mermin J., and Schweig J. *Borel Generators, Journal of Algebra* $332(2011)522-542$

[33] Greuel G., Seelisch F., Wienand O. *The Gröbner basis of the ideal of vanishing polynomials, Journal of Symbolic Computation* 46 (2011) $561-570$

[34] Herzog J., Hibi T. *Monomial Ideals. Graduate Text in Mathematics* 260. *Springer*

[35] Herzog J., Popescu D. *On the regularity of p-Borel ideals, Proceedings of the American Mathematical Society. Volume* 129, *Number* 9, *Pages* $2563-2570$ *S* $0002-9939$ (01) $05840-3$ (2001)

[36] Hironaka H. *Resolution of singularities of an algebraic variety over a field of characteristic zero : I. The Annals of Mathematics Second Series,* 79(1) : $109-203, 1964$.

[37] Hosten S., Smith G. G. *Monomial Ideals, Computations in Algebraic Geometry with Macaulay* 2. *Algorithms and Computations in Mathematics, volume* 8 (*Springer New York,* 2001). *pp* $73-100$

[38] Kandri-Rody A., Kapur D. *Computing a Gröbner basis of a polynomial ideal over a Euclidean domain, Journal of Symbolic Computation* (1988) 7, $37-57$

[39] Kandri-Rody A., Weispfenning W. *Non-commutative Gröbner Bases in Algebras of Solvable Type, Journal of Symbolic Computation* 9 (1990), $1-26$

[40] Kapur D., Yongyang C. *An Algorithm for Computing a Gröbner Basis of a Polynomial Ideal over a Ring with Zero Divisors. Mathematics in Computer Science. pages 601-634. December* 2009.

[41] La Sacla R., Levandovsky V. *Letterplace ideals and non-commutative Gröbner bases, Journal of Symbolic Computation* $44(2009)$, $1374-1393$

[42] Lee K., O'Sullivan M. E. *List decoding of Reed-Salomon codes from a Gröbner basis perspective, Germany J. Symbolic Computation* 43 (2008) , 6455 – 658

[43] Levandovsky *Noncommutative Computer Algebra for polynomial algebras : Gröbner bases, applications and implementation, PhD thesis defended in june, 8th,* 2005 *at the University of Kaiserslautern*

[44] Mikhalev A. A. *A composition lemma and the word problem for color Lie superalgebras, Moscow Univ. Math. Bull.* 44 (5), (1989) 87 – 90

[45] Möller H. M. *The construction of Gröbner bases using syzygies, Journal of Symbolic Computation* (1988), 6, 345 – 359

[46] Mora T. *An introduction to commutative and non-commutative Gröbner Bases, Journal of Theoretical Computer Science* (1994), 13, 131 – 173

[47] Mora T. *Zacharias Representation of Effective Associative Rings, J. Symb. Comp. (submitted)*

[48] Murray R. B. *free associative algebras, non commutative Gröbner bases, and universal associative envelopes for non associative structures, CMUC : Comment. Math. Univ. Carolin.* 55, 3(2014) 341 – 379

[49] Norton G. H., Sălăgean A. *Strong Gröbner bases for polynomials over a principal ideal ring, Bull. Austral. Math. Soc., Vol.* 64(2001) 505 – 528

[50] Pan L. *On the D-bases of Polynomial Ideals Over Principal Ideal Domain, Bell Communications Research. 33 Knightsbridge Road, PY4 4J-223, Piscataway, NJ 08854, U.S.A., J. Symbolic Computation* (1988) 7, 55 – 69

[51] Pauer F. *Gröbner bases with coefficients in rings, Institut für Mathematik, Universität Innsbruck, Technikerstr. 13, A-6020 Innsbruck, Austria, Journal of Symbolic Computation* 42(2007) 1003 – 1011

[52] Peeva I., Stillman M., *The minimal free resolution of a Borel ideal, Expositioes Mathematicae* 26 (2008)237 – 247

[53] Retenauer C. *Mots de Lyndon et un théorème de Shirshov, Ann. sc. math. Québec,* 1986, *Vol.* 10, *No* 2, *pp.* 237 – 245

[54] Shirshov A. I. *Some algorithmic problems for Lie algebras Mat. Sb. N.* 45(1958) 113 – 12

[55] Shirshov A. I. *On free Lie rings. Sib. Math. Zh. N.* 3(1962) 292 – 296

[56] Simoes B. *PhD thesis : New strategies for computing Gröbner bases, defended in April* 12, 2013, *Athesina Studiorum Universitas*

[57] Spear D.A. *A constructive approach to commutative ring theory*, in *Proc. of the* 1977 *MACSYMA Users' Conference, NASA CP*-2012 (1977), 369 – 376

[58] Stifter S. *Gröbner bases of modules over reduction rings, Research Institute of Symbolic Computation-Linz, Johanes Kepler University, A-4040, Linz Austia, Journal of Algebra* 159, 54 – 63(1993)

[59] Tran Q. *A new class of term orders for elimination, Rice University, Houston, TX, USA, Lamar University, Beaumont, TX, USA, Journal of Symbolic Computation* 42(2007) 533 – 548

[60] Xiangui Z. *Gröbner-Shirshov Bases in Some Noncommutative Algebras A thesis submitted to the Faculty of Graduate Studies of The University of Manitoba,* 2014

[61] Xianqiang X. *Non-Commutative Gröbner Bases and Applications. PhD thesis. Department of Informatics and Mathematics of the University of Passau. May* 2012.

[62] Yengui I. *Constructive Commutative Algebra. Projective Modules Over Polynomial Rings and Dynamical Gröbner Bases. Lecture Notes in Mathematics* 2138, *Springer series* 304, 2015

[63] Yengui I. *Dynamical Gröbner bases, Journal of Algebra* 301 (2006) 447 – 458.

[64] Yengui I. *Dynamical Gröbner bases over Dedekind rings, Journal of Algebra* 324(1) (2010) 12 – 24

[65] Yengui I. *Corrigendum to "Dynamical Gröbner bases"* [*J. Algebra* 301(2) (2006) 447 – 458] *and to "Dynamical Gröbener bases over Dedekind rings" [J. Algebra* 324 (1) (2010)12 – 24], *Journal of Algebra* 339 (2011) 370 – 375.

UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR
ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE
THÈSE DE DOCTORAT UNIQUE

Option: Mathématiqus et Modélisation

Spécialité: Codage, Cryptologie, Algèbre et Applications

Nom et prénom du Candidat: DIOP Yatma

Sujet de thèse: Bases de Gröbner-Shirshov sur les anneaux de valuation et caractérisation de certaines bases de Gröbner non commutatives finies

Soutenue le 02 novembre 2020 devant le jury composé de:

PRÉSIDENT	Pr. Cheikh Thiécoumba GUEYE	Université Cheikh Anta Diop de Dakar
RAPPORTEURS	Pr. Edgar MARINEZ-MORO	Université de Valladolid
	Pr. El Mamoun SOUIDI	Université Mohammed V de Rabat
EXAMINATEURS	Pr. Mamadou BARRY	Université Cheikh Anta Diop de Dakar
	Pr. Mohamed Ben Fraj Ben MAAOUIA	Université Gaston Berger
	Pr. Mamadou SANGHARE	Université Cheikh Anta Diop de Dakar
DIRECTEURS DE THÈSE	Pr. Djiby SOW	Université Cheikh Anta Diop de Dakar
	Dr. Laila MESMOUDI	Université Cheikh Anta Diop de Dakar

Résumé:

Depuis leur introduction en algèbre commutative dans les années 60, les bases de Gröbner ont connu plusieurs généralisations. Leur extension en algèbre non commutative a entrainé la perte partielle de l'existence d'une base de Gröbner finie pour tout idéal donné.
En 1998, Eisenbud, Peeva et Strumfels ont montré que si γ est l'homomorphisme de l'anneau non commutatif $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ vers l'anneau commuatif $\mathbb{K}[x_1, x_2, ..., x_n]$, qui associe x_i à X_i, alors tout idéal $\mathcal{I}$ de $\mathbb{K}[x_1, x_2, ..., x_n]$, l'idéal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ admet une base de Gröbner finie. Dans cette thèse, nous avons montré que tout idéal $\mathcal{J}$ de $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ admettant une base de Gröbner finie et contenant tous les commutateurs est l'image réciproque par γ d'un idéal $\mathcal{I}$ de $\mathbb{K}[x_1, x_2, ..., x_n]$.
En 2013, Bokut et Chen introduisent les bases de Gröbner-Shirshov sur les semi-anneaux. Dans cette approche, l'ensemble des monômes est muni d'une structure de semi-anneau et non de celle habituelle de monïde. Nous avons généralisé cette approche aux anneaux de valuation. Concrètement, nous avons donné la caractérisation des bases de Gröbner en munissant les monômes d'une structure de semi-anneau et les coefficients, d'une structure d'anneau de valuation.

Abstract:

Introduced in commutative algebra during the years $60's$, the Gröbner-bases theory was then generalized in several ways. Its generalization in the noncommutative multivariate polynomial ring implied a major consequence: there exist ideals which do not admit a finite Gröbner basis. Then, the question "how to recognize whether a non commutative ideal admits a finite Gröbner basis ?" became a challenge. In 1998, by considering the homomorphism γ from the noncommutative polynomial ring $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ to the commutaive one $\mathbb{K}[x_1, x_2, ..., x_n]$ which replaces X_i by x_i, Eisenbud, Peeva and Strumfels proved that for any ideal $\mathcal{I}$ of $\mathbb{K}[x_1, x_2, ..., x_n]$, the ideal $\mathcal{J} = \gamma^{-1}(\mathcal{I})$ admits a finte Gröbner basis. In this thesis, we proved that for any ideal $\mathcal{J}$ of $\mathbb{K}\langle X_1, X_2, ..., X_n\rangle$ which contains all commutators and admits a finte Gröbner basis, there exists an ideal $\mathcal{I}$ of $\mathbb{K}[x_1, x_2, ..., x_n]$ such that $\mathcal{J} = \gamma^{-1}(\mathcal{I})$.
In 2013, Bokut and Chen introduced a new approach to the study of Gröbner bases. Namely, they considerd a semiring as the set of monomilas instead of the usual structure of monoid. In this thesis, we extend this approach to the noetherian valuation ring as the set of coefficients and we give the correspondig Buchberger criterion.