INSTITUT JOSEPH FOURIER

UNIVERSITÉ GRENOBLE ALPES

TRAVAIL D'ETUDE ET DE RECHERCHE

# Bases de Gröbner et algèbres de Fomin-Kirillov (duales)

*Auteure*
HABIBATOU
DIALLO

*Enseignant encadrant*
ESTANISLAO
HERSCOVICH

20 mai 2020

# Table des matières

# 1 Introduction

La théorie des bases de Gröbner a été introduite par Heisuke Hironaka et Bruno Buchberger dans les années 1960, et doit son nom au directeur de thèse de ce dernier, Wolfgang Gröbner.

Les bases de Gröbner sont employées par les mathématiciens mais également les informaticiens comme outils pour une multitude d'applications. On doit à Buchberger un algorithme récursif permettant de calculer une base de Gröbner. On a également de nombreux logiciels, tel que GAP, qui permettent les calculer.

Dans ce mémoire, on utilisera essentiellement les bases de Gröbner dans le but de calculer une base des algèbres de Fomin-Kirillov et ses duales de paramètre n=3 ou n=4.. Ces algèbres quadratiques ont une importance fondamentale en géométrie algébrique. Elles ont été introduites par Fomin et Kirillov au milieu du vingtième siècle comme un outil pour étudier le calcul de Schubert et la cohomologie des variétés de drapeaux. (voir [2], [3], [3]).

Ce travail se décompose en deux grandes parties. Dans un premier temps, nous nous intéresserons à la théorie autour des bases de Gröbner d'algèbres non commutatives. On va suivre pour cela l'article [1] (voir aussi [5]. Suite à cela, nous entrerons dans le concret et nous proposerons une applications direct sur les algèbres de Fomin-Kirillov et ses duales.

# 2 Théorie des bases de Gröbner non commutatives

## 2.1 Notations et définitions

Soit $\mathbb{K}$ un corps et $X$ un ensemble quelconque.

On pose

$$X^0 = \{1_w\} \text{ où } 1_w \text{ est appelé le } \textbf{mot vide},$$

$$X^k := \underbrace{X \times ... \times X}_{\text{k facteurs}}.$$

***Notation*** : Si $y = (y_1, ..., y_k) \in X^k$, alors on notera $y = y_1...y_k$, avec la convention que $k = 0$ équivaut à $y = 1_w$.

Considérons

$$W = \bigcup_{k \in \mathbb{N}} X^k.$$

On définit la **loi de concaténation** $\bullet$ sur $W$,

$$\begin{array}{ccc} W \times W & \to & W \\ (y, z) & \mapsto & y \bullet z, \end{array}$$

telle que

- $y_1...y_r \bullet z_1...z_l = y_1...y_r z_1...z_l, \quad \forall\, y_1...y_r, z_1...z_l \in W$ avec $r, l \geq 1$
- $1_w \bullet y = y \bullet 1_w = y, \quad \forall y \in W.$

*Remarque* 2.1. Cette loi est associative et de neutre $1_w$. Ainsi, munit de la concaténation, $W$ n'est autre que le monoïde unitaire engendré par $X$.

Maintenant considérons

$$\boxed{T = Vect_{\mathbb{K}}(W).}$$

Un élément de $T$ est de la forme

$$\sum_{w \in W} c_w w$$

avec $c_w \in k$ et tel que $\{w \in W : c_w \neq 0\}$ est fini. On va supposer que cette condition est toujours vérifiée lorsque l'on écrit un élément de $T$.

$T$ est munit de la loi

$$\star : T \times T \to T$$

donnée par

$$\left(\sum_{w\in W} c_w w\right) \star \left(\sum_{w'\in W} c'_{w'} w'\right) = \sum_{w\in W, w'\in W} c_w c'_{w'} w \bullet w'.$$

*Remarque* 2.2. Si 1 est le neutre multiplicatif dans $\mathbb{K}$, alors $1.1_w$ est le neutre de l'anneau $(T, +, \star)$. $T$ est ce que l'on appelle l'algèbre tensorielle engendrée par $X$.

Par la suite, on appellera $X$ l'ensemble des *lettres*, $W$, celui des *monômes* ou des *mots* et $T$ celui des tenseurs.

Maintenant on souhaiterait munir $W$ d'un ordre adapté.

**Définition 2.1** (Ordre monomial)**.** Soit $<$, un ordre partiel strict sur W, (i.e. irréfléchie, asymétrique et transitive). On dit que $<$ est un **ordre monomial** (non commutatif) s'il satisfait les conditions suivantes :

(i) $1 < m, \quad \forall m \in W$,

(ii) $m_1 < m_2 \Rightarrow lm_1r < lm_2r, \quad \forall l, r, m_1, m_2 \in W$.

**Exemple 2.1** (Ordre lexicographique)**.** On considère $X = \{x_1, ..., x_n\}$ et l'ordre $<$ sur $X$, tel que $x_1 < x_2 < \cdots < x_n$. L'ordre lexicographique $<_{lex}$ sur $W$ est donné par

$$y = y_1 \dots y_r <_{lex} z = z_1 \dots z_l$$

$$\Leftrightarrow \begin{cases} \text{s'il existe } 0 \leqslant s < r \text{ tel que } y_1 = z_1, y_2 = z_2, \dots, y_s = z_s, y_{s+1} < z_{s+1} & \text{ou,} \\ 0 < r < l \text{ et } y_1 = z_1, y_2 = z_2, \dots y_r = z_l & \text{ou,} \\ r = 0 < l, \end{cases}$$

pour tous $y = y_1 \dots y_r$ et $z = z_1 \dots z_l$ dans $W$.

L'ordre lexicographique n'est pas un ordre monomial. En effet, si $y = x_1x_1x_2$ et $z = x_1x_2$ alors par ce qui précède $y <_{lex} z$. Mais maintenant, si $<_{lex}$ est un ordre monomial, alors par la condition (i), $1 <_{lex} x_2$ et par (ii) cela implique que $z = x_1x_2 <_{lex} x_1x_1x_2 = y$, ce qui donne une contradiction.

**Exemple 2.2** (Ordre deglexicographique)**.** Comme çi-dessus on considère $X = \{x_1, ..., x_n\}$ et l'ordre $<$ sur $X$, tel que $x_1 < x_2 < \cdots < x_n$. Si $y = y_1 \dots y_r \in W$, on définit $deg(y) = r$. L'ordre deglexicographique $<_{deglex}$ sur $W$ est donné par

$$y = y_1 \dots y_r <_{deglex} z = z_1 \dots z_l$$

$$\Leftrightarrow \begin{cases} deg(y) = r < l = deg(z) & \text{ou,} \\ deg(y) = r = l = deg(z) \text{ et } y <_{lex} z, \end{cases}$$

pour $y = y_1 \dots y_r$ et $z = z_1 \dots z_l$ dans $W$.

On peut vérifier sans difficultés que deglexicographique est bien un ordre monomial.

## 2.2 Réduction tensorielle

Dans toute cette partie, on reprend les mêmes notations : $\mathbb{K}$ est un corps, $X$ désigne l'ensemble des lettres, $W$ celui des mots, et $T = Vect_{\mathbb{K}}(W)$ est l'ensemble des tenseurs.

Etant données une famille $(w_\sigma)_{\sigma\in\Sigma}$ de mots et une famille $(f_\sigma)_{\sigma\in\Sigma}$ de tenseurs telles que si $\sigma \neq \sigma'$ alors $w_\sigma \neq w_{\sigma'}$, on s'intéresse à l'algèbre $A = T/I$ où $I$ est l'idéal bilatère engendré par les éléments $w_\sigma - f_\sigma$, $\sigma \in \Sigma$. En d'autre termes, $A$ est l'algèbre engendrée par $X$ où l'on ajoute les relations

$$\boxed{w_\sigma = f_\sigma, \forall \sigma \in \Sigma.}$$

**Définition 2.2.** On pose l'ensemble, $D = \{w \in W |\text{ il existe } u, v \in W \text{ et } \sigma \in \Sigma \text{ tels que } w = uw_\sigma v\}$ et

$$\boxed{S^0 = W \setminus D.}$$

On définit ainsi,

$$\boxed{S = Vect(S^0).}$$

On appelle **mots standards**, les éléments dans S.

**Exemple 2.3.** Considérons l'algèbre $A = K\langle x, y\rangle/(xy - yx)$
On choisit $w_\sigma = xy$ et $f_\sigma = yx$ et dans ce cas, on a $S^0 = \{y^m x^n |\, n, m \in \mathbb{N}\}$

**Définition 2.3** (Opérateur de réduction)**.** Pour tous $u, v \in W\, et\, w_\sigma$ on définit **l'opérateur de réduction élémentaire**, $\mathbb{K}$-linéaire

$$\begin{array}{cccccl} R_{(u,w_\sigma,v)} & : & T & \to & T & \\ & & uw_\sigma v & \mapsto & uf_\sigma v & \\ & & w & \mapsto & w & \text{si } w \neq uw_\sigma v \end{array}$$

$R$ est un **opérateur de réduction** si c'est la composée d'opérateurs de réduction élémentaires, à savoir

$$R = R_n...R_1 \text{ avec } R_i \text{ opérateur de réduction élémentaire}$$

*Remarque* 2.3. La composée d'applications linéaires étant encore linéaire, les opérateurs de réduction sont des opérateurs $\mathbb{K}$-linéaires.

Si on prend un tenseur dans $T$, le processus que l'on souhaite établir consiste à lui appliquer des opérateurs de réduction jusqu'à qu'il appartienne à S. On obtiendrait ainsi sa forme réduite. Seulement rien ne garantit que ce processus peut être réaliser avec un nombre fini d'opérateurs. Se pose également la question de l'unicité. Un même mot peut posséder deux formes réduites différentes, qui dépendent des opérateurs de réductions choisis.

**Définition 2.4.** On définit, les sous-ensemble $T_f$ et $T_u$ de $T$

$$\begin{aligned} T_f = \{ & t \in T \mid \text{pour toute suite } (R_n)_{n\in\mathbb{N}}, \text{ avec } R_n \text{ opérateur de} \\ & \text{réduction élémentaire, la suite } (R_n...R_0(t))_{n\in\mathbb{N}} \text{ est stationnaire,} \\ & i.e.\ \exists N \in \mathbb{N} \text{ tel que } R_n...R_0(t) = R_N...R_0(t),\ \forall n \geqslant N \} \end{aligned}$$

$$\begin{aligned} T_u = \{ & y \in T \mid \text{si } R\,et\,R' \text{ sont deux opérateurs de réductions tels que} \\ & R(t),\ R'(t) \in S, \quad \text{alors} \quad R(t) = R'(t) \} \end{aligned}$$

Pour tout $t \in T_u$, on définit $\mathcal{R}t = Rt$, où $R$ est un opérateur de réduction tel que $Rt \in S$. Cela nous permet de construire l'application **projection** de $T_u$ dans $S$,

$$\begin{array}{cccc} \mathcal{R} & : & T_u & \to & S \\ & & t & \mapsto & \mathcal{R}t. \end{array}$$

On appelle $\mathcal{R}t$ la **forme réduite** dans $S$ de $t \in T_u$.

*Remarque* 2.4. Noter que $t \in T_f$ si et seulement s'il existe un opérateur de réduction $R$ tel que $R(t) \in S$.

Par la suite on dira que les éléments dans $T_f$, sont de réduction finie et ceux dans $T_u$, de réduction unique.

*Remarque* 2.5. Noter les inclusions évidentes $S \subseteq T_u \subseteq T_f \subseteq T$.

**Proposition 2.1.** *$T_f$ et $T_u$ sont des sous-espaces vectoriels de $T$ et $\mathcal{R}$ est un opérateur $\mathbb{K}$-linéaire.*

*Preuve.* Il est clair que $\lambda t \in T_f$ (resp., $\lambda t \in T_u$ et que $\mathcal{R}(\lambda t) = \lambda\mathcal{R}(t)$) si $t \in T_f$ (resp., $t \in T_u$) et $\lambda \in \mathbb{K}$. Donc prouvons la stabilité par l'addition de $T_f$ et $T_u$ et l'additivité de $\mathcal{R}$.
Soient $t, t' \in T_f$ et $(R_n)_{n\in\mathbb{N}}$ une suite d'opérateurs élémentaires.
Il existe $N$, $N' \in \mathbb{N}$ tels que

$$R_n...R_0(t) = R_N...R_0(t)\,\forall n \geq N \text{ et } R_n...R_0(t') = R_{N'}...R_0(t')\,\forall n \geq N'.$$

On pose $N_0 = \max(N, N')$. Soit $n \geq N_0$,

$$\begin{aligned} R_n...R_0(t+t') &= R_n...R_0(t) + R_n...R_0(t') = R_N...R_0(t) + R_{N'}...R_0(t') \\ &= R_{N_0}...R_0(t) + R_{N_0}...R_0(t') = R_{N_0}...R_0(t+t'). \end{aligned}$$

La suite $(R_n...R_0(t+t'))_{n\in\mathbb{N}}$ est bien stationnaire, donc $t + t' \in T_f$.

Si maintenant $t, t' \in T_u$, alors notons $t_0, t_0'$ leur forme réduite. Par la remarque 2.5 et par ce qui précède $t + t' \in T_f$, donc il existe un opérateur $M$ tel que $M(t + t') = u_0 \in S$. Or on peut trouver des opérateurs $L, L'$ tels que $LMt = t_0$ et $L'LMt = t_0'$. D'où

$$u_0 = L'Lu_0 = L'LM(t+t') = L'LMt + L'LMt = t_0 + t_0,$$

ce qui prouve que $t + t' \in T_u$, et par la même occasion que $\mathcal{R}(t + t') = \mathcal{R}(t) + \mathcal{R}(t')$. $\square$

**Exemple 2.4.** Considérons l'algèbre $A = K\langle x, y\rangle/(xy - yx, yz = zy)$
On choisit $w_1 = xy$, $f_1 = yx$ et $w_2 = yz$, $f_2 = zy$ et on aimerait réduire le mot $xyz$. Deux possibilités s'offrent à nous.
0n lui applique l'opérateur de réduction élémentaire $R_{(1,w_1,z)}$,

$$R_{(1,w_1,z)}(xyz) = yxz \in S,$$

ou on lui applique $R_{(x,w_2,1)}$,

$$R_{(x,w_2,1)}(xyz) = xzy \in S.$$

On constate donc que $xyz$ possède deux formes réduites différentes : $xyz$ est donc dans $T_f$ mais pas $T_u$. Ici, ce fait est dû à ce que l'on nomme une ambiguïté.

**Définition 2.5** (Ambiguïtés)**.** Soit $(w_1, w_2, w_3) \in W^3$. On dit que $(w_1, w_2, w_3)$

1. est une **d'ambiguïté de chevauchement** (ou une ambiguïté de type C) s'il existe $\sigma$ et $\tau$ dans $\Sigma$ tel que $w_\sigma = w_1w_2$ et $w_\tau = w_2w_3$,
2. est une **d'ambiguïté d'inclusion** (ou une ambiguïté de type I) s'il existe $\sigma$ et $\tau$ dans $\Sigma$ tel que $w_\sigma = w_2$ et $w_\tau = w_1w_2w_3$.

**Définition 2.6.** En reprenant les même notations que ci-dessus, on dit qu'une ambiguïté $(w_1, w_2, w_3)$ est **résoluble** s'il existe deux opérateurs de réduction $R^{'}$, $R^{''}$ tels que

1. $R^{'}(f_\sigma w_3) = R^{''}(w_1 f_\tau) \in S$ si $(w_1, w_2, w_3)$ est une ambiguïté de type C,

2. $R^{'}(w_1 f_\sigma w_3) = R^{''}(f_\tau) \in S$ si $(w_1, w_2, w_3)$ est une ambiguïté de type I.

**Théorème 2.1.** *Si $T = T_f$, alors $T = S \oplus I$ si et seulement si $T = T_u$*

*Preuve.* Montrons tout d'abord que tout opérateur de réduction $\mathcal{R}$ vérifie que pour tout $t \in T$,

$$t \equiv \mathcal{R}(t) \bmod I. \tag{1}$$

La preuve se fait par récurrence sur le nombre d'opérateur de réduction élémentaires composant $\mathcal{R}$. Si $\mathcal{R} = R$ est un opérateur de réduction élémentaire, il vient immédiatement que $t \equiv R(t)$ modulo I.
Supposons désormais que pour tout $s \in T$ et pour tout $q \leqslant n$, $s - R_q ... R_1(s) \in I$. On a

$$\begin{aligned} t - R_{n+1}...R_1(t) &= t - R_1(t) + \underbrace{R_1(t)}_{s} - R_{n+1} \dots \underbrace{R_1(t)}_{s} \\ &= \underbrace{t - R_1(t)}_{\in I} + \underbrace{s - R_{n+1}...R_2(s)}_{\in I}, \end{aligned}$$

ce qui conclut la preuve par récurrence de (1).
Supposons que $T = S \oplus I$.

Ainsi si $t \in T = T_f$, alors il existe un opérateur $R$ tel que $R(t) = s$, avec $s \in S$. Donc $t \equiv s$ modulo I ce qui équivaut à $t = s + i$ avec $s \in S$ et $i \in I$. Or puisque $T = S \oplus I$, on obtient l'unicité de s et pour tout opérateur de réduction $R'$, $R'(t) = s$. Donc $T = T_u$.

Réciproquement, supposons que $T = T_u$. Ici $\mathcal{R}$ est ainsi la projection de T dans S. Donc $T = S \oplus K$, où K est le noyau de $\mathcal{R}$. Montrons que $K = I$. Supposons que $t \in K$. Il existe un opérateur de réduction $R$ tel que

$$R(t) = \mathcal{R}(t) = 0.$$

Or, on a montré ci-dessus que $t \equiv R(t)\ (modulo\, I) \equiv 0\ (modulo\, I)$. Donc $K \subset I$.

Pour l'inclusion inverse, soit $w_\sigma$ où $\sigma \in \Sigma$. Posons $t = uw_\sigma v$, avec $u, v \in W$ et considérons l'opérateur de réduction élémentaire $R = R_{(u,w_\sigma,v)}$. La forme réduite de $t$ étant unique, il s'ensuit que

$$\mathcal{R}t = \mathcal{R}(Rt) = \mathcal{R}(uf_\sigma v).$$

Par linéarité, cela donne

$$\mathcal{R}(u(w_\sigma - f_\sigma)v) = 0.$$

Ceci nous montre que $I \subset K$. On a donc bien $K = I$. $\square$

Ce théorème nous offre donc une condition nécessaire et suffisante pour que $T = S \oplus I$. La question qui se pose désormais est comment s'assurer que l'on a bien $T = T_u$ ? C'est ici que l'on va vouloir munir W d'un ordre monomial pour nous conduire au théorème de Bergman.

## 2.3 Théorème de Bergman

Soit $\mathbb{K}$ un corps, $X$ l'ensemble des lettres, $W$ celui des mots, et $T = Vect_{\mathbb{K}}(W)$, l'ensemble des tenseurs.

On rappelle que si $<$ est un ordre monomial sur $W$ alors il satisfait

(i) $1 < m, \quad \forall m \in W$,

(ii) $m_1 < m_2 \Rightarrow lm_1r < lm_2r, \quad \forall l, r, m_1, m_2 \in W$.

***Notation*** Soit $<$ est un ordre monomial sur $W$. Etant donnés $t = \sum_{i=1}^{n} c_i w_i \in T$, avec $c_i \neq 0$, $\forall i \in [\![1, n]\!]$ et $w' \in W$, alors écrit

$$t < w' \text{ si et seulement si } w_i < w' \text{ pour tout } 1 \leq i \leq n.$$

**Définition 2.7** (Condition de chaîne descendante (DCC en anglais))**.** Si $<$ est un ordre sur un ensemble $E$, alors on dit que $<$ satisfait la DCC si toute suite descendante $x_1 > x_2 > ... > x_n > \dots$ dans $E$ est stationnaire, *i.e.* il existe un $n_0$ tel que $x_m = x_{n_0}$, pour tout $m \geqslant n_0$.

*Remarque* 2.6. On note que $E$ est muni d'un ordre qui satisfait la DCC équivaut à dire que tout sous-ensemble non vide $S$ inclus dans $E$ possède un élément minimal, *i.e.* il existe $S$ tel que pour tout $y \in E$, $y < x$ implique $y \notin S$. En effet s'il existe un sous-ensemble non vide $S$ ne possédant pas d'élément minimal, alors si $x_1$ est dans S, il existe un $x_2$ dans $S$ tel que $x_1 > x_2$. Mais de même, il existe un $x_3$ dans $S$ tel que $x_1 > x_2 > x_3$, et ainsi de suite. On obtient donc une suite descendante $x_1 > x_2 > ... > x_n > \dots$ infinie. Réciproquement, si tout sous-ensemble de $E$ admet un élément minimal et si $x_1 > x_2 > ... > x_n > \dots$ est une suite descendante d'éléments de E, alors on considère le sous-ensemble $S = \{x_1, ..., x_n, ...\}$. $S$ possède un élément minimal, noté $x_k$. Et pour tout $m \geqslant k$, puisque $x_m < x_k$ alors $x_m$ n'est pas dans $S$, donc $S$ est fini.

**Exemple 2.5.** L'ordre deglexicographique de l'exemple 2.2 est un ordre qui satisfait la DCC.

Désormais, à partir de maintenant, on munit $W$ d'un ordre monomial $<$, et on suppose en plus que $<$ satisfait les conditions suivantes

(iii) $<$ satisfait la DDC,

(iv) $\forall \sigma \in \Sigma$, $f_\sigma < w_\sigma$.

Les opérateurs de réductions, définis précédemment, sont dénommés ainsi car avec la conditions (*iv*), il est bien question de réduire la taille de chaque mots.

**Théorème 2.2** (Bergman)**.** *Si $W$ est munit d'un ordre comme ci-dessus, alors $T = S \oplus I$ si et seulement si toutes les ambiguïtés sont résolubles.*

*Preuve.* Tout d'abord, on remarque ici que $T = T_f$. En effet, si $T \neq T_f$, soit $P = T \setminus T_f$ et soit $w$ un élément minimal de $P$. Un tel $w$ existe bien par la condition (iii) et la remarque 2.6. Or $w$ ne peut être un tenseur de réduction fini, donc il existe une suite d'opérateurs de réduction élémentaire $(R_n)_{n\in\mathbb{N}^*}$ telle que $R_n \dots R_1(w) < R_{n-1} \dots R_1(w)$ pour tout $n \in \mathbb{N}^*$. Mais par la conditions (*iv*), $R_1(w) < w$ donc $R_1(w) \in T_f$. Or ceci implique également que $w \in T_f$.

Par le théorème. 2.1, il suffit donc de montrer que toutes les ambiguïtés résolubles équivaut à $T = T_u$. Mais s'il existe une ambiguïté non résoluble, on obtient aisément que $T \neq T_u$, ce qui justifie l'une des implications.

Désormais, supposons que toutes les ambiguïtés sont résolubles et montrons que $T = T_u$. Supposons que ce n'est pas vrai, *i.e.* $T \neq T_u$. Soit $W_u = W \cap T_u$. La condition précédente est équivalente à $Q = W \setminus W_u \neq \emptyset$. C'est clair que $1 \neq Q$. D'après (iii) et la Remarque 2.6, il existe un élément minimal $w$ dans $Q$. En conséquence, $w' \in W_u$ pour tout $w' < w$. On va trouver une contradiction. En effet, on va montrer que, étant donné $w \in W$ tel que $w' \in W_u$ pour tout $w' < w$ implique $w \in W_u$.
Au préalable, si $t = \sum_{u\in W} c_u u$, alors on note qu'il y a également les opérateurs de réduction $R_{(t,w_\sigma,v)} := \sum_{u\in W} c_u R_{(u,w_\sigma,v)}$ et symétriquement, $R_{(v,w_\sigma,t)} := \sum_{u\in W} c_u R_{(v,w_\sigma,u)}$.

Soient $(R_n)_{n\in\mathbb{N}^*}$ et $(S_n)_{n\in\mathbb{N}^*}$ deux suites d'opérateurs de réduction élémentaires avec $R_1 = R_{(u_1,w_\rho,v_1)}$ et $S_1 = R_{(y_1,w_\sigma,z_1)}$. On peut supposer sans perte de généralité que $R_1(w) \neq w$ et $S_1(w) \neq w$. On sait que $w \in T_f$ , donc pour $n$ suffisamment grand $R_n \dots R_1(w)$ et $S_n \dots S_1(w)$ sont dans $S$. Montrons que $R_n \dots R_1(w) = S_n \dots S_1(w)$ pour $n$ suffisamment grand. On rappelle que $R_1(w) < w$ et $S_1(w) < w$, donc par hypothèse $R_1 w$ et $S_1 w$ appartiennent à $T_u$. On distingue trois cas différents.

**Cas 1.** Si $w = uw_\rho xw_\sigma v$, alors $u_1 = u$, $v_1 = xw_\sigma v$, $y_1 = uw_\rho x$ et $z_1 = v$. On pose $R'_1 = R_{(u,w_\rho,xf_\sigma v)}$ et $S'_1 = R_{(uf_\rho x,w_\sigma,v)}$ et on a

$$S'_1 R_1(w) = uf_\rho xf_\sigma v = R'_1 S_1(w).$$

Or pour toute suite $(T_n)_{n\in\mathbb{N}^*}$ d'opérateurs de réduction élémentaires, avec $n$ et $m$ suffisamment grands

$$\begin{aligned}(R_n \dots R_2)(R_1 w) &= (T_m \dots T_2)(S'_1(R_1 w)) = (T_m \dots T_2)(R'_1(S_1 w)) \\ &= (S_n \dots S_2)(S_1 w).\end{aligned}$$

**Cas 2.** Si $w_\rho$ et $w_\sigma$ se chevauchent. Quitte à intervertir $w_\rho$ et $w_\sigma$, on peut supposer que $w = uw_1w_2w_3v$ où $w_\rho = w_1w_2$ et $w_\sigma = w_2w_3$ avec $u, v \in W$ alors $u_1 = u$, $v_1 = w_3v$, $y_1 = uw_1$ et $z_1 = v$. Par hypothèse, il existe $R''$ et $S''$, opérateurs de réduction tels que $R''(f_\rho w_3) = S''(w_1 f_\sigma) \in S$.
On considère les opérateurs de réduction $R''_1$ et $S''_1$ tels que pour tout $t \in T$,

$$u(R''t)v = R''_1(t) \text{ et } u(S''t)v = S''_1(t),$$

et on a

$$S''_1(uf_\rho w_3 v) = R''_1(uw_1 f_\sigma v).$$

Enfin, comme précédemment, pour toute suite $(T_n)_{n\in\mathbb{N}^*}$ d'opérateurs de réduction élémentaires, pour $n$ et $m$ suffisamment grands,

$$\begin{aligned}(R_n \dots R_2)(R_1(w)) &= (T_m \dots T_2)(S''_1(R_1(w))) = (T_m \dots T_2)(R''_1(S_1(w))) \\ &= (S_n \dots S_2)(S_1(w)).\end{aligned}$$

**Cas 3.** Si $w_\sigma$ est inclus dans $w_\tau$ ou inversement, alors la preuve est similaire au cas 2.

Ainsi on a prouvé que dans les trois cas, $w \in W_u$, on donc bien une contradiction.

□

La dernière étape est de donc de trouver un processus nous permettant de pouvoir trouver une famille $(w_\sigma)_{\sigma\in\Sigma}$ dans laquelle toutes les ambiguïtés sont résolubles.

## 2.4 Base de Gröbner et algorithme de Buchberger-Bergman

On note $G = \{(w_\sigma - f_\sigma) \mid \sigma \in \Sigma\}$, et on s'intéresse toujours à l'algèbre $A = T/I$, avec $I$ l'idéal engendré par G. On rappelle que $W$ est munit du même ordre que dans la partie précédente, ainsi $T = T_f$.

Désormais, considérons un second ensemble $H = \{(w_i - f_i) \mid i \in I\} \subset T$ composé d'autres relations.

***Notation.*** Pour réduire l'extension, dans toute la suite, on confondra l'ambiguïté $(w_1, w_2, w_3)$ et le mot $w_1w_2w_3$.

**Définition 2.8.** On pose $A(G, H)$, l'ensemble de toutes les ambiguïtés possibles relativement à $G$ et $H$, *i.e.*, $w_1w_2w_3 \in A(G, H)$ si et seulement s'il existe $(w_\sigma - f_\sigma, w_i - f_i) \in G \times H$ tel que l'on est dans l'un des quatre cas suivants :

1. $w_\sigma = w_1w_2$ et $w_i = w_2w_3$,
2. $w_i = w_1w_2$ et $w_\sigma = w_2w_3$,
3. $w_\sigma = w_2$ et $w_i = w_1w_2w_3$,
4. $w_i = w_2$ et $w_\sigma = w_1w_2w_3$.

**Définition 2.9** (Base de Gröbner)**.** $G$ est une base de Gröbner de I si et seulement si toutes les ambiguïtés dans $A(G, G)$ sont résolubles.

*Remarque* 2.7. Dans la plupart des ouvrages, la définition énoncée ci-dessus est une caractérisation des bases de Gröbner. On peut trouver une autre définition faisant intervenir un formalisme différent (voir [1], section 3.1).

**Définition 2.10.** Une base de Gröbner $G$ de $I$ est dite minimale si toute partie $G' \subsetneq G$ non vide n'est pas une base de Gröbner de I.

**Définition 2.11** (S-polynôme)**.** Selon les différents cas énoncés dans la Définition 2.8, on définit l'application $S : A(G, H) \to T$ par

1. $S(w_1w_2w_3) = (w_\sigma - f_\sigma)w_3 - w_1(w_i - f_i) = -f_\sigma w_3 + w_1 f_i$,
2. $S(w_1w_2w_3) = (w_i - f_i)w_3 - w_1(w_\sigma - f_\sigma) = -f_i w_3 + w_1 f_\sigma$,
3. $S(w_1w_2w_3) = w_1(w_\sigma - f_\sigma)w_3 - (w_i - f_i) = -w_1 f_\sigma w_3 + f_i$,
4. $S(w_1w_2w_3) = w_1(w_i - f_i)w_3 - (w_\sigma - f_\sigma) = -w_1 f_i w_3 + f_\sigma$.

**Proposition 2.2** (Caractérisation des bases de Gröbner non commutatives)**.** *On a l'équivalence entre les propriétés suivantes :*

*(i)* *$G$ est une base de Gröbner de $I$;*

*(ii)* $T = S \oplus I$ *;*

*(iii)* $T = T_u$ *;*

*(iv)* *Pour tout $w_1w_2w_3$ dans $A(G, G)$, $S(w_1w_2w_3)$ possède une forme réduite égale à* 0.

*Preuve.* On a déja prouvé *(i)* $\Leftrightarrow$ *(ii)* $\Leftrightarrow$ *(iii)*, donc montrons *(iii)* $\Rightarrow$ *(iv)* et *(iv)* $\Rightarrow$ *(i)*.

*(iii)* $\Rightarrow$ *(iv)*. On a $T = T_u$, donc si $w_1w_2w_3 \in A(G,G)$ est de type C (resp. de type I), alors $\mathcal{R}(w_1w_2w_3) = \mathcal{R}(f_\sigma w_3) = \mathcal{R}(w_1 f_\tau)$ (resp. $\mathcal{R}(w_1w_2w_3) = \mathcal{R}(w_1 f_\sigma w_3) = \mathcal{R}(f_\tau)$), et on a

$$\mathcal{R}(S(w_1w_2w_3)) = -\mathcal{R}(f_\sigma w_3) + \mathcal{R}(w_1 f_\tau) = 0$$

(resp. $\mathcal{R}(S(w_1w_2w_3)) = -\mathcal{R}(w_1(w_\sigma - f_\sigma)w_3) + \mathcal{R}(f_\tau) = 0$).

*(iv)* $\Rightarrow$ *(i)*. Prenons une ambiguïté $w_1w_2w_3$ de type C (resp. de type I) dans $A(G,G)$, et supposons qu'elle a une forme réduite nulle. Alors il existe un opérateur de réduction $R$ tel que $R(-f_\sigma w_3 + w_1 f_\tau) = 0$ (resp. $R(-w_1 f_\sigma w_3 + f_\tau) = 0$). D'où $R(f_\sigma w_3) = R(w_1 f_\tau)$ (resp. $R(w_1 f_\sigma w_3) = R(f_\tau)$ ). Donc cette ambiguïté est résoluble.

$\square$

Le but de l'algorithme de Buchberger-Bergman, que nous présentons ci-dessous, est donc d'ajouter progressivement et récursivement à l'ensemble $G$, les formes réduites de $S(w)$ non nulle, pour tout $w$ dans $A(G,G)$.

**Algorithme de Buchberger-Bergman**

$i := 0$ ; $G_0 = G$ $H_0 = G$ ;
**tant que** $H_i \neq \emptyset$ **faire**
  $H_{i+1} := \emptyset$ ;
  $A_i := A(G_i, H_i)$ ;
  **tant que** $A_i \neq \emptyset$ **faire**
    choisir $w \in A_i$ ;
    $A_i := A_i - \{w\}$ ;
    $s := S(w)$ ;
    **si** $s$ *ne possède pas de forme réduite égale à 0* **alors**
      $H_{i+1} := H_{i+1} \cup \{r\}$, ou r est une forme réduite de $S(w)$ ;
    **fin**
  **fin**
  $G_{i+1} = G_i \cup H_{i+1}$ ;
  $i := i + 1$ ;
**fin**

## *Commentaires sur l'algorithme.*

Si $r$ est une forme réduite que l'on ajoute à $G$, alors $r$ peut s'écrire $r = c_\theta w_\theta - f_\theta$, avec $w_\theta > f_\theta$ et $c_\theta \in \mathbb{K}$.

Cet algorithme se termine en un certain $i + 1$, si et seulement si en sortie $G_i$ est notre base de Gröbner (pour la preuve voir [1], page 49-50). Néanmoins, soulignons le fait important que cet algorithme ne s'arrête pas nécessairement.

Dans le cas où l'algorithme se termine, on remarque également que la base que nous obtenons n'est pas minimale. En effet, il se peut que certaines formes réduites que l'on ajoute à $G$ deviennent des formes réduites nulle suite à certains ajouts postérieurs. Dans les calculs qui vont suivre, nous chercherons à obtenir une base minimal. Ainsi, en certains points, nous dévierons légèrement de l'algorithme, notamment pour le calcul de la base de Gröbner de l'algèbre de Fomin-Kirillov $FK(4)$.

# 3 Calculs

## 3.1 Préliminaires

On travaillera sur le corps $\mathbb{C}$. Pour $n \geq 2$, on considère l'ensemble

$$X(n) = \big\{[i,j] \mid 1 \leq i < j \leq n\big\}$$

Et on note $T(n)$, la $\mathbb{C}$-algèbre engendrée par $X(n)$.

*Remarque* 3.1. Si on pose $V(n) := Vect_{\mathbb{K}}(X(n)) \subset T(n)$, alors pour tout $j > i$, on note $[j,i] := -[i,j] \in V(n)$. Dans toute la suite on utilisera cette notation.

Maintenant considérons les sous-ensemble de T(n) suivants,

- $\mathbf{R}_2(n) = \big\{[i,j]^2 \mid i,j \in [\![1,n]\!] \text{ avec } \#\{i,j\} = 2\big\}$,
- $\mathbf{R}_3(n) = \big\{[i,j][j,k] + [j,k][k,i] + [k,i][i,j] \mid i,j,k \in [\![1,n]\!] \text{ avec } \#\{i,j,k\} = 3\big\}$, $\forall n \geq 3$ (sinon $\mathbf{R}_3(n) = \emptyset$) ,
- $\mathbf{R}_4(n) = \big\{[i,j][k,l] - [k,l][i,j] \mid i,j,k,l \in [\![1,n]\!] \text{ avec } \#\{i,j,k,l\} = 4\big\}$, $\forall n \geq 4$ (sinon $\mathbf{R}_4(n) = \emptyset$).

Et on pose, $I(n)$ l'idéal bilatère engendré par $\mathbf{R}_2(n) \cup \mathbf{R}_3(n) \cup \mathbf{R}_4(n)$.

**Définition 3.1.** L'algèbre $T(n)/I(n)$ est appelée **algèbre de Fomin-Kirillov** et est notée **FK(n)**.

De même on considère, $X^*(n) = \big\{\langle i,j\rangle \mid 1 \leq i < j \leq n\big\}$, et $T^*(n)$ est la $\mathbb{C}$-algèbre engendrée par $X^*(n)$. Comme précédemment on pose $V^*(n) := Vect_{\mathbb{K}}(X(n)) \subset T^*(n)$, et pour tout $j > i$, on note $\langle j,i\rangle := -\langle i,j\rangle \in V^*(n)$. De plus on considère

- $\mathbf{R}^*_3(n) = \big\{\langle i,j\rangle\langle j,k\rangle + \langle j,k\rangle\langle i,k\rangle \mid i,j,k \in [\![1,n]\!]\ avec\ \#\{i,j,k\} = 3\big\}$, $\forall n \geq 3$ (sinon $\mathbf{R}^*_3(n) = \emptyset$),
- $\mathbf{R}^*_4(n) = \big\{\langle i,j\rangle\langle k,l\rangle + \langle k,l\rangle\langle i,j\rangle \mid i,j,k,l \in [\![1,n]\!]\ avec\ \#\{i,j,k,l\} = 4\big\}$, $\forall n \geq 4$ (sinon $\mathbf{R}^*_4(n) = \emptyset$).

Et $I^*(n)$ est l'idéal bilatère engendré par $\mathbf{R}^*_3(n) \cup \mathbf{R}^*_4(n)$.

**Définition 3.2.** L'algèbre $T^*(n)/I^*(n)$ est appelée **dual quadratique de** $FK(n)$ et est notée $FK^*(n)$.

L'objectif de ce qui suit est d'étudier les algèbres $FK(3)$, $FK^*(3)$, $FK(4)$ et notamment de leur trouver une base de Gröbner minimale en appliquant l'algorithme de Buchberger-Bergman. Pour chacune de ces algèbres, on choisira un ordre sur les éléments dans $X(n)$ (resp. $X^*(n)$) et on appliquera sur $W(n)$ (resp. $W^*(n)$) l'ordre deglexicographique, défini dans l'Exemple 2.2.

## 3.2 Algèbre de Fomin-Kirillov FK(3)

Dans cette partie, on calcule une base de Gröbner, $\mathcal{B}_{FK(3)}$, de $FK(3)$. Commençons par donner tous les éléments dans $R_2(3)$ et $R_3(3)$. On a $R_2(3) = \{[1,2]^2, [1,3]^2, [2,3]^2\}$. Et $R_3(3) = \{[1,2][2,3]+[2,3][3,1]+[3,1][1,2], [1,3][3,2]+[3,2][2,1]+[2,1][1,3] = [3,1][2,3]+[2,3][1,2]+[1,2][3,1]\}$.

Pour faciliter l'écriture, on pose $[1,2] = a$, $[2,3] = b$, $[3,1] = c$ et on introduit l'ordre suivant sur les lettres :

$$\boxed{a < b < c}$$

et on peut désormais débuter l'algorithme.

### *Début de l'algorithme*

**Premières relations**

$$\boxed{a^2 = 0} \tag{1}$$

$(w_1 = a^2,\ f_1 = 0)$,

$$\boxed{b^2 = 0} \tag{2}$$

$(w_2 = b^2,\ f_2 = 0)$,

$$\boxed{c^2 = 0} \tag{3}$$

$(w_3 = c^2,\ f_3 = 0)$,

$$\boxed{ca = -ab - bc} \tag{4}$$

$(w_4 = ca,\ f_4 = -ab - bc)$,

$$\boxed{cb = -ac - ba} \tag{5}$$

$(w_5 = cb,\ f_5 = -ac - ba)$.

**Liste ambiguïtés 1.** (On exhibe ici la liste $A_1$, de toutes les ambiguïtés données par les 5 relations ci-dessus). $A_1 = \{a^3,\ b^3,\ c^3,\ c^2a,\ c^2b\ ca^2,\ cb^2\}$

**Ambiguïtés non résolubles 1.** (On donne l'ensemble $B_1$, des ambiguïtés qui ne sont pas résolubles parmi celles présentées ci-dessus et on calcule $S(x)$, pour tout $x$ dans $B_1$). $B_1 = \{ca^2\}$.

$$\begin{aligned} S(ca^2) &= (ca + ab + bc)a - ca^2 = aba + bca = aba + b(-ab - bc) \\ &= aba - bab - b^2c = aba - bab. \end{aligned}$$

**Nouvelle relation.**

$$\boxed{bab = aba} \tag{6}$$

($w_6 = ede$, $f_6 = -ded$).

**Liste ambiguïtés 2.** : $A_2 = \{bab^2,\ b^2ab,\ cbab,\ babab\}$.

**Ambiguïtés non résolubles 2.** : $B_2 = \emptyset$.

## *Fin de l'algorithme.*

La base de Gröbner $\mathcal{B}_{FK(3)}$ est donc donnée par

$\mathcal{B}_{FK(3)} = \{a^2, b^2, c^2, ca + ab + bc, cb + ac + ba, bab - aba\}$

Ou encore,

$$\mathcal{B}_{FK(3)} = \left\{ \begin{array}{c} [1,2]^2, [2,3]^2, [3,1]^2, [3,1][1,2] + [1,2][2,3] + [2,3][3,1], \\ [3,1][2,3] + [1,2][3,1] + [2,3][1,2], [2,3][1,2][2,3] - [1,2][2,3][1,2] \end{array} \right\}$$

## 3.3 Dual quadratique FK*(3)

### 3.3.1 Calcul de la base de Gröbner

Comme précédemment, on calcule une base de Gröbner, $\mathcal{B}_{FK^*(3)}$ de $FK^*(3)$.

On écrit la liste exhaustive des éléments distincts dans $R_3^*(4)$.

$$\begin{aligned} R_3^*(4) = \{&\langle 1,2\rangle\langle 2,3\rangle + \langle 2,3\rangle\langle 1,3\rangle = \langle 1,2\rangle\langle 2,3\rangle - \langle 2,3\rangle\langle 3,1\rangle, \\ &\langle 1,3\rangle\langle 3,2\rangle + \langle 3,2\rangle\langle 1,2\rangle = \langle 3,1\rangle\langle 2,3\rangle - \langle 2,3\rangle\langle 1,2\rangle, \\ &\langle 2,1\rangle\langle 1,3\rangle + \langle 1,3\rangle\langle 2,3\rangle = \langle 1,2\rangle\langle 3,1\rangle - \langle 3,1\rangle\langle 2,3\rangle, \\ &\langle 2,3\rangle\langle 3,1\rangle + \langle 3,1\rangle\langle 2,1\rangle = \langle 2,3\rangle\langle 3,1\rangle - \langle 3,1\rangle\langle 1,2\rangle, \\ &\langle 3,1\rangle\langle 1,2\rangle + \langle 1,2\rangle\langle 3,2\rangle = \langle 3,1\rangle\langle 1,2\rangle - \langle 1,2\rangle\langle 2,3\rangle, \\ &\langle 3,2\rangle\langle 2,1\rangle + \langle 2,1\rangle\langle 3,1\rangle = \langle 2,3\rangle\langle 1,2\rangle - \langle 1,2\rangle\langle 3,1\rangle\}. \end{aligned}$$

On pose $\langle 1,2\rangle = A$, $\langle 2,3\rangle = B$, $\langle 3,1\rangle = C$ et on introduit l'ordre suivant sur les lettres :

$$\boxed{A < B < C.}$$

En réécrivant les relations, on obtient $BC = AB$, $CB = BA$, $CB = AC$, $CA = BC$, $CA = AB$, $BA = AC$. On observe que certaines de ces relations se simplifient. En effet, $CB = BA$ donne $CB = AC$ en utilisant que $BA = AC$. On retrouve une relation déjà connue, donc on peut la supprimer. De même $CA = BC$, est supprimable. On trouve donc 4 premières relations.

## *Début de l'algorithme.*

**Premières relations.**

$$\boxed{BA = AC} \tag{1}$$

$(w_1 = BA,\ f_1 = AC)$,

$$\boxed{BC = AB} \tag{2}$$

$(w_2 = BC,\ f_2 = AB)$,

$$\boxed{CA = AB} \tag{3}$$

$(w_3 = CA,\ f_3 = AB)$,

$$\boxed{CB = AC} \tag{4}$$

$(w_4 = CB,\ f_4 = AC)$.

**Liste ambiguïtés 1.** $A_1 = \{BCA,\ BCB,\ CBA,\ CBC\}$.

**Ambiguïtés non résolubles 1.** : $B_1 = \{BCB, CBC\}$.

$$S(BCB) = (BC - AB)B - B(CB - AC) = -AB^2 + BAC - AB^2 + AC^2,$$
$$S(CBC) = -AB^2 + AC^2.$$

**Nouvelle relation.**

$$\boxed{AC^2 = AB^2} \tag{5}$$

$(w_3 = AC^2,\ f_3 = AB^2)$.

**Liste ambiguïtés 2.** $A_2 = \{BAC^2,\ CAC^2,\ AC^2A,\ AC^2B\}$.

**Ambiguïtés non résolubles 2.** : $B_2 = \{CAC^2, AC^2B\}$.

$$\begin{aligned} S(CAC^2) &= (CA - AB)C^2 - C(AC^2 - AB^2) = -ABC^2 + CAB^2 \\ &= -A^2BC + AB^3 = -A^3B + AB^3, \\ S(AC^2B) &= -A^3B + AB^3. \end{aligned}$$

**Nouvelle relation.**

$$\boxed{AB^3 = A^3B} \tag{6}$$

$(w_3 = AB^3,\ f_3 = A^3B)$.

**Liste ambiguïtés 3.** : $A_3 = \{AB^3A,\ AB^3C,\ BAB^3,\ CAB^3\}$.

**Ambiguïtés non résolubles 3.** : $B_3 = \emptyset$.

## ***Fin de l'algorithme.***

La base de Gröbner, $\mathcal{B}_{FK^*(3)}$, est donc donnée par

$\mathcal{B}_{FK^*(3)} = \{BA - AC, BC - AB, CA - AB, CB - AC, AC^2 - AB^2, AB^3 - A^3B\}$,
à savoir,

$$\mathcal{B}_{FK^*(3)} = \left\{ \begin{array}{c} \langle 2,3\rangle\langle 1,2\rangle - \langle 1,2\rangle\langle 3,1\rangle, \langle 2,3\rangle\langle 3,1\rangle - \langle 1,2\rangle\langle 2,3\rangle, \\ \langle 3,1\rangle\langle 1,2\rangle - \langle 1,2\rangle\langle 2,3\rangle, \langle 3,1\rangle\langle 2,3\rangle - \langle 1,2\rangle\langle 3,1\rangle, \\ \langle 1,2\rangle\langle 3,1\rangle^2 - \langle 1,2\rangle\langle 2,3\rangle^2, \langle 1,2\rangle\langle 2,3\rangle^3 - \langle 1,2\rangle^3\langle 2,3\rangle \end{array} \right\}.$$

### 3.3.2 Calcul de la table de multiplication

Grâce à la base de Gröbner, on peut en déduire la base de $A$, à savoir l'ensemble $S_0$ et on trouve

$$\boxed{S^0 = \{1, A^n, B^n, C^n, A^nC, A^nB, A^nB^2 \,|\, n \geq 1\}.}$$

Dans cette section, on aimerait calculer la table de multiplication de l'algèbre A. Commençons tout d'abord par montrer quelques résultats intermédiaires.

On a

$$\boxed{A^nC^m = \begin{cases} A^{n+m-2}B^2 & \text{si m pair} \\ A^{n+m-1}C & \text{si m impair.} \end{cases}} \quad (1)$$

*Preuve.* Par récurrence sur m, on fixe $n \in \mathbb{N}$. Le cas $m = 1$ est clair.
Si $m = 2$, $A^nC^2 = A^{n-1}AC^2 = A^{n-1}AB^2 = A^nB^2$.
Supposons le résultat vrai au rang m, alors si m pair,
$A^nC^{m+1} = A^nC^mC = A^{n+m-2}B^2C = A^{n+m-2}BAB = A^{n+m-2}ACB$
$= A^{n+m-2}A^2C = A^{n+m}C$.
Si m impair $A^nC^{m+1} = A^nC^mC = A^{n+m-1}C^2 = A^{n+m-1}B^2$.

□

$$\boxed{A^nB^m = \begin{cases} A^{n+m-2}B^2 & \text{si m pair} \\ A^{n+m-1}B & \text{si m impair.} \end{cases}} \quad (2)$$

La preuve est similaire à précédemment.

On a également

$$\boxed{B^mA^n = \begin{cases} A^nB^m & \text{si n pair} \\ A^nC^m & \text{si n impair.} \end{cases}} \quad (3)$$

*Preuve.* Montrons par récurrence sur n que $BA^n = \begin{cases} A^nB & \text{si n pair} \\ A^nC & \text{si n impair.} \end{cases}$
Si $n = 1$, on bien que $BA = AC$. Supposons l'hypothèse vraie au rang n, alors si n pair, $BA^{n+1} = A^nBA = A^{n+1}C$, et si n impair, $BA^{n+1} = A^nCA = A^{n+1}B$.
Enfin par une récurrence immédiate sur m on obtient bien,
$B^mA^n = \begin{cases} A^nB^m & \text{si n pair} \\ A^nC^m & \text{si n impair.} \end{cases}$

□

$$\boxed{C^mA^n = \begin{cases} A^nC^m & \text{si n pair} \\ A^nB^m & \text{si n impair.} \end{cases}} \quad (4)$$

La preuve est similaire à précédemment.

Et en enfin on a

$$\boxed{BC^n = A^nB.} \tag{5}$$

*Preuve.* Par récurrence sur n. Si $n = 1$, $BC = AB$.
Si vrai au rang n, $BC^{n+1} = BC^nC = A^nBC = A^{n+1}B$.

□

$$\boxed{CB^n = A^nC.} \tag{6}$$

La preuve est similaire à précédemment.

Désormais, grâce à l'ensemble de ces résultats, procédons aux calculs.
Par exemple calculons $B^nC^m$ (on utilisera ici les résultats (5),(3),(2) et (1)).
$B^nC^m = B^{n-1}BCC^{m-1} = B^{n-1}ABC^{m-1} = B^{n-1}A^mB$.
On voit désormais qu'il faut différencier les cas m pair ou m impair.
Si m pair, alors

$$B^nC^m = A^mB^n = \begin{cases} A^{n+m-2}B^2 & \text{si n pair} \\ A^{n+m-1}B & \text{si n impair.} \end{cases}$$

Si m impair, alors

$$B^nC^m = A^mC^{n-1}B = \begin{cases} A^{n+m-1}C & \text{si n pair} \\ A^{n+m-1}B & \text{si n impair.} \end{cases}$$

Par des calculs similaires, on trouve ainsi les différentes tables de multiplication dans $S^0$ en fonction de la parité de n et m.

**Si n et m pairs.**

| $\times$ | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
| $A^n$ | $A^n$ | $A^{n+m}$ | $A^{n+m-2}B^2$ | $A^{n+m-2}B^2$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $B^n$ | $B^n$ | $A^{n+m-2}B^2$ | $B^{n+m}$ | $A^{n+m-2}B^2$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $C^n$ | $C^n$ | $A^{n+m-2}B^2$ | $A^{n+m-2}B^2$ | $C^{n+m}$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $A^nC$ | $A^nC$ | $A^{n+m}C$ | $A^{n+m}C$ | $A^{n+m}C$ | $A^{n+m}B^2$ | $A^{n+m+1}C$ | $A^{n+m+2}C$ |
| $A^nB$ | $A^nB$ | $A^{n+m}B$ | $A^{n+m}B$ | $A^{n+m}B$ | $A^{n+m+1}B$ | $A^{n+m}B^2$ | $A^{n+m+2}B$ |
| $A^nB^2$ | $A^nB^2$ | $A^{n+m}B^2$ | $A^{n+m}B^2$ | $A^{n+m}B^2$ | $A^{n+m+2}C$ | $A^{n+m+2}B$ | $A^{n+m+2}B^2$ |

**Si n pair et m impair.**

| $\times$ | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
| $A^n$ | $A^n$ | $A^{n+m}$ | $A^{n+m-1}B$ | $A^{n+m-1}C$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $B^n$ | $B^n$ | $A^{n+m-2}B^2$ | $B^{n+m}$ | $A^{n+m-1}C$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $C^n$ | $C^n$ | $A^{n+m-2}B^2$ | $A^{n+m-1}B$ | $C^{n+m}$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $A^nC$ | $A^nC$ | $A^{n+m}B$ | $A^{n+m}C$ | $A^{n+m-1}B^2$ | $A^{n+m+1}B$ | $A^{n+m}B^2$ | $A^{n+m+2}B$ |
| $A^nB$ | $A^nB$ | $A^{n+m}C$ | $A^{n+m}B^2$ | $A^{n+m}B$ | $A^{n+m}B^2$ | $A^{n+m+1}C$ | $A^{n+m+2}C$ |
| $A^nB^2$ | $A^nB^2$ | $A^{n+m}B^2$ | $A^{n+m+1}B$ | $A^{n+m+1}C$ | $A^{n+m+2}C$ | $A^{n+m+2}B$ | $A^{n+m+2}B^2$ |

**Si n impair et m pair.**

| $\times$ | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
| $A^n$ | $A^n$ | $A^{n+m}$ | $A^{n+m-2}B^2$ | $A^{n+m-2}B^2$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $B^n$ | $B^n$ | $A^{n+m-1}B$ | $B^{n+m}$ | $A^{n+m-1}B$ | $A^{n+m}B$ | $A^{n+m-1}B^2$ | $A^{n+m+1}B$ |
| $C^n$ | $C^n$ | $A^{n+m-1}C$ | $A^{n+m-1}C$ | $C^{n+m}$ | $A^{n+m-1}B^2$ | $A^{n+m}C$ | $A^{n+m+1}C$ |
| $A^nC$ | $A^nC$ | $A^{n+m}C$ | $A^{n+m}C$ | $A^{n+m}C$ | $A^{n+m}B^2$ | $A^{n+m+1}C$ | $A^{n+m+2}C$ |
| $A^nB$ | $A^nB$ | $A^{n+m}B$ | $A^{n+m}B$ | $A^{n+m}B$ | $A^{n+m+1}B$ | $A^{n+m}B^2$ | $A^{n+m+2}B$ |
| $A^nB^2$ | $A^nB^2$ | $A^{n+m}B^2$ | $A^{n+m}B^2$ | $A^{n+m}B^2$ | $A^{n+m+2}C$ | $A^{n+m+2}B$ | $A^{n+m+2}B^2$ |

**Si n et m impairs.**

| $\times$ | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | $A^m$ | $B^m$ | $C^m$ | $A^mC$ | $A^mB$ | $A^mB^2$ |
| $A^n$ | $A^n$ | $A^{n+m}$ | $A^{n+m-1}B$ | $A^{n+m-1}C$ | $A^{n+m}C$ | $A^{n+m}B$ | $A^{n+m}B^2$ |
| $B^n$ | $B^n$ | $A^{n+m-1}C$ | $B^{n+m}$ | $A^{n+m-1}B$ | $A^{n+m-1}B^2$ | $A^{n+m}C$ | $A^{n+m+1}C$ |
| $C^n$ | $C^n$ | $A^{n+m-1}B$ | $A^{n+m-1}C$ | $C^{n+m}$ | $A^{n+m}B$ | $A^{n+m-1}B^2$ | $A^{n+m+1}B$ |
| $A^nC$ | $A^nC$ | $A^{n+m}B$ | $A^{n+m}C$ | $A^{n+m-1}B^2$ | $A^{n+m+1}B$ | $A^{n+m}B^2$ | $A^{n+m+2}B$ |
| $A^nB$ | $A^nB$ | $A^{n+m}C$ | $A^{n+m}B^2$ | $A^{n+m}B$ | $A^{n+m}B^2$ | $A^{n+m+1}C$ | $A^{n+m+2}C$ |
| $A^nB^2$ | $A^nB^2$ | $A^{n+m}B^2$ | $A^{n+m+1}B$ | $A^{n+m+1}C$ | $A^{n+m+2}C$ | $A^{n+m+2}B$ | $A^{n+m+2}B^2$ |

### 3.4 Algèbre de Fomin-Kirillov FK(4)

Calculons la base de Gröbner, $\mathcal{B}_{FK(4)}$, de $FK(4)$.

On a $R_2(4) = \{[1,2]^2, [1,3]^2, [1,4]^2, [2,3]^2, [2,4]^2, [3,4]^2\}$,

$R_3(4) = \{[1,2][2,3] + [2,3][3,1] + [3,1][1,2] = [1,2][2,3] - [2,3][1,3] - [1,3][1,2],$
$[1,3][3,2] + [3,2][2,1] + [2,1][1,3] = -[1,3][2,3] + [2,3][1,2] - [1,2][1,3],$
$[1,2][2,4] + [2,4][4,1] + [4,1][1,2] = [1,2][2,4] - [2,4][1,4] - [1,4][1,2],$
$[1,4][4,2] + [4,2][2,1] + [2,1][1,4] = -[1,4][2,4] + [2,4][1,2] - [1,2][1,4],$
$[1,4][4,3] + [4,3][3,1] + [3,1][1,4] = -[1,4][3,4] + [3,4][1,3] - [1,3][1,4],$
$[1,3][3,4] + [3,4][4,1] + [4,1][1,3] = [1,3][3,4] - [3,4][1,4] - [1,4][1,3],$
$[4,2][2,3] + [2,3][3,4] + [3,4][4,2] = -[2,4][2,3] + [2,3][3,4] - [3,4][2,4],$
$[4,3][3,2] + [3,2][2,4] + [2,4][4,3] = [3,4][2,3] - [2,3][2,4] - [2,4][3,4]\}$,

et $R_4(4) = \{[1,2][3,4] - [3,4][1,2],\ [1,3][2,4] - [2,4][1,3],\ [1,4][2,3] - [2,3][1,4]\}$.

Pour faciliter l'écriture, on pose $[1,2] = a$, $[1,3] = b$, $[1,4] = c$, $[2,3] = d$, $[2,4] = e$, $[3,4] = f$ et on introduit l'ordre suivant sur les lettres :

$$\boxed{a < b < c < d < e < f.}$$

## ***Début de l'algorithme.***

**Premières relations.**

$$\boxed{a^2 = 0} \tag{1}$$

$(w_1 = a^2,\ f_1 = 0)$,

$$\boxed{b^2 = 0} \tag{2}$$

$(w_2 = b^2,\ f_2 = 0)$,

$$\boxed{c^2 = 0} \tag{3}$$

$(w_3 = c^2,\ f_3 = 0)$,

$$\boxed{d^2 = 0} \tag{4}$$

$(w_4 = d^2,\ f_4 = 0)$,

$$\boxed{e^2 = 0} \tag{5}$$

$(w_5 = e^2,\ f_5 = 0)$,

$$\boxed{f^2 = 0} \tag{6}$$

$(w_6 = f^2,\ f_6 = 0)$,

$$\boxed{db = -ba + ad} \tag{7}$$

$(w_7 = db,\ f_6 = -ba + ad)$,

$$\boxed{da = ab + bd} \tag{8}$$

$(w_8 = da,\ f_8 = ab + bd)$,

$$\boxed{ec = -ca + ae} \tag{9}$$

$(w_9 = ec,\ f_9 = -ca + ae)$,

$$\boxed{ea = ac + ce} \tag{10}$$

$(w_{10} = ea,\ f_{10} = ac + ce)$,

$$\boxed{fb = bc + cf} \tag{11}$$

$(w_{11} = fb,\ f_{11} = bc + cf)$,

$$\boxed{fc = -cb + bf} \tag{12}$$

$(w_{12} = fc,\ f_{12} = -cb + bf)$,

$$\boxed{fe = -ed + df} \tag{13}$$

$(w_{13} = fe,\ f_{13} = -ed + df)$,

$$\boxed{fd = de + ef} \tag{14}$$

$(w_{14} = fd,\ f_{14} = de + ef)$,

$$\boxed{fa = af} \tag{15}$$

$(w_{15} = fa,\ f_{15} = af)$,

$$\boxed{dc = cd} \tag{16}$$

$(w_{16} = dc,\ f_{16} = cd)$,

$$\boxed{eb = be} \tag{17}$$

$(w_{17} = eb,\ f_{17} = be)$.

**Liste ambiguïtés 1.**$A_1 = \{a^3,\ b^3,\ c^3,\ d^3,\ e^3,\ f^3,\ d^2a,\ d^2b,\ d^2c,\ e^2a,\ e^2b,\ e^2c,\ f^2a,\ f^2b,\ f^2c,\ f^2d,\ f^2e,\ fa^2,\ fb^2,\ fc^2,\ fd^2,\ fda,\ fdb,\ fdc,\ fe^2,\ fea,\ feb,\ fec,\ ea^2,\ eb^2,\ ec^2,\ da^2,\ db^2,\ dc^2\}$.

**Ambiguïtés non résolubles 1.** : $B_1 = \{fb^2, fc^2, fd^2, fe^2, ea^2, ec^2, da^2, db^2\}$.

$$\begin{aligned}
S(fb^2) &= (fb - bc - cf)b - fb^2 = -bcb - cfb = -bcb - c(bc + cf) \\
&= -bcb - cbc - c^2 f = -bcb - cbc, \\
S(fc^2) &= -bcb - cbc, \\
S(fd^2) &= ede + ded, \\
S(fe^2) &= ede + ded, \\
S(ea^2) &= cac + aca, \\
S(ec^2) &= cac + aca, \\
S(da^2) &= bab + aba, \\
S(db^2) &= bab + aba.
\end{aligned}$$

**Nouvelles relations.** :

$$\boxed{ede = -ded} \tag{18}$$

$(w_{19} = ede,\ f_{19} = -ded)$,

$$\boxed{cbc = -bcb} \tag{19}$$

$(w_{18} = cbc,\ f_{18} = -bcb)$,

$$\boxed{cac = -aca} \tag{20}$$

$(w_{20} = cac,\ f_{20} = -aca)$,

$$\boxed{bab = -aba} \tag{21}$$

$(w_{21} = bab,\ f_{21} = -aba)$.

**Liste ambiguïtés 2.** $A_2 = \{cbc^2,\ fcbc,\ ecbc,\ dcbc,\ c^2bc,\ ede^2,\ edea,\ edeb,\ edec,\ e^2de,\ fede,\ cac^2,\ c^2ac,\ fcac,\ ecac,\ dcac,\ bab^2,\ b^2ab,\ fbab,\ ebab,\ dbab,\ cbcac,\ cacbc\}$.

**Ambiguïtés non résolubles 2.** : $B_2 = \{ecbc, dcbc, fcac, dcac, fbab, ebab,$

$cbcac, cacbc\}$.

$$\begin{aligned}
S(ecbc) &= (ec+ca-ae)bc - e(cbc+bcb) = cabc - aebc - ebcb\\
&= cabc - abec - becb = cabc + abca - abae + bcab - baed\\
&= cabc + abca - abae + bcab - babe\\
&= cabc + abca - abae + bcab - abae\\
&= cabc + bcab + abca,\\
S(dcac) &= cabc + bcab + abca,\\
S(fbab) &= cabc + bcab + abca,\\
S(ebab) &= cbac + bacb + acba, \quad *\\
S(dcbc) &= cbac + bacb + acba,\\
S(fcac) &= cbac + bacb + acba,\\
S(cbcac) &= cbaca + bcbac, \quad **\\
S(cacbc) &= cabcb + acabc.
\end{aligned}$$

On remarque que $*$ nous donne

$$\begin{aligned}
\underbrace{cbac}_{*}a &= (-bacb - acba)a\\
&= -bacba - acba^2\\
&= -bacba.
\end{aligned}$$

Et par $**$

$$\begin{aligned}
cbaca &= -b\underbrace{cbac}_{*}\\
&= -bacba - acba^2\\
&= -bacba.
\end{aligned}$$

Ainsi $**$ est une relation superflue car $*$ est suffisante à la retrouver. Comme on souhaite une base minimale, on ne l'ajoute donc pas aux nouvelles relations. De même, la relation $cabcb = -acabc$, donnée par $S(cacbc)$ ne nous est pas utile.

**Nouvelles relations.**

$$\boxed{cbac = -bacb - acba} \tag{22}$$

$(w_{22} = cbac,\ f_{22} = -bacb - acba)$,

$$\boxed{cabc = -bcab - abca} \tag{23}$$

$(w_{23} = cabc,\ f_{23} = -bcab - abca)$.

**Liste ambiguïtés 3.** $A_3 = \{cabc^2,\ cabcbc,\ cabcac,\ c^2abc,\ fcabc,\ ecabc,\ dcabc,\ cbcabc,\ cacabc,\ cbac^2,\ cbacbc,\ cbacac,\ c^2bac,\ fcbac,\ ecbac,\ dcbac,\ cbcbac,\ cacbac,\ cabcbac,\ cbacabc\}$.

**Ambiguïtés non résolubles 3.** : $B_3 = \{cabcac, cbcbac, cbacbc, cacbac\}$.

$$\begin{aligned}
S(cabcac) &= (cabc + bcab + abca)ac - cab(cac + aca)\\
&= bcabac + abca^2c - cabaca\\
&= bcabac - cabaca,\\
S(cbacbc) &= bcabac - cabaca,\\
S(cbcbac) &= acabac - cabacb,\\
S(cacbac) &= acabac - cabacb,\\
S(cabcbac) &= abcabac - cabacba,\\
S(cbacabc) &= bacabac - cabacab.
\end{aligned}$$

Comme précédemment, on remarque que les relations données par $S(cabcbac)$ et $S(cbacabc)$, ne sont pas nécessaires.

**Nouvelles relations.** :

$$\boxed{cabacb = acabac} \tag{24}$$

$(w_{24} = cabacb,\ f_{24} = acabac)$,

$$\boxed{cabaca = bcabac} \tag{25}$$

$(w_{25} = cabaca,\ f_{25} = bcabac)$.

**Liste ambiguïtés 4** $A_4 = \{cabaca^2,\ cabacac,\ c^2abaca,\ fcabaca,\ ecabaca,\ dcabaca,\ cabacb^2,\ cabacbc,\ cabacbab,\ cabacabc,\ cbcabaca,\ cacabaca,\ cabcabaca,\ cbacabaca,\ cabacbac,\ c^2abacb,\ fcabacb,\ ecabacb,\ dcabacb,\ cacabacb,\ cabcabacb,\ cbacabacb,\ cabacabacb\}$.

**Ambiguïtés non résolubles 4.** : $B_4 = \emptyset$.

## *Fin de l'algorithme.*

La base de Gröbner est donc donnée par

$\mathcal{B}_{FK(4)} = \big\{a^2,\ b^2,\ c^2,\ d^2,\ e^2,\ f^2,\ db + ba - ad,\ da - ab - bd,\ ec + ca - ae,$ $ea - ac - ce,\ fb - bc - cf,\ fc + cb - bf,\ fe + ed - df,\ fd - de - ef,\ fa - af,$ $dc - cd,\ eb - be,\ ede + ded,\ cbc + bcb,\ cac + aca,\ bab + aba,\ cbac + bacb + acba,$ $cabc + bcab + abca,\ cabacb - acabac,\ cabaca - bcabac\big\}$, à savoir,

$$\begin{gathered}\mathcal{B}_{FK(4)} = \Big\{[1,2]^2, [1,3]^2, [1,4]^2, [2,3]^2, [2,4]^2, [3,4]^2,\\ [1,2][2,3] - [2,3][1,3] - [1,3][1,2],\ -[1,3][2,3] + [2,3][1,2] - [1,2][1,3],\\ [1,2][2,4] - [2,4][1,4] - [1,4][1,2],\ -[1,4][2,4] + [2,4][1,2] - [1,2][1,4],\\ [3,4][1,3] - [1,4][3,4] - [1,3][1,4],\ -[3,4][1,4] + [1,3][3,4] - [1,4][1,3],\\ -[2,4][2,3] + [2,3][3,4] - [3,4][2,4],\ [3,4][2,3] - [2,3][2,4] - [2,4][3,4],\\ [1,2][3,4] - [3,4][1,2],\ [1,3][2,4] - [2,4][1,3],\ [1,4][2,3] - [2,3][1,4],\\ [2,4][2,3][2,4] + [2,3][2,4][2,3],\ [1,4][1,3][1,4] + [1,3][1,4][1,3],\\ [1,4][1,2][1,4] + [1,2][1,4][1,2],\ [1,3][1,2][1,3] + [1,2][1,3][1,2],\\ [1,4][1,3][1,2][1,4] + [1,3][1,2][1,4][1,3] + [1,2][1,4][1,3][1,2],\\ [1,4][1,2][1,3][1,4] + [1,3][1,4][1,2][1,3] + [1,2][1,3][1,4][1,2],\\ [1,4][1,2][1,3][1,2][1,4][1,3] + [1,2][1,4][1,2][1,3][1,2][1,4],\\ [1,4][1,2][1,3][1,2][1,4][1,2] + [1,3][1,4][1,2][1,3][1,2][1,4]\Big\}.\end{gathered}$$

*Remarque* 3.2. Il est intéressant de souligner que l'ordre initial sur les lettres que nous avons choisi dans les sections 3.2, 3.3 et 3.4 a été déterminant dans l'obtention d'une base finie (voir Proposition 3.1 dans [6]). En effet, considérons $X = \{x, y\}$ et $A = T/I$, avec $I$ l'idéal engendré par $R = \{x^2 - xy\}$. On utilise toujours l'ordre delexicographique induit par un ordre sur $X$.

(1) Si $x < y$, alors $R = \{x^2 - xy\}$ est une base de Gröbner minimale, car il n'y a pas d'ambiguïtés.

(2) Si $y < x$, alors $R$ n'est pas une base de Gröbner. En fait dans ce cas, $\{xy^n x - xy^{n+1} : n \geq 0\}$ est une base de Gröbner minimale réduite de $A$.

# Références


[1] George M. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29** (1978), no. 2, 178–218.

[2] Sergey Fomin and Anatol N. Kirillov, *Quadratic algebras, Dunkl elements, and Schubert calculus*, Advances in geometry, Progr. Math., vol. 172, Birkhäuser Boston, Boston, MA, 1999, pp. 147–182.

[3] A. N. Kirillov, *On some quadratic algebras*, L. D. Faddeev's Seminar on Mathematical Physics, Amer. Math. Soc. Transl. Ser. 2, vol. 201, Amer. Math. Soc., Providence, RI, 2000, pp. 91–113.

[4] Anatol N. Kirillov, *On some quadratic algebras I $\frac{1}{2}$ : combinatorics of Dunkl and Gaudin elements, Schubert, Grothendieck, Fuss-Catalan, universal Tutte and reduced polynomials*, SIGMA Symmetry Integrability Geom. Methods Appl. **12** (2016), Paper No. 002, 172.

[5] V. S. Varadarajan, *Supersymmetry for mathematicians : an introduction*, Courant Lecture Notes in Mathematics, vol. 11, New York University, Courant Institute of Mathematical Sciences, New York ; American Mathematical Society, Providence, RI, 2004.

[6] Ed Green, Teo Mora, and Victor Ufnarovski, *The non-commutative Gröbner freaks*, Symbolic rewriting techniques (Ascona, 1995), Progr. Comput. Sci. Appl. Logic, vol. 15, Birkhäuser, Basel, 1998, pp. 93–104.