Transfert algébrique et représentation modulaire du groupe linéaire

Trần Ngọc Nam *

8 octobre 2003

Dédié aux Professeurs Frédéric Phạm et Huỳnh Mùi à l'occasion respectivement de leur soixante-cinquième et soixantième anniversaires

Résumé

On se propose
- de déterminer la dimension d'une représentation du groupe linéaire définie par un sous-espace vectoriel de l'algèbre à puissances divisées,
- d'expliciter l'image du transfert algébrique en degré générique et celle du transfert algébrique quadruple,
- d'identifier les indécomposables de degré pair de l'algèbre polynomiale à 4 variables, vue comme module sur l'algèbre de Steenrod mod 2.

Table des matières

*L'auteur bénificie d'une bourse BDI 2002 du CNRS.

1 Introduction

Soit $\mathcal{P} := \mathbb{F}_2[x_1, \ldots, x_k]$ l'algèbre polynomiale graduée à k variables sur le corps à deux éléments $\mathbb{F}_2$, chacune de degré 1. En tant que cohomologie modulo 2 du classifiant $B(\mathbb{Z}/2)^k \simeq (\mathbb{R}P^\infty)^k$, l'algèbre $\mathcal{P}$ est dotée d'une structure naturelle d'algèbre instable sur $\mathcal{A}$, l'algèbre de Steenrod mod 2.

Soient $\bar{\mathcal{A}} \subset \mathcal{A}$ l'idéal de l'augmentation et $\bar{\mathcal{A}}\mathcal{P} \subset \mathcal{P}$ le sous-espace vectoriel engendré par les éléments θP avec $\theta \in \bar{\mathcal{A}}$ et $P \in \mathcal{P}$. Le problème qui constitue le point de départ de notre recherche consiste à expliciter une base de l'espace vectoriel gradué $\mathcal{P}_{\mathcal{A}} := \mathcal{P}/\bar{\mathcal{A}}\mathcal{P}$. Que ce problème ait des liens étroits avec l'algèbre homologique, le cobordisme, la théorie de représentation, l'étude des espaces de lacets infinis et la théorie d'invariants a été bien expliqué à travers les travaux de Singer [49], Peterson [44], Wood [56], Lannes–Zarati [21, 22, 23], Hung [16] et Hung–Nam [18]. Ceci dit, nous en avons résolu dans [40] une bonne partie par la découverte d'une base de $\mathcal{P}_{\mathcal{A}}$ dans les degrés dits génériques. Cet article fait suite à ce travail. Nous nous proposons d'étudier

- $\mathcal{P}_{\mathcal{A}}$ et son dual comme représentation du groupe $\mathcal{GL} := \mathcal{GL}_k$ des matrices $k \times k$ inversibles à coefficients dans $\mathbb{F}_2$,
- le transfert algébrique Tr_k, autrement dit le dual du morphisme Tr_k^* : $Tor_k^{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) \longrightarrow Tor_0^{\mathcal{A}}(\mathbb{F}_2, \mathcal{P})^{\mathcal{GL}} \cong (\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$ défini par Singer [49].

Le transfert algébrique Tr_k est induit "au niveau E_2" par le transfert homotopique $\pi_*^S(B(\mathbb{Z}/2)_+^k) \longrightarrow \pi_*^S(S^0)$ [4, 12, 29, 37, 45]. Une analyse de son comportement apportera sans doute des informations importantes à la théorie de l'homotopie, comme l'ont montré les travaux de Minami [34, 36]. La nécessité d'une telle analyse contribuera, nous l'espérons, à justifier la raison d'être de nos présents travaux.

Fixons d'abord quelques notations. Tous les espaces vectoriels rencontrés dans l'article ont $\mathbb{F}_2$ pour le corps de base. Sauf indication explicite, tous les produits tensoriels ont $\mathbb{F}_2$ pour l'anneau de base. Un espace vectoriel gradué V étant donné, V^d ou V_d désigne sa composante de degré d. Un ensemble B

étant donné, $\mathbb{F}_2\langle B\rangle$ signifie l'espace vectoriel ayant B pour base. Si B est un sous-ensemble d'un $\mathcal{GL}$-module, $\mathcal{GL}\langle B\rangle$ est le sous-$\mathcal{GL}$-module engendré par B de celui-ci. Enfin, le crochet $\langle *, *\rangle$ désigne l'accouplement canonique entre un espace vectoriel (gradué ou non) et son dual.

Avec ces préliminaires, voici le panorama de nos résultats :

1.1 Dimension d'une sous-représentation

Soit Γ l'espace vectoriel gradué dual de $\mathcal{P}$. Chaque composante Γ_d est un $\mathcal{GL}$-module à droite. Notons $a_1^{(i_1)}\cdots a_k^{(i_k)} \in \Gamma$ l'élément dual de $x_1^{i_1}\cdots x_k^{i_k}$ par rapport à la base monomiale usuelle de $\mathcal{P}$. Soit Ω l'ensemble des suites d'entiers

$$\omega = (r, k_0, k_1, \ldots, k_r, k_{r+1}, m_1, \ldots, m_r, m_{r+1})$$

vérifiant $0 < r \leq k$, $0 = k_0 < k_1 < \cdots < k_r \leq k_{r+1} = k$ et $m_1 > \cdots > m_r > m_{r+1} = 0$. À chaque $\omega \in \Omega$ nous associons l'élément

$$a_\omega := \prod_{i=1}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}$$

de degré $\deg a_\omega = (k_1 - k_0)(2^{m_1}-1) + \cdots + (k_r - k_{r-1})(2^{m_r}-1)$, et le groupe

$$G_\omega := \begin{pmatrix} \mathcal{GL}_{k_1-k_0} & & 0 \\ & \ddots & \\ * & & \mathcal{GL}_{k_{r+1}-k_r} \end{pmatrix}.$$

Le problème qui nous intéresse consiste à déterminer la structure du sous-$\mathcal{GL}$-module $\mathcal{GL}\langle a_\omega\rangle \subset \Gamma_{\deg a_\omega}$ et, en particulier, sa dimension en tant qu'espace vectoriel. L'intérêt de ce problème provient de ce que $\mathcal{GL}\langle a_\omega\rangle$ constitue une bonne approximation de l'espace vectoriel dual $(\mathcal{P}_{\mathcal{A}}^{\deg a_\omega})^*$, l'approximation qui est exacte dans le cas "générique" (cf. la Section 1.2). L'information que nous obtenons sur $\mathcal{GL}\langle a_\omega\rangle$ et sa dimension est la clef de nos Théorèmes 1.2, 1.3 et 1.4(ii).

Étant un sous-groupe parabolique [52] de $\mathcal{GL}$, le groupe G_ω est d'indice

$$|\mathcal{GL}/G_\omega| = \prod_{i=1}^{k}(2^i - 1) \;/\; \prod_{i=1}^{r+1} \prod_{j=1}^{k_i - k_{i-1}} (2^j - 1)$$

et coïncide avec le stabilisateur de a_ω pour l'action du groupe $\mathcal{GL}$. Le morphisme naturel $\mathbb{F}_2\langle \mathcal{GL}/G_\omega\rangle \longrightarrow \mathcal{GL}\langle a_\omega\rangle$, $G_\omega g \longmapsto a_\omega g$ est un épimorphisme de $\mathcal{GL}$-modules à droite. En tant que tel, ce morphisme a été étudié par Crabb–Hubbuck [9] qui ont démontré son injectivité sous l'hypothèse $k_1 = 1, \ldots, k_r = r$, $2^{m_1 - m_2} > k, \ldots, 2^{m_r - m_{r+1}} > k - r + 1$. Ceci étant, notre théorème est une généralisation du leur, que nous avons eu l'occasion d'énoncer dans [40].

Soit $\mathcal{W}^\perp \subset \Gamma$ le sous-espace vectoriel gradué engendré par les éléments $a_1^{(i_1)}\cdots a_k^{(i_k)}$ avec $\prod_{j=1}^{k} i_j$ impair.

Théorème 1.1 *Soit $\omega = (r, k_0, \ldots, k_{r+1}, m_1, \ldots, m_{r+1}) \in \Omega$. Pour tout $1 \leq i \leq r$, notons* $G_\omega^i := \begin{pmatrix} \mathcal{GL}_{k_1-k_0} & & & 0 \\ & \ddots & & \\ & & \mathcal{GL}_{k_i-k_{i-1}} & \\ * & & & \mathcal{GL}_{k-k_i} \end{pmatrix}$.

(i) *Supposons* $m_1 - m_2 = 1$. *Posons*

$$\widetilde{a}_\omega := \prod_{j=1}^{k_1} a_j^{(2^{m_2}-1)} \cdot \prod_{i=2}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}.$$

Alors

$$\begin{aligned} \dim \mathcal{GL}\langle a_\omega\rangle &\geq \binom{k_2}{k_1} \dim \mathcal{GL}\langle \widetilde{a}_\omega\rangle, \\ \dim \mathcal{GL}\langle a_\omega\rangle / \mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp &\geq \binom{k_2}{k_1} \dim \mathcal{GL}\langle \widetilde{a}_\omega\rangle / \mathcal{GL}\langle \widetilde{a}_\omega\rangle \cap \mathcal{W}^\perp. \end{aligned}$$

(ii) *Supposons qu'il existe* $1 \leq s \leq r$ *tel que* $m_i - m_{i+1} \geq k_{i+1} - k_{i-1}$ *pour tout* $1 \leq i < s$ *et que*
– *soit* $m_s - m_{s+1} \geq k - k_{s-1}$,
– *soit* $m_s - m_{s+1} = k - k_{s-1} - 1$ *et* $k > k_{s+1}$.
Notons $\widetilde{W}^\perp \subset \Gamma$ *le sous-espace vectoriel gradué engendré par les éléments* $a_{k_s+1}^{(i_{k_s+1})} \cdots a_k^{(i_k)}$ *avec* $\prod_{j=k_s+1}^{k} i_j$ *impair,* $\widetilde{\mathcal{GL}} := \mathcal{GL}_{k-k_s}$ *et*

$$\widetilde{a}_\omega := \prod_{i=s+1}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}.$$

Alors

$$\begin{aligned} \dim \mathcal{GL}\langle a_\omega\rangle &= |\mathcal{GL}/G_\omega^s| \dim \widetilde{\mathcal{GL}}\langle \widetilde{a}_\omega\rangle, \\ \dim \mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp &= |\mathcal{GL}/G_\omega^s| \dim \widetilde{\mathcal{GL}}\langle \widetilde{a}_\omega\rangle \cap \widetilde{\mathcal{W}}^\perp. \end{aligned}$$

En particulier, si $m_i - m_{i+1} \geq k_{i+1} - k_{i-1}$ *pour* $1 \leq i \leq r$, *alors l'épimorphisme naturel* $\mathbb{F}_2\langle \mathcal{GL}/G_\omega\rangle \longrightarrow \mathcal{GL}\langle a_\omega\rangle$ *est un isomorphisme, et l'on a*

$$\mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp = \begin{cases} 0 & si \quad k_r < k, \\ \mathcal{GL}\langle a_\omega\rangle & si \quad k_r = k. \end{cases}$$

1.2 Transfert algébrique en degré générique

Soit Γ l'espace vectoriel gradué mentionné dans la section précédente. Γ étant un $\mathcal{A}$-module à droite, on note $\Gamma^{\mathcal{A}}$ son sous-espace vectoriel gradué invariant sous l'action de l'opération de Steenrod totale $Sq = \sum_{r\geq 0} Sq^r$. Chaque composante $\Gamma_d^{\mathcal{A}}$ est un $\mathcal{GL}$-module à droite. Ceci dit, le transfert algébrique

$$Tr_k : (\Gamma^{\mathcal{A}})_{\mathcal{GL}} = \bigoplus_{d\geq 0} (\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow H^k(\mathcal{A})$$

est défini sur les $\mathcal{GL}$-coinvariants de $\Gamma^{\mathcal{A}}$ et prend sa valeur dans le k-ième groupe de cohomologie de l'algèbre de Steenrod. C'est un morphisme d'espaces vectoriels gradués avec les composantes

$$Tr_k : (\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow H^{k,d+k} := Ext_{\mathcal{A}}^{k,d+k}(\mathbb{F}_2, \mathbb{F}_2).$$

Notons $\widetilde{\mathcal{P}} := \mathbb{F}_2[x_1, \ldots, x_{k-1}] \subset \mathcal{P}$ et $\widetilde{\mathcal{P}}_{\mathcal{A}} := \mathbb{F}_2 \otimes_{\mathcal{A}} \widetilde{\mathcal{P}}$. Pour tout entier $N > 0$, notons $\alpha(N)$ le nombre d'occurrences du chiffre 1 dans son écriture binaire.

Étant donnés des entiers $m, n, d, \widetilde{d} \geq 0$ avec $d = 2^{m+n}(\widetilde{d}+k-1)+2^n-k$, le résultat principal de notre article [40] est le suivant : $\dim \mathcal{P}^d_{\mathcal{A}} = (2^k-1)\dim \widetilde{\mathcal{P}}^{\widetilde{d}}_{\mathcal{A}}$ si $m \geq k$ et soit $\alpha(\widetilde{d}+k-1) = k-1$, soit $n = 0$ et $\alpha(\widetilde{d}+k-2) \geq k-2$. Afin d'étudier en degré générique (au sens de [40]) le transfert *algébrique* qui concerne $\Gamma^{\mathcal{A}}$ plutôt que $\mathcal{P}_{\mathcal{A}}$ (qui est le dual de $\Gamma^{\mathcal{A}}$), il est nécessaire d'avoir une version duale de ce résultat.

L'espace vectoriel gradué dual $\widetilde{\Gamma} := \widetilde{\mathcal{P}}^*$ s'identifie au sous-espace vectoriel gradué de Γ engendré par les monômes $a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})}$ avec $i_1, \ldots, i_{k-1} \geq 0$. Soit $\widetilde{\mathcal{GL}} := \begin{pmatrix} \mathcal{GL}_{k-1} & 0 \\ 0 & 1 \end{pmatrix}$. Les espaces vectoriels gradués $\widetilde{\Gamma}$ et $\widetilde{\Gamma}^{\mathcal{A}} := \widetilde{\Gamma} \cap \Gamma^{\mathcal{A}}$ sont des $\widetilde{\mathcal{GL}}$-modules à droite. En désignant par $\iota^* : \Gamma^{\mathcal{A}} \longrightarrow (\Gamma^{\mathcal{A}})_{\mathcal{GL}}$ et $\widetilde{\iota}^* : \widetilde{\Gamma}^{\mathcal{A}} \longrightarrow (\widetilde{\Gamma}^{\mathcal{A}})_{\widetilde{\mathcal{GL}}}$ les projections canoniques, l'inclusion $\widetilde{\Gamma}^{\mathcal{A}} \longrightarrow \Gamma^{\mathcal{A}}$ induit [49] un morphisme $\varphi : (\widetilde{\Gamma}^{\mathcal{A}})_{\widetilde{\mathcal{GL}}} \longrightarrow (\Gamma^{\mathcal{A}})_{\mathcal{GL}}$ qui rend commutatif le diagramme

$$\begin{array}{ccc} \widetilde{\Gamma}^{\mathcal{A}} & \longrightarrow & \Gamma^{\mathcal{A}} \\ \downarrow{\scriptstyle \widetilde{\iota}^*} & & \downarrow{\scriptstyle \iota^*} \\ (\widetilde{\Gamma}^{\mathcal{A}})_{\widetilde{\mathcal{GL}}} & \xrightarrow{\varphi} & (\Gamma^{\mathcal{A}})_{\mathcal{GL}} \end{array}$$

Notons $Sq^0 : \Gamma^{\mathcal{A}} \longrightarrow \Gamma^{\mathcal{A}}$ la restriction à $\Gamma^{\mathcal{A}}$ du morphisme linéaire $\Gamma \longrightarrow \Gamma$ défini [3, 8] par $a_1^{(i_1)} \cdots a_k^{(i_k)} \longmapsto a_1^{(2i_1+1)} \cdots a_k^{(2i_k+1)}$. Le morphisme Sq^0 se factorise par les $\mathcal{GL}$-coinvariants et induit un morphisme $Sq^0 : (\Gamma^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow (\Gamma^{\mathcal{A}})_{\mathcal{GL}}$. Il existe des analogues $\widetilde{\Gamma}^{\mathcal{A}} \longrightarrow \widetilde{\Gamma}^{\mathcal{A}}$ et $(\widetilde{\Gamma}^{\mathcal{A}})_{\widetilde{\mathcal{GL}}} \longrightarrow (\widetilde{\Gamma}^{\mathcal{A}})_{\widetilde{\mathcal{GL}}}$ qu'il est d'usage de noter également Sq^0.

Soient $Sq^0 : H^{s,t} \longrightarrow H^{s,2t}$ l'opération de Steenrod classique [25, 41], et h_i la multiplication par l'élément $h_i \in H^{1,2^i}$ dans l'anneau de cohomologie $H^*(\mathcal{A})$.

Théorème 1.2 *Soit $d = 2^{m+n}(\widetilde{d}+k-1)+2^n-k$ avec $m+n \geq n \geq 0$ et $\widetilde{d} \geq 0$. Posons $d' := 2^m(\widetilde{d}+k-1)-k+1$.*

(i) *On a $\dim \Gamma^{\mathcal{A}}_{d'} \geq \dim \mathcal{GL}\langle \widetilde{\Gamma}^{\mathcal{A}}_{d'} \rangle \geq (\binom{k}{1}+\cdots+\binom{k}{m}) \dim \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}$, les égalités ayant lieu si $m \geq k$ et $\alpha(\widetilde{d}+k-2) \geq k-2$.*

(ii) *On a le diagramme commutatif*

$$\begin{array}{ccccccc} (\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}})_{\widetilde{\mathcal{GL}}} & \xrightarrow{(Sq^0)^m} & (\widetilde{\Gamma}^{\mathcal{A}}_{d'})_{\widetilde{\mathcal{GL}}} & \xrightarrow{\varphi} & (\Gamma^{\mathcal{A}}_{d'})_{\mathcal{GL}} & \xrightarrow{(Sq^0)^n} & (\Gamma^{\mathcal{A}}_{d})_{\mathcal{GL}} \\ \downarrow{\scriptstyle Tr_{k-1}} & & \downarrow{\scriptstyle Tr_{k-1}} & & \downarrow{\scriptstyle Tr_k} & & \downarrow{\scriptstyle Tr_k} \\ H^{k-1,\widetilde{d}+k-1} & \xrightarrow{(Sq^0)^m} & H^{k-1,d'+k-1} & \xrightarrow{h_0} & H^{k,d'+k} & \xrightarrow{(Sq^0)^n} & H^{k,d+k} \end{array}$$

Dans la première ligne :
- *$(Sq^0)^m$ est bijectif si $\alpha(\widetilde{d}+k-2) \geq k-2$,*
- *$(Sq^0)^n$ est bijectif si $n = 0$ ou $\alpha(\widetilde{d}+k-1) \geq k-1$,*
- *φ est surjectif si $m \geq k$ et $\alpha(\widetilde{d}+k-2) \geq k-2$.*

Dans la deuxième ligne : $(Sq^0)^n h_0 (Sq^0)^m = h_n (Sq^0)^{m+n}$. D'où

$$(\operatorname{Im} Tr_k)^d = h_n (Sq^0)^{m+n} \big((\operatorname{Im} Tr_{k-1})^{\widetilde{d}} \big)$$

si $m \geq k$ et soit $\alpha(\widetilde{d}+k-1) = k-1$, soit $n = 0$ et $\alpha(\widetilde{d}+k-2) \geq k-2$.

(iii) *Supposons que* $d = 2^{m_1} + \cdots + 2^{m_k} - k$ *et que* $m_{i-1} - m_i \geq i$ *pour* $2 < i \leq k$, $m_1 - m_2 \geq 1$ *si* $k > 1$. *Alors* $(\operatorname{Im} Tr_k)^d$, *la composante de degré* d *de* $\operatorname{Im} Tr_k$, *est le sous-espace vectoriel de* $Ext^{k,k+d}(\mathbb{F}_2, \mathbb{F}_2)$ *engendré par* $h_{m_1} \cdots h_{m_k}$. *De plus* $\Gamma^{\mathcal{A}}_d = \mathcal{GL}\langle a_1^{(2^{m_1}-1)} \cdots a_k^{(2^{m_k}-1)} \rangle$ *et*

$$(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = \begin{cases} \mathbb{F}_2 & si \quad k = 1 \quad ou \quad m_1 - m_2 \geq 2, \\ 0 & si \quad k > 1 \quad et \quad m_1 - m_2 = 1. \end{cases}$$

1.3 Indécomposables de degré pair

L'intérêt pour l'étude de $\mathcal{P}_{\mathcal{A}}$, initiée par Singer [47] en 1980, a été amplifié par Peterson [43] en 1986. C'est dans [43] que Peterson a déterminé $\mathcal{P}_{\mathcal{A}}$ pour $k = 1, 2$ et formulé sa célèbre conjecture sur la $\mathcal{A}$-décomposabilité en général, qui devait être démontrée par Wood [55] quelques années plus tard. $\mathcal{P}_{\mathcal{A}}$ pour $k = 3$ est compliqué et a été exhibé par Kameko dans sa thèse [19] à l'Université Johns Hopkins en 1990. Presqu'en même temps et indépendamment, $\Gamma^{\mathcal{A}}$ pour $k = 3$ a été explicité par Alghamdi–Crabb–Hubbuck [3] à l'Université d'Aberdeen. Probablement à cause des difficultés techniques, les raffinements du théorème de Wood mis à part, aucune tentative d'aller plus loin dans cette direction n'a été enregistrée pendant les dix ans qui suivent. Ce n'est que très récemment (2002) qu'un calcul effectif de $\mathcal{P}_{\mathcal{A}}$ en degré $d = 2^{p+3} + 2^{p+2} - 4$ pour $k = 4$ a été réalisé par Bruner–Hà–Hung [8]. Au moment d'écrire ces lignes, nous avons appris que Kameko est en train de rédiger ses résultats complets [20] sur $\mathcal{P}_{\mathcal{A}}$ pour $k = 4$. En attendant, en vue de déterminer l'image du transfert algébrique quadruple, nous identifions $\mathcal{P}_{\mathcal{A}}$ en degré *pair* pour $k = 4$.

Précisons un peu. Étant donné un entier pair quelconque $d \geq 4$, il existe une formule qui exprime $\mathcal{P}^d_{\mathcal{A}}$ en termes de $\mathcal{P}^{d/2-2}_{\mathcal{A}}$ et un certain espace vectoriel $(\operatorname{Ker}\psi)^d$. Ce que nous faisons, c'est d'expliciter une base de ce dernier. Ceci permet de connaître $\mathcal{P}_{\mathcal{A}}$ en tout degré pair moyennant sa connaissance dans les degrés impairs inférieurs.

Les détails de nos arguments sont les suivants. Soient $\pi : \mathcal{P} \longrightarrow \mathcal{P}_{\mathcal{A}}$ la projection canonique et $\psi : \mathcal{P}_{\mathcal{A}} \longrightarrow \mathcal{P}_{\mathcal{A}}$ l'épimorphisme défini [19] par

$$\pi(P) \longmapsto \begin{cases} \pi(Q) & \text{si } P = x_1 \cdots x_k Q^2,\ Q \in \mathcal{P}, \\ 0 & \text{sinon.} \end{cases}$$

Le morphisme dual ψ^*, noté Sq^0 selon l'usage, est la restriction à $\Gamma^{\mathcal{A}}$ du monomorphisme $\Gamma \longrightarrow \Gamma$, $a_1^{(i_1)} \cdots a_k^{(i_k)} \longmapsto a_1^{(2i_1+1)} \cdots a_k^{(2i_k+1)}$. En identifiant $\operatorname{Coker} Sq^0$ à un sous-espace vectoriel de $\Gamma^{\mathcal{A}}$, on obtient les formules récursives

$$\begin{array}{lll} \mathcal{P}^d_{\mathcal{A}} \cong \mathcal{P}^{(d-k)/2}_{\mathcal{A}} \oplus (\operatorname{Ker}\psi)^d & \text{si } d \equiv k \pmod 2, \\ \Gamma^{\mathcal{A}}_d = Sq^0(\Gamma^{\mathcal{A}}_{(d-k)/2}) \oplus (\operatorname{Coker} Sq^0)_d & \text{si } d \equiv k \pmod 2, \\ \mathcal{P}^d_{\mathcal{A}} = (\operatorname{Ker}\psi)^d,\ \Gamma^{\mathcal{A}}_d = (\operatorname{Coker} Sq^0)_d & \text{si } d \not\equiv k \pmod 2. \end{array}$$

Notre théorème détermine $\dim(\operatorname{Ker}\psi)^d$ pour $k = 4$ et d pair > 22. Le cas $d \leq 22$ sera traité dans la Section 6.

Théorème 1.3 *Soient* $k = 4$ *et* $d \geq 0$ *un entier pair.*

(i) *Si* $\alpha(d+2) > 2$, *alors* $(\operatorname{Ker}\psi)^d = (\operatorname{Coker} Sq^0)_d = 0$.

(ii) *Supposons que* $d = 2^{p+q} + 2^p - 2 > 22$ *avec* $p \geq 1$ *et* $q \geq 0$. *Alors*

$$\dim(\mathrm{Ker}\,\psi)^d = \begin{cases} 35 & si \quad p \geq 4 \quad et \quad q = 0, \\ 70 & si \quad p \geq 4 \quad et \quad q = 1, \\ 105 & si \quad p \geq 3 \quad et \quad q \geq 2, \\ 90 & si \quad p = 2 \quad et \quad q \geq 3, \\ 45 & si \quad p = 1 \quad et \quad q \geq 4, \end{cases}$$

$$\Gamma^{\mathcal{A}}_d = \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)} \rangle + Sq^0(\Gamma^{\mathcal{A}}_{d/2-2}),$$

$$(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = \begin{cases} Sq^0(\Gamma^{\mathcal{A}}_{d/2-2})_{\mathcal{GL}} \ si\ p \leq 2 \ ou\ q = 1, \\ \mathbb{F}_2\,\langle \iota^*(a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}) \rangle \oplus Sq^0(\Gamma^{\mathcal{A}}_{d/2-2})_{\mathcal{GL}} \ sinon, \end{cases}$$

où $\iota^* : \Gamma^{\mathcal{A}} \longrightarrow (\Gamma^{\mathcal{A}})_{\mathcal{GL}}$ *désigne la projection canonique.*

1.4 Transfert algébrique quadruple

Soit F_k la k-ième filtration d'Adams (relative à la cohomologie [2]) du groupe d'homotopie stable $\pi^S_*(S^0)$. Lannes–Zarati ont montré dans [22] l'existence d'un morphisme $F_k/F_{k+1} \longrightarrow Hom_{\mathcal{A}}(\mathcal{P}^{\mathcal{GL}}, \mathbb{F}_2)$, qu'ils notent $\mathcal{H}$ (pour Hopf). Ils ont aussi construit dans [21, 23] un morphisme $H^k(\mathcal{A}) \longrightarrow Hom_{\mathcal{A}}(\mathcal{P}^{\mathcal{GL}}, \mathbb{F}_2)$, que nous notons $\mathcal{LZ}$. Les espaces vectoriels gradués $H^k(\mathcal{A})$, F_k/F_{k+1} sont respectivement les termes E_2, E_∞ de la suite spectrale d'Adams stable du sphère S^0. On a le triangle

$$\begin{array}{ccc} F_k/F_{k+1} & & \\ \Uparrow & \searrow^{\mathcal{H}} & \\ H^k(\mathcal{A}) & \xrightarrow{\mathcal{LZ}} & Hom_{\mathcal{A}}(\mathcal{P}^{\mathcal{GL}}, \mathbb{F}_2) \end{array}$$

Lannes–Zarati [22] et Goerss [14] ont démontré que ce triangle est commutatif en un sens approprié. Hung [16] y a vu une possibilité d'attaquer une vieille conjecture qui (d'après Minami [35]) est attribuée à Curtis–Madsen [11, 27] et qui s'énonce : *le morphisme de Hurewicz* $\pi^S_*(S^0) \cong \pi_*(Q_0 S^0) \longrightarrow H_*(Q_0 S^0; \mathbb{F}_2)$ *ne détecte que les invariants de Hopf et ceux de Kervaire.* En s'appuyant sur le résultat de Lannes–Zarati et Goerss, Hung a eu l'idée de ramener la conjecture de Curtis–Madsen à ce que $\mathcal{LZ}$ *est nul en degré positif si* $k > 2$. Cette idée est incorrecte et l'erreur en a été identifiée par Kuhn (cf. [16, Erratum]). Malgré cela, l'idée de Hung s'est révélée fructueuse en ce qu'elle l'a amené à conjecturer [16] que *la composée* $\mathcal{LZ} \circ Tr_k$ *est nulle en degré positif si* $k > 2$, conjecture qui est correcte et qui a été démontrée par Hung et l'auteur [18]. C'est dans ce contexte que nous nous intéressons au transfert, particulièrement à l'image du transfert algébrique.

Soient h_i le générateur [1] de $H^{1,2^i} = \mathbb{F}_2$ et c_i celui [53] de $H^{3,11\cdot 2^i} = \mathbb{F}_2$. La composante $H^4(\mathcal{A})$ de l'algèbre de cohomologie $H^*(\mathcal{A})$ contient [32, 51] les indécomposables

$$\begin{array}{llll} d_i \in H^{4,18\cdot 2^i}, & e_i \in H^{4,21\cdot 2^i}, & f_i \in H^{4,22\cdot 2^i}, & p_i \in H^{4,37\cdot 2^i}, \\ g_{i+1} \in H^{4,24\cdot 2^i}, & D_3(i) \in H^{4,65\cdot 2^i}, & p'_i \in H^{4,73\cdot 2^i}, & \text{où } i \geq 0. \end{array}$$

Un théorème de Lin [24] confirme que ce sont les seuls indécomposables de $H^4(\mathcal{A})$. En tant qu'espace vectoriel gradué, $H^4(\mathcal{A})$ est donc engendré par ces

éléments et les décomposables de la forme $h_{i_1}h_{i_2}h_{i_3}h_{i_4}$, h_ic_j. Encore d'après Lin [24], toute relation dans $H^4(\mathcal{A})$ découle des suivantes :

$$\begin{array}{llll} h_ih_{i+1}=0, & h_{i+1}^3=h_i^2h_{i+2}, & h_ih_{i+2}^2=0, & h_i^2h_{i+3}^2=0, \\ h_ic_{i+1}=0, & h_ic_i=0, & h_{i+2}c_i=0, & h_{i+3}c_i=0, \quad \text{où } i\geq 0. \end{array}$$

Basé sur ces propriétés, notre théorème détermine l'image du transfert algébrique quadruple $Tr_4 : (\Gamma^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow H^4(\mathcal{A})$ et partiellement établit l'injectivité conjecturale [47] de ce morphisme.

Théorème 1.4 (i) *En tant qu'espace vectoriel gradué,* $\mathrm{Im}\, Tr_4$ *est engendré par les décomposables de* $H^4(\mathcal{A})$ *et les indécomposables* d_i, e_i, f_i *avec* $i \geq 0$.

(ii) *Soit* $d = 2^s(d'+4)-4$ *avec* $d' > 0$ *impair et* $s \geq 0$. *Alors* Tr_4 *est injectif en degré* d *si et seulement s'il est injectif en degré* d'. *De plus,* Tr_4 *est injectif en degré* d *dans les cas suivants :*
- $d \leq 22$,
- $\alpha(d+4) > 4$,
- $H^{4,d+4}$ *contient au moins un indécomposable,*
- $H^{4,d+4}$ *contient* h_ic_j *avec* $j \geq i+4 \geq 4$,
- $H^{4,d+4}$ *contient* $h_{i_1}h_{i_2}h_{i_3}h_{i_4}$ *avec* $i_4 > i_3 \geq i_2 \geq i_1+4 \geq 4$.

Remerciements Je tiens d'abord à remercier le Pr. John Hubbuck qui a rendu possible ma visite à l'Université d'Aberdeen en Janvier 2003. J'aimerais ensuite remercier le Dr. Gérald Gaudens et le Pr. Sadok Kallel pour leur invitation aux séminaires qu'ils organisent à l'Université de Nantes et à l'Université de Lille I. Mes remerciements vont également aux Professeurs : Michael Weiss pour les renseignements qu'il m'a donnés sur le cobordisme, Bob Bruner pour avoir vérifié mes résultats avec son logiciel pendant le Congrès de Topologie Algébrique (Barcelone, Juillet 2002), Wen Hsiung Lin pour l'envoi de [24], et Bill Singer pour l'envoi de [43, 47]. Enfin, je tiens à remercier le Dr. Masaki Kameko pour les conversations fort intéressantes que nous avons eues lors de la Conférence de Théorie d'Invariants (Göttingen, Mars 2003), et je le remercie par ailleurs de m'avoir permis de reproduire une partie de ses travaux.

2 Démonstration du Théorème 1.1

2.1 Algèbre à puissances divisées

Multiplication Soit $a_1^{(i_1)}\cdots a_k^{(i_k)}$ l'élément dual de $x_1^{i_1}\cdots x_k^{i_k}$ par rapport à la base monomiale usuelle de $\mathcal{P}$. Les éléments $a_1^{(i_1)}\cdots a_k^{(i_k)}$ avec $i_1,\ldots,i_k \geq 0$ forment une base de Γ en tant qu'espace vectoriel gradué. Γ est une algèbre commutative, et $a_1^{(i_1)}\cdots a_k^{(i_k)}$ est précisément le produit de $a_1^{(i_1)},\ldots,a_k^{(i_k)}$. La multiplication de Γ vérifie : $a_i^{(i_1)}a_i^{(i_2)} = \binom{i_1+i_2}{i_1}a_i^{(i_1+i_2)}$ pour tout $i_1, i_2 \geq 0$ et $1 \leq i \leq k$. D'où Γ s'appelle l'algèbre à puissances divisées (les éléments $a_i^{(j)}$ vérifient la même règle de multiplication que les monômes $a_i^j/j!$ de l'anneau polynomial $\mathbb{Q}[a_i]$).

Par analogie avec les polynômes, nous appelons $a_1^{(i_1)}\cdots a_k^{(i_k)}$ un monôme en $a_1,\ldots,a_k$. Le degré de a_r $(1 \leq r \leq k)$ dans ce monôme est i_r. Un polynôme en $a_1,\ldots,a_k$ est une somme de monômes distincts en $a_1,\ldots,a_k$. Le degré de a_r

dans un polynôme non nul est le plus grand degré de a_r dans les monômes dont il est la somme.

Comme dans tout espace vectoriel gradué, dans Γ un élément est homogène s'il appartient à Γ_d pour un certain entier d. Le degré d'un élément homogène γ est noté $\deg\gamma$. Si $\gamma \in \Gamma_d$, on a $\deg\gamma = d$.

Comultiplications L'algèbre polynomiale $\mathcal{P}$ est une algèbre de Hopf dont la comultiplication $\delta_{\mathcal{P}} : \mathcal{P} \longrightarrow \mathcal{P} \otimes \mathcal{P}$ est donnée par

$$\begin{cases} \delta_{\mathcal{P}}(P'P'') &= \delta_{\mathcal{P}}(P')\delta_{\mathcal{P}}(P''), \quad P' \in \mathcal{P},\ P'' \in \mathcal{P}, \\ \delta_{\mathcal{P}}(x_i) &= 1 \otimes x_i + x_i \otimes 1, \qquad\qquad 1 \leq i \leq k. \end{cases}$$

L'espace vectoriel gradué dual $\Gamma = \mathcal{P}^*$ est également une algèbre de Hopf dont la comultiplication $\delta_\Gamma : \Gamma \longrightarrow \Gamma \otimes \Gamma$ est donnée par

$$\begin{cases} \delta_\Gamma(\gamma'\gamma'') &= \delta_\Gamma(\gamma')\delta_\Gamma(\gamma''), \qquad\qquad \gamma' \in \Gamma,\ \gamma'' \in \Gamma, \\ \delta_\Gamma(a_i^{(j)}) &= \sum_{j'+j''=j} a_i^{(j')} \otimes a_i^{(j'')}, \quad 1 \leq i \leq k,\ j \geq 0. \end{cases}$$

La multiplication de Γ est induite par $\delta_{\mathcal{P}}$, celle de $\mathcal{P}$ est induite par δ_Γ. D'où

$$\begin{cases} \langle \gamma'\gamma'', P\rangle &= \langle \gamma' \otimes \gamma'', \delta_{\mathcal{P}}(P)\rangle, \quad \gamma' \in \Gamma,\ \gamma'' \in \Gamma,\ P \in \mathcal{P}, \\ \langle \gamma, P'P''\rangle &= \langle \delta_\Gamma(\gamma), P' \otimes P''\rangle, \quad \gamma \in \Gamma,\ P' \in \mathcal{P},\ P'' \in \mathcal{P}. \end{cases}$$

Autre interprétation Afin d'introduire dans la Section 2.2 l'action des matrices sur l'algèbre Γ, nous avons besoin de l'interprétation suivante de celle-ci. Soient $a_1, \ldots, a_k$ les formes linéaires $\mathbb{F}_2\langle x_1, \ldots, x_k\rangle \longrightarrow \mathbb{F}_2$ définies par $\langle a_i, x_j\rangle = \delta_{ij}$ (le symbole de Kronecker). Notons $\mathcal{V}^0 := \mathbb{F}_2$ et $\mathcal{V} := \mathbb{F}_2\langle a_1, \ldots, a_k\rangle$. Pour $n \geq 0$, le groupe symmétrique à n lettres $\mathfrak{S}_n$ agit sur $\mathcal{V}^{\otimes n} := \underbrace{\mathcal{V} \otimes \cdots \otimes \mathcal{V}}_{n}$ par permutation des facteurs. Désignons par $(\mathcal{V}^{\otimes n})^{\mathfrak{S}_n} \subset \mathcal{V}^{\otimes n}$ le sous-espace vectoriel des éléments $\mathfrak{S}_n$-invariants.

Considérons le morphisme bilinéaire $\mathcal{V}^{\otimes m} \times \mathcal{V}^{\otimes n} \longrightarrow \mathcal{V}^{\otimes(m+n)}$ qui envoie le couple $(v_1 \otimes \cdots \otimes v_m, v_{m+1} \otimes \cdots \otimes v_{m+n})$ sur

$$\sum_{\sigma \in \mathfrak{S}_{m+n}/\mathfrak{S}_m \times \mathfrak{S}_n} v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(m+n)},$$

où $\mathfrak{S}_{m+n}/\mathfrak{S}_m \times \mathfrak{S}_n$ désigne l'ensemble des permutations $\sigma \in \mathfrak{S}_{m+n}$ vérifiant $\sigma(1) < \cdots < \sigma(m)$, $\sigma(m+1) < \cdots < \sigma(m+n)$. Par restriction, puis par passage au quotient, ce morphisme induit une morphisme linéaire

$$(\mathcal{V}^{\otimes m})^{\mathfrak{S}_m} \otimes (\mathcal{V}^{\otimes n})^{\mathfrak{S}_n} \longrightarrow (\mathcal{V}^{\otimes(m+n)})^{\mathfrak{S}_{m+n}},\ u \otimes v \longmapsto u \cdot v,$$

qui munit $\Gamma(\mathcal{V}) = \Gamma(a_1, \ldots, a_k) := \bigoplus_{n \geq 0} (\mathcal{V}^{\otimes n})^{\mathfrak{S}_n}$ d'une structure de $\mathbb{F}_2$-algèbre unitaire commutative. L'application linéaire

$$\Gamma \longrightarrow \Gamma(\mathcal{V}),\ a_1^{(i_1)} \cdots a_k^{(i_k)} \longmapsto \underbrace{(a_1 \otimes \cdots \otimes a_1)}_{i_1} \cdots \underbrace{(a_k \otimes \cdots \otimes a_k)}_{i_k}$$

est un isomorphisme d'algèbres [9]. En identifiant Γ et $\Gamma(\mathcal{V})$, puis en posant $v^{(d)} := v^{\otimes d}$ pour tout $v \in \mathcal{V}$, on établit sans peine que

$$(a_{j_1} + \cdots + a_{j_s})^{(d)} = \sum_{d_1 + \cdots + d_s = d} a_{j_1}^{(d_1)} \cdots a_{j_s}^{(d_s)}$$

pour tout $d \geq 0$ et $1 \leq j_1 < \cdots < j_s \leq k$.

L'identification $\Gamma \equiv \Gamma(\mathcal{V}) = \Gamma(a_1, \ldots, a_k)$ permet de voir chaque élément $\gamma \in \Gamma$ comme une fonction $\gamma = \gamma(a_1, \ldots, a_k)$ qui dépend des variables $a_1, \ldots, a_k$. D'où l'on peut former l'expression $\gamma(v_1, \ldots, v_k)$ pour tout $v_1, \ldots, v_k \in \mathcal{V}$ en substituant respectivement $v_1, \ldots, v_k$ à la place de $a_1, \ldots, a_k$ dans l'écriture de γ. On aura l'occasion d'effectuer ces substitutions dans la Section 2.2.

L'action des matrices sur Γ rencontrée dans le lemme qui suit sera définie dans la Section 2.2.

Lemme 2.1.1 *Soient $m \geq 0$, $P \in \mathcal{P}$ et $\gamma \in \Gamma$ un polynôme en $a_1, \ldots, a_k$, non nul, homogène, ayant le degré de chaque a_i inférieur à 2^m. Supposons que $\deg \gamma \geq \deg P$. Alors, pour tout $v_1, \ldots, v_r \in \mathcal{V}$, $i_1, \ldots, i_r \geq 0$ et $Q \in \mathcal{P}$, on a*

$$\langle \gamma v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)}, PQ^{2^m} \rangle = \langle \gamma, P \rangle \cdot \langle v_1^{(i_1)} \cdots v_r^{(i_r)}, Q \rangle.$$

De plus $\langle (\gamma v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)})g, PQ^{2^m} \rangle = \langle \gamma g, P \rangle \cdot \langle (v_1^{(i_1)} \cdots v_r^{(i_r)})g, Q \rangle$ pour toute matrice carrée g d'ordre k à coefficients dans $\mathbb{F}_2$.

Démonstration D'abord

$$\langle \gamma v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)}, PQ^{2^m} \rangle = \langle \gamma \otimes v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)}, \delta_{\mathcal{P}}(PQ^{2^m}) \rangle.$$

Supposons que

$$\delta_{\mathcal{P}}(P) = P \otimes 1 + \sum_{\deg P'' > 0} P' \otimes P'', \ \delta_{\mathcal{P}}(Q) = 1 \otimes Q + \sum_{\deg Q' > 0} Q' \otimes Q''.$$

Alors

$$\begin{aligned} \delta_{\mathcal{P}}(PQ^{2^m}) &= P \otimes Q^{2^m} + \sum_{\deg P'' > 0} P' \otimes P''Q^{2^m} + \sum_{\deg Q' > 0} P(Q')^{2^m} \otimes (Q'')^{2^m} \\ &\quad + \sum_{\deg P'' > 0,\ \deg Q' > 0} P'(Q')^{2^m} \otimes P''(Q'')^{2^m}. \end{aligned}$$

Par hypothèse sur le degré $\langle \gamma, P(Q')^{2^m} \rangle = \langle \gamma, P'(Q')^{2^m} \rangle = \langle \gamma, P' \rangle = 0$. D'où

$$\begin{aligned} \langle \gamma \otimes v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)}, \delta_{\mathcal{P}}(PQ^{2^m}) \rangle &= \langle \gamma \otimes v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)}, P \otimes Q^{2^m} \rangle \\ &= \langle \gamma, P \rangle \cdot \langle v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)}, Q^{2^m} \rangle. \end{aligned}$$

Pour toute suite d'entiers positifs ou nuls $J = (j_1, \ldots, j_r)$, posons $2J := (2j_1, \ldots, 2j_r)$ et $v^J := v_1^{(j_1)} \cdots v_r^{(j_r)}$. Observons que $\langle v^{2J}, R^2 \rangle = \langle v^J, R \rangle$ pour tout $R \in \mathcal{P}$ et toute suite J. En effet, δ_Γ étant $\mathcal{M}$-équivariante (cf. le Lemme 2.2.1), il est facile de voir que $\delta_\Gamma(v^{2J}) = \sum_{J'+J''=2J} v^{J'} \otimes v^{J''}$. D'où

$$\langle v^{2J}, R^2 \rangle = \langle \delta_\Gamma(v^{2J}), R \otimes R \rangle = \sum_{J'+J''=2J} \langle v^{J'}, R \rangle \cdot \langle v^{J''}, R \rangle = \langle v^J, R \rangle^2 = \langle v^J, R \rangle.$$

Posons $I := (i_1, \ldots, i_r)$. La première partie du Lemme 2.1.1 résulte de ce que $\langle v^{2^m I}, Q^{2^m} \rangle = \cdots = \langle v^I, Q \rangle$. Pour montrer la seconde partie, il suffit de savoir que

$$\begin{aligned} (\gamma v_1^{(2^m i_1)} \cdots v_r^{(2^m i_r)})g &= (\gamma g)(v_1 g)^{(2^m i_1)} \cdots (v_r g)^{(2^m i_r)}, \\ (v_1^{(i_1)} \cdots v_r^{(i_r)})g &= (v_1 g)^{(i_1)} \cdots (v_r g)^{(i_r)}, \end{aligned}$$

et que le degré de chaque variable $a_1, \ldots, a_k$ dans γg est inférieur à 2^m. Ceci résulte facilement de la formule

$$(a_{j_1} + \cdots + a_{j_s})^{(d)} = \sum_{d_1+\cdots+d_s=d} a_{j_1}^{(d_1)} \cdots a_{j_s}^{(d_s)}$$

qui se vérifie pour tout $1 \leq j_1 < \cdots < j_s \leq k$, $d \geq 0$, et du fait que l'ensemble des polynômes en $a_1, \ldots, a_k$ ayant le degré de chaque variable a_i inférieur à 2^m forme une sous-algèbre de Γ (cela parce que tout carré de Γ est nul). □

Soit $\mathcal{W} \subset \mathcal{P}$ le sous-espace vectoriel gradué engendré par les monômes $x_1^{i_1} \cdots x_k^{i_k}$ avec $\prod_{j=1}^k i_j$ pair. Notons $\mathcal{W}^* \subset \Gamma$ le sous-espace vectoriel gradué engendré par les monômes $a_1^{(i_1)} \cdots a_k^{(i_k)}$ avec $\prod_{j=1}^k i_j$ pair. L'accouplement canonique entre $\mathcal{P}$ et Γ permet d'identifier $\mathcal{W}^*$ au dual de $\mathcal{W}$. Rappelons que $\mathcal{W}^\perp \subset \Gamma$ désigne le sous-espace vectoriel gradué engendré par les monômes $a_1^{(i_1)} \cdots a_k^{(i_k)}$ avec $\prod_{j=1}^k i_j$ impair.

Lemme 2.1.2 *Soient $d > 0$, $m \geq 0$ et $\gamma_1, \ldots, \gamma_N \in \Gamma_d$. Supposons que les classes modulo $\mathcal{W}^\perp$ de $\gamma_1, \ldots \gamma_N$ sont linéairement indépendantes dans $\Gamma/\mathcal{W}^\perp$. Alors il existe $P_1, \ldots, P_N \in \mathcal{W}^d$ vérifiant*

$$\langle \gamma_i, P_j \rangle = \delta_{ij} := \begin{cases} 1 & si\ 1 \leq i = j \leq N, \\ 0 & si\ 1 \leq i \neq j \leq N. \end{cases}$$

Démonstration L'espace vectoriel gradué Γ se décompose en $\Gamma = \mathcal{W}^\perp \oplus \mathcal{W}^*$. Soient $\bar{\gamma}_1, \ldots, \bar{\gamma}_N$ les images de $\gamma_1, \ldots, \gamma_N$ (respectivement) par la projection canonique $\Gamma \longrightarrow \mathcal{W}^*$. Par hypothèse, les éléments $\bar{\gamma}_1, \ldots, \bar{\gamma}_N$ sont linéairement indépendants dans $\mathcal{W}_d^*$. Comme les espaces vectoriels $\mathcal{W}_d^*$ et $\mathcal{W}^d$ sont en dualité, il existe $P_1, \ldots, P_N \in \mathcal{W}^d$ tels que $\langle \bar{\gamma}_i, P_j \rangle = \delta_{ij}$ pour tout $1 \leq i, j \leq N$. En observant $\gamma_i - \bar{\gamma}_i \in \mathcal{W}^\perp$, il suit que $\langle \gamma_i - \bar{\gamma}_i, P_j \rangle = 0$, d'où $\langle \gamma_i, P_j \rangle = \langle \bar{\gamma}_i, P_j \rangle = \delta_{ij}$ pour tout $1 \leq i, j \leq N$. □

2.2 Action du semigroupe des matrices

Soit $\mathcal{M}$ le semigroupe multiplicatif des matrices $k \times k$ à coefficients dans $\mathbb{F}_2$. L'action naturelle à gauche de $\mathcal{M}$ sur $\mathcal{P}$ est définie [38] par la formule

$$(gP)(x_1, \ldots, x_k) := P\big((x_1, \ldots, x_k)g\big),\ P \in \mathcal{P},\ g \in \mathcal{M},$$

où $(x_1, \ldots, x_k)g$ est le produit matriciel de g et $(x_1, \ldots, x_k)$, ce dernier vu comme une matrice ligne $(1 \times k)$. En particulier, $(gx_1, \ldots, gx_k) = (x_1, \ldots, x_k)g$ en tant que matrices lignes, $g(x_1^{i_1} \cdots x_k^{i_k}) = (gx_1)^{i_1} \cdots (gx_k)^{i_k}$ pour tout $i_1, \ldots i_k \geq 0$ et $g(\sum P) = \sum gP$ pour toute somme $\sum P$ dans $\mathcal{P}$.

Par transposition, l'action à droite de $\mathcal{M}$ sur Γ est définie par la formule

$$(\gamma g)(a_1, \ldots, a_k) := \gamma\big((a_1, \ldots, a_k)g^T\big),\ \gamma \in \Gamma,\ g \in \mathcal{M},$$

où g^T est le transposé de g. On observera que $(a_1 g, \ldots, a_k g) = (a_1, \ldots, a_k)g^T$ en tant que matrices lignes, $(a_1^{(i_1)} \cdots a_k^{(i_k)})g = (a_1 g)^{(i_1)} \cdots (a_k g)^{(i_k)}$ pour tout $i_1, \ldots i_k \geq 0$ et $(\sum \gamma)g = \sum \gamma g$ pour toute somme $\sum \gamma$ dans Γ.

L'action de $\mathcal{M}$ sur $\mathcal{P} \otimes \mathcal{P}$ et sur $\Gamma \otimes \Gamma$ est définie respectivement par

$$\begin{cases} g(P' \otimes P'') := gP' \otimes gP'', & g \in \mathcal{M},\ P' \in \mathcal{P},\ P'' \in \mathcal{P}, \\ (\gamma' \otimes \gamma'')g := \gamma' g \otimes \gamma'' g, & g \in \mathcal{M},\ \gamma' \in \Gamma, \gamma'' \in \Gamma. \end{cases}$$

Lemme 2.2.1 (i) *La multiplication, la comultiplication de $\mathcal{P}$ et celles de Γ sont $\mathcal{M}$-équivariantes.*
(ii) $\langle \gamma g, P\rangle = \langle \gamma, gP\rangle$ *pour tout* $\gamma \in \Gamma$, $g \in \mathcal{M}$, $P \in \mathcal{P}$.

Démonstration Lionel Schwartz nous a communiqué la démonstration conceptuelle suivante. L'espace vectoriel $\mathbb{F}_2\langle x_1, \ldots, x_k\rangle$ s'identifie au dual $\mathcal{V}^*$ de l'espace vectoriel $\mathcal{V} = \mathbb{F}_2\langle a_1, \ldots, a_k\rangle$ défini dans la Section 2.1. Pour $n \geq 0$, le groupe symmétrique $\mathfrak{S}_n$ opère sur $(\mathcal{V}^*)^{\otimes n}$ par permutation des facteurs. L'algèbre $\mathcal{P}$ s'identifie à l'algèbre symmétrique $S(\mathcal{V}^*) := \bigoplus_{n\geq 0}(\mathcal{V}^*)^{\otimes n}_{\mathfrak{S}_n}$ formée des coinvariants pour l'action des groupes symmétriques. En identifiant $\mathcal{GL}$ au groupe des applications linéaires inversibles $\mathcal{GL}(\mathcal{V}^*)$, ce groupe opère de manière naturelle à gauche sur $S(\mathcal{V}^*) \equiv \mathcal{P}$. Par transposition, $\mathcal{GL}(\mathcal{V}^*)$ opère à droite sur $\mathcal{V}$ et donc à droite sur $\Gamma(\mathcal{V}) \equiv \Gamma$. En examinant de près, on s'aperçoit que cette action de $\mathcal{GL} \equiv \mathcal{GL}(\mathcal{V}^*)$ sur $\mathcal{P}$ et sur Γ est donnée par les formules citées plus haut. Cela démontre le lemme. □

Soit Ω l'ensemble mentionné dans la Section 1.1. Ses éléments sont des suites d'entiers $\omega = (r, k_0, \ldots, k_{r+1}, m_1, \ldots, m_{r+1})$ ayant $0 < r < k$, $0 = k_0 < \cdots < k_r \leq k_{r+1} = k$ et $m_1 > \cdots > m_{r+1} = 0$. À chaque $\omega \in \Omega$ sont associés le monôme $a_\omega = \prod_{i=1}^{k}\prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}$ et le groupe

$$G_\omega = \begin{pmatrix} \mathcal{GL}_{k_1-k_0} & & 0 \\ & \ddots & \\ * & & \mathcal{GL}_{k_{r+1}-k_r} \end{pmatrix}.$$

Lemme 2.2.2 *Soient $\omega = (r, k_0, \ldots, k_{r+1}, m_1, \ldots, m_{r+1}) \in \Omega$, $g \in \mathcal{M}$, $m > 0$ et $0 < s < k$. Alors*
(i) $(a_1^{(2^m-1)} \cdots a_k^{(2^m-1)})g = \begin{cases} a_1^{(2^m-1)} \cdots a_k^{(2^m-1)} & \text{si } g \in \mathcal{GL}, \\ 0 & \text{si } g \notin \mathcal{GL}. \end{cases}$
(ii) $\langle (a_1 \cdots a_s)g, x_1 \cdots x_s\rangle = 1$ *si et seulement si* $g \in \begin{pmatrix} \mathcal{GL}_s & * \\ * & * \end{pmatrix}$. *Par conséquent* $(a_1 \cdots a_s)g = a_1 \cdots a_s$ *si et seulement si* $g \in \begin{pmatrix} \mathcal{GL}_s & 0 \\ * & * \end{pmatrix}$. *Le stabilisateur de $a_1 \cdots a_s$ pour l'action du groupe $\mathcal{GL}$ est* $\begin{pmatrix} \mathcal{GL}_s & 0 \\ * & \mathcal{GL}_{k-s} \end{pmatrix}$.
(iii) $a_\omega g = a_\omega$ *si et seulement si* $(a_1 \cdots a_{k_i})g = a_1 \cdots a_{k_i}$ *pour tout* $1 \leq i \leq r$. *Par conséquent, G_ω est le stabilisateur de a_ω pour l'action du groupe $\mathcal{GL}$.*

Démonstration (i) Soit $g = (g_{i,j})_{i,j=1}^k$ avec $g_{i,j} \in \mathbb{F}_2$. Désignons par $\det g$ le déterminant de la matrice g. Posons $\gamma_m := a_1^{(2^m-1)} \cdots a_k^{(2^m-1)}$. Montrons $\gamma_m g = \det g \cdot \gamma_m$ par récurrence sur m. Si $m = 1$, on a

$$\begin{aligned} \gamma_1 g &= (a_1 g) \cdots (a_k g) = \prod_{i=1}^{k} (g_{1,i}a_1 + \cdots + g_{k,i}a_k) \\ &= \sum_{1 \leq i_1 \neq \cdots \neq i_k \leq k} g_{i_1,1} \cdots g_{i_k,k} \cdot a_1 \cdots a_k = \det g \cdot a_1 \cdots a_k = \det g \cdot \gamma_1. \end{aligned}$$

Supposons $m > 1$ et $\gamma_{m-1} = \det g \cdot \gamma_{m-1}$. On a

$$\begin{aligned}\gamma_m g &= \gamma_{m-1} g \cdot (a_1 g)^{(2^{m-1})} \cdots (a_k g)^{(2^{m-1})} \\ &= \det g \cdot \gamma_{m-1} \prod_{i=1}^{k} (g_{1,i} a_1 + \cdots + g_{k,i} a_k)^{(2^{m-1})} \\ &= \det g \cdot \gamma_{m-1} \prod_{i=1}^{k} \Big(\sum_{j_1+\cdots+j_k=2^{m-1}} g_{1,i}^{j_1} \cdots g_{k,i}^{j_k} a_1^{(j_1)} \cdots a_k^{(j_k)} \Big).\end{aligned}$$

Il est facile de voir que $\gamma_{m-1} a_t^{(j_t)} = 0$ si $1 \le t \le k$ et $0 < j_t < 2^{m-1}$. D'où

$$\begin{aligned}\gamma_m g &= \det g \cdot \gamma_{m-1} \prod_{i=1}^{k} (g_{1,i} a_1^{(2^{m-1})} + \cdots + g_{k,i} a_k^{(2^{m-1})}) \\ &= \det g \cdot \gamma_{m-1} \sum_{1 \le i_1 \ne \cdots \ne i_k \le k} g_{i_1,1} \cdots g_{i_k,k} \cdot a_1^{(2^{m-1})} \cdots a_k^{(2^{m-1})} = \det g \cdot \gamma_m.\end{aligned}$$

(ii) Soit $g = (g_{i,j})_{i,j=1}^{k}$ avec $g_{i,j} \in \mathbb{F}_2$. Posons $\bar{g} := (g_{i,j})_{i,j=1}^{s}$. On a

$$\begin{aligned}(a_1 \cdots a_s) g &= (a_1 g) \cdots (a_s g) = \prod_{i=1}^{s} (g_{1,i} a_1 + \cdots + g_{k,i} a_k) \\ &= \sum_{1 \le i_1 \ne \cdots \ne i_s \le s} g_{i_1,1} \cdots g_{i_s,s} \cdot a_1 \cdots a_k + a_{s+1} u_{s+1} + \cdots + a_k u_k \\ &= \deg \bar{g} \cdot a_1 \cdots a_s + a_{s+1} u_{s+1} + \cdots + a_k u_k\end{aligned}$$

pour certains $u_{k+1}, \ldots, u_k \in \Gamma$. D'où $\langle (a_1 \cdots a_s) g, x_1 \cdots x_s \rangle = 1$ si et seulement si $\bar{g} \in \mathcal{GL}_s$, c'est-à-dire si et seulement si $g \in \begin{pmatrix} \mathcal{GL}_s & * \\ * & * \end{pmatrix}$.

Supposons $(a_1 \cdots a_s) g = a_1 \cdots a_s$. Par ce qui précède $\bar{g} \in \mathcal{GL}_s$. Notons que $(a_1 \cdots a_s) \begin{pmatrix} \bar{g}^{-1} & 0 \\ 0 & \mathbb{I}_{k-s} \end{pmatrix} = (a_1 \cdots a_s) \bar{g}^{-1} = a_1 \cdots a_s$ d'après le Lemme 2.2.2(i). Posant $\begin{pmatrix} \bar{g}^{-1} & 0 \\ 0 & \mathbb{I}_{k-s} \end{pmatrix} g = \begin{pmatrix} \mathbb{I}_s & \widetilde{g} \\ * & * \end{pmatrix}$ avec $\widetilde{g} = (\widetilde{g}_{i,j})_{1 \le i \le s < j \le k}$, on a

$$\begin{aligned}a_1 \cdots a_s &= (a_1 \cdots a_s) g = (a_1 \cdots a_s) \begin{pmatrix} \bar{g}^{-1} & 0 \\ 0 & \mathbb{I}_{k-s} \end{pmatrix} g \\ &= (a_1 \cdots a_s) \begin{pmatrix} \mathbb{I}_s & \widetilde{g} \\ * & * \end{pmatrix} = \prod_{i=1}^{s} (a_i + \widetilde{g}_{i,s+1} a_{s+1} + \cdots + \widetilde{g}_{i,k} a_k).\end{aligned}$$

En développant ce produit, on voit apparaître le monôme $\widetilde{g}_{i,s+q} a_{s+q} \prod_{1 \le j \ne i \le s} a_j$ pour tout $1 \le i \le s < s+q \le k$. Il s'ensuit que $\widetilde{g}_{i,s+q} = 0$ et que

$$g = \begin{pmatrix} \bar{g} & 0 \\ 0 & \mathbb{I}_{k-s} \end{pmatrix} \begin{pmatrix} \mathbb{I}_s & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} \bar{g} & 0 \\ * & * \end{pmatrix} \in \begin{pmatrix} \mathcal{GL}_s & 0 \\ * & * \end{pmatrix}.$$

Inversement, si $g = \begin{pmatrix} \bar{g} & 0 \\ * & * \end{pmatrix} \in \begin{pmatrix} \mathcal{GL}_s & 0 \\ * & * \end{pmatrix}$, alors d'après le Lemme 2.2.2(i) on a $(a_1 \cdots a_s) g = (a_1 \cdots a_s) \bar{g} = a_1 \cdots a_s$.

Finalement, si $g \in \mathcal{GL}$, il résulte clairement de ce qui précède que g est le stabilisateur de $a_1 \cdots a_s$ si et seulement si

$$g \in \mathcal{GL} \cap \begin{pmatrix} \mathcal{GL}_s & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} \mathcal{GL}_s & 0 \\ * & \mathcal{GL}_{k-s} \end{pmatrix}.$$

(iii) Supposons $a_\omega g = a_\omega$. Soient $P_0, \ldots, P_{m_1-1} \in \mathcal{P}$ des polynômes homogènes vérifiant $\deg P_j = k_i$ si $m_{i+1} \leq j < m_i$ et $1 \leq i \leq r$. Posons

$$f(P_0, \ldots, P_{m_1-1}) := \prod_{i=1}^{r} \prod_{j=m_{i+1}}^{m_i-1} P_j^{2^j}.$$

Puisque

$$a_\omega = \prod_{i=1}^{r} \prod_{j=m_{i+1}}^{m_i-1} a_1^{(2^j)} \cdots a_{k_i}^{(2^j)},$$

d'après le Lemme 2.1.1 on a

$$\langle a_\omega g, f(P_0, \ldots, P_{m_1-1}) \rangle = \prod_{i=1}^{r} \prod_{j=m_{i+1}}^{m_i-1} \langle (a_1 \cdots a_{k_i}) g, P_j \rangle.$$

Il suit que

$$\prod_{i=1}^{r} \prod_{j=m_{i+1}}^{m_i-1} \langle (a_1 \cdots a_{k_i}) g, P_j \rangle = \prod_{i=1}^{r} \prod_{j=m_{i+1}}^{m_i-1} \langle a_1 \cdots a_{k_i}, P_j \rangle.$$

Pour $1 \leq i \leq r$ et $m_{i+1} \leq j < m_i$, en choisissant $P_j := x_1 \cdots x_{k_i} + Q_j$ avec Q_j étant un monôme quelconque de degré k_i et différent de $x_1 \cdots x_{k_i}$, de sorte que $\langle a_1 \cdots a_{k_i}, P_j \rangle = 1$, on obtient $\langle (a_1 \cdots a_{k_i}) g, P_j \rangle = 1$. Les Q_j étant quelconques, ceci implique que $(a_1 \cdots a_{k_i}) g = a_1 \cdots a_{k_i}$ pour tout $1 \leq i \leq r$.

Supposons $(a_1 \cdots a_{k_i}) g = a_1 \cdots a_{k_i}$ pour tout $1 \leq i \leq r$. Montrons $a_\omega g = a_\omega$ par récurrence sur r. Si $r = 1$, ceci est vrai à cause du Lemme 2.2.2(i). Supposons $r > 1$ et qu'il est vrai pour toute valeur inférieure de r. D'abord, d'après le Lemme 2.2.2(ii) on a $g \in \begin{pmatrix} g_1 & 0 \\ * & \widetilde{g} \end{pmatrix}$ pour certains $g_1 \in \mathcal{GL}_{k_1}$ et $\widetilde{g} \in \mathcal{GL}_{k-k_1}$ vérifiant $(a_{k_1+1} \cdots a_{k_i}) g = a_{k_1+1} \cdots a_{k_i}$ pour tout $1 < i \leq r$. Posant $\widetilde{a}_\omega := \prod_{i=2}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}$, on a

$$a_\omega g = (\widetilde{a}_\omega \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}) g = \widetilde{a}_\omega g \cdot (\prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}) g_1 = \widetilde{a}_\omega g \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}$$

d'après le lemme 2.2.2(i). Il est facile de vérifier que $\widetilde{a}_\omega g = \widetilde{a}_\omega \widetilde{g} + \sum_{i,\ell} u_{i\ell} a_i^{(\ell)}$ pour certains $u_{i\ell} \in \Gamma$, où $1 \leq i \leq k_1$ et $1 \leq \ell < 2^{m_2}$. D'où

$$\begin{aligned} a_\omega g &= \widetilde{a}_\omega \widetilde{g} \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)} + \sum_{i\ell} u_{i\ell} a_i^{(\ell)} \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)} \\ &= \widetilde{a}_\omega \widetilde{g} \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)} = \widetilde{a}_\omega \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)} = a_\omega, \end{aligned}$$

car $\widetilde{a}_\omega \widetilde{g} = \widetilde{a}_\omega$ par hypothèse de récurrence. □

Lemme 2.2.3 *Soient $1 \leq i_1 < \cdots < i_r \leq k$ des entiers. Alors il existe $g \in \mathcal{GL}$ tel que*

$$(a_1 \cdots a_{k-1})g = \sum_{j=1}^{r} \prod_{1 \leq i \neq i_j \leq k} a_i.$$

Démonstration Le lemme est démontré en observant

- que $\{(a_1 \cdots a_{k-1})g \mid g \in \mathcal{GL}\} \cong \mathcal{GL}/G_0$, où $G_0 := \begin{pmatrix} \mathcal{GL}_{k-1} & 0 \\ * & 1 \end{pmatrix}$ est le stabilisateur de $a_1 \cdots a_{k-1}$ pour l'action du groupe $\mathcal{GL}$,
- que $\{(a_1 \cdots a_{k-1})g \mid g \in \mathcal{GL}\}$ est inclu dans l'ensemble des expressions

$$\prod_{1 \leq i \neq i_1 \leq k} a_i + \cdots + \prod_{1 \leq i \neq i_r \leq k} a_i$$

  avec $1 \leq i_1 < \cdots < i_r \leq k$,
- que $|\mathcal{GL}/G_0| = 2^k - 1$ est égal au nombre de suites d'entiers $(i_1, \ldots, i_r)$ vérifiant $1 \leq i_1 < \cdots < i_r \leq k$.

□

Le lemme suivant sera utile pour la démonstration des Théorèmes 1.1(i) et 1.3(ii).

Lemme 2.2.4 *Soit m un entier positif.*

(i) *On a* $\dim \mathcal{GL}\langle a_1^{(2^m-1)} \rangle = \binom{k}{1} + \cdots + \binom{k}{2^m-1}$ *et*

$$\dim \mathcal{GL}\langle a_1^{(2^m-1)} \rangle \cap \mathcal{W}^\perp = \begin{cases} 1 & \text{si} \quad 2^m - 1 = k, \\ 0 & \text{sinon.} \end{cases}$$

(ii) *Supposons $k > 1$. Alors* $\dim \mathcal{GL}\langle a_1^{(2^m-1)} \cdots a_{k-1}^{(2^m-1)} \rangle = \binom{k}{1} + \cdots + \binom{k}{m}$ *et*

$$\mathcal{GL}\langle a_1^{(2^m-1)} \cdots a_{k-1}^{(2^m-1)} \rangle \cap \mathcal{W}^\perp = 0.$$

Démonstration (i) Pour tout sous-ensemble $I = \{i_1 < \cdots < i_r\}$ de $\{1, \ldots, k\}$ vérifiant $r \leq 2^m - 1$, notons

$$x_I := \begin{cases} x_{i_1}^{2^m - r} x_{i_2} x_{i_3} \cdots x_{i_r} & \text{si} \quad 2^m - 1 \leq k, \\ x_{i_1}^{2^m - r - 1} x_{i_2}^2 x_{i_3} \cdots x_{i_r} & \text{si} \quad 2^m - 1 > k. \end{cases}$$

En utilisant la formule

$$(a_{i_1} + \cdots + a_{i_r})^{(2^m-1)} = \sum_{m_1 + \cdots + m_r = 2^m - 1} a_{i_1}^{(m_1)} \cdots a_{i_r}^{(m_r)},$$

il est facile de vérifier que $\langle (a_{i_1} + \cdots + a_{i_r})^{(2^m-1)}, x_J \rangle = \delta_{IJ}$ pour tous sous-ensembles $I = \{i_1 < \cdots < i_r\}$, $J = \{j_1 < \cdots < j_s\}$ de $\{1, \ldots, k\}$ vérifiant $r, s \leq 2^m - 1$. Il s'ensuit que le dual de l'espace vectoriel $\mathcal{GL}\langle a_1^{(2^m-1)} \rangle$ s'identifie à $\bigoplus_I \mathbb{F}_2 \langle x_I \rangle$. D'où $\mathcal{GL}\langle a_1^{(2^m-1)} \rangle \cap \mathcal{W}^\perp = 0$ si $2^m - 1 \neq k$, et $\dim \mathcal{GL}\langle a_1^{(2^m-1)} \rangle = \binom{k}{1} + \cdots + \binom{k}{2^m-1}$.

Supposons $2^m - 1 = k$. Puisque $\langle (a_{i_1} + \cdots + a_{i_r})^{(k)}, x_1 \cdots x_k \rangle = 0$ si $r < k$, on a $\dim \mathcal{GL}\langle a_1^{(k)} \rangle \cap \mathcal{W}^\perp \leq 1$. Pour montrer que l'égalité a lieu dans ce cas, il suffit de vérifier que

$$\sum_{(m_1, \ldots, m_r)} a_{i_1}^{(m_1)} \cdots a_{i_r}^{(m_r)} \in \mathcal{GL}\langle a_1^{(k)} \rangle$$

pour tout $1 \leq i_1 < \cdots < i_r \leq k$, où $(m_1, \ldots, m_r)$ parcourt l'ensemble des suites d'entiers positifs de somme $m_1 + \cdots + m_r = k$. Montrons ceci par récurrence sur r. Il n'y a rien à faire si $r = 1$. Supposons $r > 1$ et que cette propriété est vérifiée pour toute valeur inférieure de r. On a

$$(a_{i_1} + \cdots + a_{i_r})^{(k)} = \sum_{(j_1,\ldots,j_s)} \sum_{(m_1,\ldots,m_s)} a_{j_1}^{(m_1)} \cdots a_{j_s}^{(m_s)},$$

où la première somme est prise sur l'ensemble des sous-suites de $(i_1, \ldots, i_r)$, la seconde est prise sur l'ensemble des suites d'entiers positifs $(m_1, \ldots, m_s)$ vérifiant $m_1 + \cdots + m_s = k$. Par hypothèse de récurrence

$$\sum_{(m_1,\ldots,m_s)} a_{j_1}^{(m_1)} \cdots a_{j_s}^{(m_s)} \in \mathcal{GL}\langle a_1^{(k)} \rangle$$

pour toute sous-suite propre $(j_1, \ldots, j_s) \subsetneq (i_1, \ldots, i_r)$. Il suit donc que

$$\sum_{(m_1,\ldots,m_r)} a_{i_1}^{(m_1)} \cdots a_{i_r}^{(m_r)} \in \mathcal{GL}\langle a_1^{(k)} \rangle.$$

(ii) Pour toute suite d'entiers $I = (i_1, \ldots, i_r)$ vérifiant $1 \leq r \leq m$ et $1 \leq i_1 < \cdots < i_r \leq k$, notons

$$P_I := \prod_{t=0}^{r} (x_1 \cdots x_k / x_{i_t})^{2^t} \cdot \prod_{r<t\leq m} (x_1 \cdots x_k / x_{i_r})^{2^t}.$$

Soit $g_I \in \mathcal{GL}$ une matrice (dont l'existence est assurée par le Lemme 2.2.3) satisfaisant à

$$(a_1 \cdots a_{k-1}) g_I = \prod_{1\leq i\neq i_1\leq k} a_i + \cdots + \prod_{1\leq i\neq i_r\leq k} a_i.$$

Soient $I = (i_1, \ldots, i_r)$, $J = (j_1, \ldots, j_s)$ des suites entiers vérifiant $1 \leq r, s \leq m$, $1 \leq i_1 < \cdots < i_r \leq k$ et $1 \leq j_1 < \cdots < j_s \leq k$. Notons $\gamma := a_1^{(2^m-1)} \cdots a_{k-1}^{(2^m-1)}$. Comme $\gamma = \prod_{0\leq t<m} a_1^{(2^t)} \cdots a_{k-1}^{(2^t)}$, par application itérative du Lemme 2.1.1 on a

$$\begin{aligned} \langle \gamma g_I, P^J \rangle &= \prod_{0\leq t<m} \langle (a_1 \cdots a_{k-1}) g_I, P^J_{[t]} \rangle \\ &= \prod_{t=0}^{s} \langle (a_1 \cdots a_{k-1}) g_I, x_1 \cdots x_k / x_{j_t} \rangle \cdot \prod_{s<t\leq m} \langle (a_1 \cdots a_{k-1}) g_I, x_1 \cdots x_k / x_{j_s} \rangle. \end{aligned}$$

D'où $\langle \gamma g_I, P^J \rangle \neq 0$ si et seulement si $j_t \in \{i_1, \ldots, i_r\}$ pour tout $1 \leq t \leq s$, c'est-à-dire si et seulement si J est une sous-suite de I. Observons que les éléments γg_I engendrent l'espace vectoriel $\mathcal{GL}\langle\gamma\rangle$. Il en résulte facilement que le dual de celui-ci est isomorphe à $\bigoplus_I \mathbb{F}_2 \langle P_I \rangle$. Puisque le nombre des suites I est égal à $\binom{k}{1} + \cdots + \binom{k}{m}$, le lemme suit. □

2.3 Lemmes clefs

Cette section est une préparation à la démonstration du Théorème 1.1(ii). Pour tous entiers positifs m, n, notons

- $\mathcal{M}_{m,n}$ l'ensemble des matrices $m \times n$ à coefficients dans $\mathbb{F}_2$,
- $\mathbb{O}_{m,n} = 0 \in \mathcal{M}_{m,n}$ la matrice dont tous les coefficients sont nuls,
- $\mathbb{I}_n \in \mathcal{GL}_n$ la matrice unité d'ordre n.

Pour $0 \leq p < m+n$, posons

$$A_p^{m,n} := \begin{cases} \mathbb{O}_{m,n} & \text{si} \quad p = 0, \\ \begin{pmatrix} 0 & \mathbb{I}_p \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{m,n} & \text{si} \quad 1 \leq p \leq \min(m,n), \\ \begin{pmatrix} 0 & \mathbb{I}_m & \mathbb{O}_{m,p-m} \end{pmatrix} \in \mathcal{M}_{m,n} & \text{si} \quad m < p \leq n, \\ \begin{pmatrix} \mathbb{O}_{p-n,n} \\ \mathbb{I}_n \\ 0 \end{pmatrix} \in \mathcal{M}_{m,n} & \text{si} \quad n < p \leq m, \\ \begin{pmatrix} 0 & 0 \\ \mathbb{I}_{m+n-p} & 0 \end{pmatrix} \in \mathcal{M}_{m,n} & \text{si} \quad \max(m,n) < p < m+n. \end{cases}$$

Étant donnés une matrice $X = (X_{i,j}) \in \mathcal{M}_{m,n}$ et un entier positif $p < m+n$, appelons le vecteur $(X_{i,j})_{i-j=m-p}$ la p-ième diagonale de X. Si X est une matrice carrée, notons $\det X$ son déterminant.

Lemme 2.3.1 *Soient m, n, q des entiers positifs, $q < m+n$, et $X = (X_{i,j}) \in \mathcal{M}_{n,m}$. Supposons que $\mathbb{I}_n + XA_p^{m,n} \in \mathcal{GL}_n$ pour tout $1 \leq p \leq q$. Alors les q premières diagonales de X sont nulles.*

Démonstration Soit $1 \leq p \leq q$. Il est facile de vérifier que si les $p-1$ premières diagonales de X sont toutes nulles, alors $\det(\mathbb{I}_n + XA_p^{m,n}) = \prod_{i-j=n-p}(1+X_{i,j})$. Ceci implique que la p-ième diagonale de X est nulle. D'où le lemme. □

Lemme 2.3.2 *Soit $\omega = (r, k_0, \ldots, k_{r+1}, m_1, \ldots, m_{r+1}) \in \Omega$ avec $m_1 \geq k$. Notons $i(p)$, pour $0 \leq p \leq k-2$, l'entier vérifiant $m_1 - m_{i(p)} \leq p < m_1 - m_{i(p)+1}$, et posons $i(k-1) := i(k-2)$. Pour tout $0 \leq p \leq k-1$ ayant $i(p) > 1$, soit $\tau_p \in \mathcal{M}_{k-k_1,k-k_1}$ une matrice dont les $k-p$ dernières lignes sont nulles. Pour tout $0 \leq p \leq k-1$, posons*

$$\sigma_p := \begin{cases} \begin{pmatrix} \mathbb{I}_{k_1} & 0 \\ A_p^{k-k_1,k_1} & 0 \end{pmatrix} \in \mathcal{M} & \textit{si} \quad i(p) = 1, \\ \begin{pmatrix} \mathbb{I}_{k_1} & 0 \\ A_p^{k-k_1,k_1} & \tau_p \end{pmatrix} \in \mathcal{M} & \textit{si} \quad i(p) > 1. \end{cases}$$

Supposons

- *que $P = \sum x_1^{i_1} \cdots x_k^{i_k}$ est une somme de monômes qui vérifient : $2^{m_1-k} > \max(i_1, i_k)$ si $m_1 - m_{i(k-2)+1} = k-1$,*
- *que $P = (x_1 \cdots x_{k_1})^{2^{m_1-k}-1}\widetilde{P} + R$ avec $\widetilde{P} \in \mathcal{P}$, et R étant une somme de monômes non divisibles par $(x_1 \cdots x_{k_1})^{2^{m_1-k}-1}$,*
- *que $g = \begin{pmatrix} A & * \\ * & \widetilde{g} \end{pmatrix} \in \mathcal{M}$ avec $A \in \mathcal{M}_{k_1,k_1}$ et $\widetilde{g} \in \mathcal{M}_{k-k_1,k-k_1}$.*

Posons $\widetilde{a}_\omega := \prod_{i=2}^r \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}$, $P_1 := \prod_{p=0}^{k-1} \sigma_p (x_1 \cdots x_{k_{i(p)}})^{2^{m_1-p-1}}$ et $\widetilde{P}_1 := \prod_{p=m_1-m_2}^{k-1} \tau_p (x_{k_1+1} \cdots x_{k_{i(p)}})^{2^{m_1-p-1}}$. Alors :

(i) *Si $g \in G_\omega^1$, on a $\langle a_\omega g, PP_1 \rangle = \langle \widetilde{a}_\omega \widetilde{g}, \widetilde{P}\widetilde{P}_1 \rangle$.*

(ii) *Si $g \notin G_\omega^1$, on a $\langle a_\omega g, PP_1 \rangle = 0$.*

Démonstration (i) Au cours de la démonstration du Lemme 2.2.2(iii) on a montré que $a_\omega g = \widetilde{a}_\omega \widetilde{g} \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}$. Notons que $P_1 + (x_1 \cdots x_{k_1})^{2^{m_1}-2^{m_1-k}} \widetilde{P}_1$ est une somme de monômes non divisibles par $(x_1 \cdots x_{k_1})^{2^{m_1}-1}$. D'où

$$\begin{aligned}
\langle a_\omega g, PP_1 \rangle &= \langle \widetilde{a}_\omega \widetilde{g} \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}, (x_1 \cdots x_{k_1})^{2^{m_1-k}-1} \widetilde{P} P_1 + RP_1 \rangle \\
&= \langle \widetilde{a}_\omega \widetilde{g} \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}, (x_1 \cdots x_{k_1})^{2^{m_1-k}-1} \widetilde{P} P_1 \rangle \\
&= \langle \widetilde{a}_\omega \widetilde{g} \cdot \prod_{j=1}^{k_1} a_j^{(2^{m_1}-1)}, (x_1 \cdots x_{k_1})^{2^{m_1}-1} \widetilde{P}\widetilde{P}_1 \rangle = \langle \widetilde{a}_\omega \widetilde{g}, \widetilde{P}\widetilde{P}_1 \rangle.
\end{aligned}$$

(ii) Raisonnons par l'absurde. Supposons que $Q = x_1^{i_1} \cdots x_k^{i_k}$ soit un monôme de P qui vérifie $\langle a_\omega g, QP_1 \rangle = 1$. Soit $1 \leq t \leq r$ l'entier tel que $m_1 - m_t \leq k-1 < m_1 - m_{t+1}$. Posant $Q_1 := Q\sigma_{k-1}(x_1 \cdots x_{k_t})^{2^{m_1-k}}$ et

$$\gamma_1 := \prod_{j=1}^{k_t} a_j^{(2^{m_1-k+1}-1)} \cdot \prod_{i=t+1}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)},$$

de sorte que $a_\omega = \gamma_1 \prod_{p=0}^{k-2} \prod_{j=1}^{k_{i(p)}} a_j^{(2^{m_1-p-1}-1)}$, on a

$$\begin{aligned}
1 &= \langle a_\omega g, QP_1 \rangle = \langle (\gamma_1 \prod_{p=0}^{k-2} \prod_{j=1}^{k_{i(p)}} a_j^{(2^{m_1-p-1}-1)}) g, Q_1 \prod_{p=0}^{k-2} \sigma_p (x_1 \cdots x_{k_1})^{2^{m_1-p-1}} \rangle \\
&= \langle \gamma_1 g, Q_1 \rangle \cdot \prod_{p=0}^{k-2} \langle (a_1 \cdots a_{k_{i(p)}}) g, \sigma_p (x_1 \cdots x_{k_{i(p)}}) \rangle
\end{aligned}$$

d'après le Lemme 2.1.1. Il suit que $1 = \langle \gamma_1 g, Q_1 \rangle$ et que $g\sigma_p \in \begin{pmatrix} \mathcal{GL}_{k_{i(p)}} & * \\ * & * \end{pmatrix}$ pour tout $0 \leq p \leq k-2$, ceci d'après les Lemmes 2.2.1(ii) et 2.2.2(ii). D'où l'on vérifie sans peine

- que $A \in \mathcal{GL}_{k_1}$,
- que $g_1 := \begin{pmatrix} A^{-1} & 0 \\ 0 & \mathbb{I}_{k-k_1} \end{pmatrix} g = \begin{pmatrix} \mathbb{I}_{k_1} & X \\ * & * \end{pmatrix}$ pour un certain $0 \neq X \in \mathcal{M}_{k_1, k-k_1}$,
- que $\gamma_1 g = \gamma_1 g_1$ et que $g_1 \sigma_p \in \begin{pmatrix} \mathcal{GL}_{k_{i(p)}} & * \\ * & * \end{pmatrix}$.

Montrons que les p premières diagonales de X sont nulles pour tout $0 \leq p \leq k-2$. Ceci étant vrai pour $p = 0$, on suppose $0 < p \leq k-2$ et qu'il est vrai pour toute valeur inférieure de p. Si $i(p) = 1$, on a

$$\begin{aligned}
g_1 \sigma_p &= \begin{pmatrix} \mathbb{I}_{k_1} & X \\ * & * \end{pmatrix} \begin{pmatrix} \mathbb{I}_{k_1} & 0 \\ A_p^{k-k_1,k_1} & 0 \end{pmatrix} \\
&= \begin{pmatrix} \mathbb{I}_{k_1} + X A_p^{k-k_1,k_1} & 0 \\ * & 0 \end{pmatrix} \in \begin{pmatrix} \mathcal{GL}_{k_1} & * \\ * & * \end{pmatrix}.
\end{aligned}$$

D'où $\det(\mathbb{I}_{k_1} + XA_p^{k-k_1,k_1}) = 1$, ce qui implique que la p-ième diagonale de X est nulle (cf. la démonstration du Lemme 2.3.1). Si $i(p) > 1$, on a

$$\begin{aligned} g_1\sigma_p &= \begin{pmatrix} \mathbb{I}_{k_1} & X \\ * & * \end{pmatrix} \begin{pmatrix} \mathbb{I}_{k_1} & 0 \\ A_p^{k-k_1,k_1} & \tau_p \end{pmatrix} \\ &= \begin{pmatrix} \mathbb{I}_{k_1} + XA_p^{k-k_1,k_1} & X\tau_p \\ * & * \end{pmatrix} \in \begin{pmatrix} \mathcal{GL}_{k_{i(p)}} & * \\ * & * \end{pmatrix}. \end{aligned}$$

Puisque les $p-1$ premières diagonales de X et les $k-p$ dernières lignes de τ_p sont nulles par hypothèse, on a $X\tau_p = 0$. D'où $\det(\mathbb{I}_{k_1} + XA_p^{k-k_1,k_1}) = 1$, ce qui implique que la p-ième diagonale de X est nulle (cf. la démonstration du Lemme 2.3.1).

On vient de montrer que les $k-2$ premières diagonales de X sont nulles. Comme $X \neq 0$, il suit que $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{k_1,k-k_1}$. Montrons que $m_1 - m_t = k-1$. En effet, supposant le contraire et posant

$$\gamma_2 := \prod_{j=1}^{k_t} a_j^{(2^{m_1-k}-1)} \cdot \prod_{i=t+1}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)},$$

de sorte que $\gamma_1 = \gamma_2 \prod_{j=1}^{k_t} a_j^{(2^{m_1-k})}$, on a

$$\begin{aligned} 1 &= \langle \gamma_1 g_1, Q_1 \rangle = \langle (\gamma_2 \prod_{j=1}^{k_t} a_j^{(2^{m_1-k})}) g_1, Q\sigma_{k-1}(x_1 \cdots x_{k_t})^{2^{m_1-k}} \rangle \\ &= \langle \gamma_2 g_1, Q \rangle \cdot \langle (a_1 \cdots a_{k_t}) g_1, \sigma_p(x_1 \cdots x_{k_t}) \rangle \end{aligned}$$

d'après le Lemme 2.1.1. D'où $g_1\sigma_{k-1} \in \begin{pmatrix} \mathcal{GL}_{k_t} & * \\ * & * \end{pmatrix}$ d'après les Lemmes 2.2.1(ii) et 2.2.2(ii), ce qui équivaut à $\mathbb{I}_{k_1} + XA_{k-1}^{k-k_1,k_1} \in \mathcal{GL}_{k_1}$. Ceci est impossible, car $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathcal{M}_{k_1,k-k_1}$ et $A_{k-1}^{k-k_1,k_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_{k-k_1,k_1}$.

On a montré que $m_1 - m_t = k-1$. Il s'ensuit facilement que $t = i(k-2)+1$. D'où $\max(i_1, i_k) < 2^{m_t-1}$ par hypothèse. Posant

$$\gamma_2 := \prod_{j=2}^{k_t} a_j^{(2^{m_t}-1)} \cdot \prod_{i=t+1}^{r} \prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)},$$

de sorte que $\gamma_1 = \gamma_2 a_1^{(2^{m_t}-1)}$, on a

$$\begin{aligned} 1 &= \langle \gamma_1 g_1, Q_1 \rangle = \langle (\gamma_2 a_1^{(2^{m_t}-1)}) g_1, Q\sigma_{k-1}(x_1 \cdots x_{k_t})^{2^{m_t-1}} \rangle \\ &= \langle \gamma_2 g_1 \cdot (a_1 + a_k)^{(2^{m_t}-1)}, Q(x_2 \cdots x_{k_t})^{2^{m_t-1}} (x_1 + x_k)^{2^{m_t-1}} \rangle. \end{aligned}$$

En extrayant la partie qui ne concerne que les variables a_1, a_k, x_1, x_k, on obtient

$$1 = \langle a_1^{(j_1)} a_k^{(j_k)} (a_1 + a_k)^{(2^{m_t}-1)}, x_1^{i_1} x_k^{i_k} (x_1 + x_k)^{2^{m_t-1}} \rangle$$

pour certains entiers j_1, j_k. Puisque $j_1 + j_k = i_1 + i_k - 2^{m_t-1} + 1 < 2^{m_t-1}$, en appliquant le Lemme 2.1.1 on a

$$\begin{aligned} 1 &= \langle a_1^{(j_1)} a_k^{(j_k)} (a_1 + a_k)^{(2^{m_t-1}-1)} \cdot (a_1 + a_k)^{(2^{m_t-1})}, x_1^{i_1} x_k^{i_k} (x_1 + x_k)^{2^{m_t-1}} \rangle \\ &= \langle a_1^{(j_1)} a_k^{(j_k)} (a_1 + a_k)^{(2^{m_t-1}-1)}, x_1^{i_1} x_k^{i_k} \rangle \cdot \langle a_1 + a_k, x_1 + x_k \rangle \\ &= \langle a_1^{(j_1)} a_k^{(j_k)} (a_1 + a_k)^{(2^{m_t-1}-1)}, x_1^{i_1} x_k^{i_k} \rangle \cdot 0 = 0. \end{aligned}$$

Ceci est une contradiction. □

Corollaire 2.3.3 *Soit* $\omega = (r, k_0, \dots, k_{r+1}, m_1, \dots, m_{r+1}) \in \Omega$. *Supposons qu'il existe* $1 \leq s \leq r$ *tel que* $m_i - m_{i+1} \geq k_{i+1} - k_{i-1}$ *pour tout* $1 \leq i < s$ *et que*

- *soit* $m_s - m_{s+1} \geq k - k_{s-1}$,
- *soit* $m_s - m_{s+1} = k - k_{s-1} - 1$ *et* $k > k_{s+1}$.

Notons $i(p)$, *pour* $0 \leq p \leq k-2$, *l'entier vérifiant* $m_1 - m_{i(p)} \leq p < m_1 - m_{i(p)+1}$, *et posons* $i(k-1) := i(k-2)$. *Soient* $\widetilde{P} \in \mathbb{F}_2[x_{k_s+1}, \dots, x_k]$ *un polynôme ayant le degré de* x_k *inférieur à* 2^{m_1-k}, *et* $P := (x_1 \cdots x_{k_s})^{2^{m_1-k}-1}\widetilde{P}$. *Alors il existe* $\sigma_0, \dots, \sigma_{k-1} \in \mathcal{M}$ *tels que pour tout* $g = \begin{pmatrix} * & * \\ * & \widetilde{g} \end{pmatrix} \in \mathcal{M}$ *avec* $\widetilde{g} \in \mathcal{M}_{k-k_s, k-k_s}$, *l'on ait*

$$\langle a_\omega g, P \prod_{p=0}^{k-1} \sigma_p (x_1 \cdots x_{k_{i(p)}})^{2^{m_1-p-1}} \rangle = \begin{cases} \langle \widetilde{a}_\omega \widetilde{g}, \widetilde{P} \rangle & si \quad g \in G_\omega^s, \\ 0 & si \quad g \notin G_\omega^s. \end{cases}$$

Démonstration Pour tout $0 \leq p \leq k-1$, soit $\sigma_p = (B_1 \cdots B_{i(p)}\ 0) \in \mathcal{M}$ la matrice ayant les blocs $B_i \in \mathcal{M}_{k, k_i - k_{i-1}}$ définis par

$$B_i := \begin{cases} \begin{pmatrix} \mathbb{I}_{k_1} \\ A_p^{k-k_1, k_1} \end{pmatrix} & \text{si} \qquad i = 1, \\ \begin{pmatrix} \mathbb{O}_{k_{i-1}, k_i - k_{i-1}} \\ \mathbb{I}_{k_1} \\ A_{p-m_1+m_i}^{k-k_i, k_i - k_{i-1}} \end{pmatrix} & \text{si} \quad 1 < i \leq i(p). \end{cases}$$

Pour tout $0 \leq p \leq k-1$ ayant $i(p) > 1$, soit $\tau_p = (C_2 \cdots C_{i(p)}\ 0) \in \mathcal{M}$ la matrice ayant les blocs $C_i \in \mathcal{M}_{k-k_1, k_i - k_{i-1}}$ définis par

$$C_i := \begin{cases} \begin{pmatrix} \mathbb{I}_{k_2} \\ A_{p-m_1+m_2}^{k-k_2, k_2-k_1} \end{pmatrix} & \text{si} \qquad i = 2, \\ \begin{pmatrix} \mathbb{O}_{k_{i-1}-k_1, k_i - k_{i-1}} \\ \mathbb{I}_{k_i - k_{i-1}} \\ A_{p-m_1+m_i}^{k-k_i, k_i - k_{i-1}} \end{pmatrix} & \text{si} \quad 2 < i \leq i(p). \end{cases}$$

Grâce à l'hypothèse sur les écarts entre $m_1, \dots, m_{s+1}$, on vérifie sans peine, pour tout $0 \leq p \leq k-1$ ayant $i(p) > 1$, que les $k-p$ dernières lignes de τ_p sont nulles et que $\sigma_p = \begin{pmatrix} \mathbb{I}_{k_1} & 0 \\ A_p^{k-k_1, k_1} & \tau_p \end{pmatrix}$. Le corollaire résulte alors du Lemme 2.3.2 par récurrence sur r. □

Lemme 2.3.4 *Soient* $m \geq 0$, *et* $\gamma = \sum a_1^{(i_1)} \cdots a_k^{(i_k)} \in \Gamma$ *un polynôme non nul dont les monômes vérifient :* $\max(i_1, \dots, i_k) < 2^{m+1}$ *et* $\binom{i_1}{2^m} \cdots \binom{i_k}{2^m} = 0$.

(i) *Il existe* $g \in \mathcal{GL}$ *tel que* γg *contienne au moins un monôme ayant le degré de* a_k *inférieur à* 2^m.

(ii) *Supposons* $\gamma \notin \mathcal{W}^\perp$. *Alors il existe* $g \in \mathcal{GL}$ *tel que* γg *contienne au moins un monôme qui ne soit pas dans* $\mathcal{W}^\perp$ *et dont le degré de* a_k *soit inférieur à* 2^m.

Démonstration Étant donné un polynôme $\gamma_1 \in \Gamma$, notons $i_k(\gamma_1)$ le degré de a_k dans celui-ci. Soient $g_1, \dots, g_k \in \mathcal{GL}$ les matrices définies par

$$a_j g_i := \begin{cases} a_j & \text{si} \quad 1 \leq j < k \quad \text{et} \quad 1 \leq i \leq k, \\ a_i + a_k & \text{si} \quad j = k \qquad \text{et} \quad 1 \leq i \leq k. \end{cases}$$

Il est facile de montrer
- que $i_k(\gamma+\gamma g_i) < i_k(\gamma)$ pour tout $1 \le i \le k$,
- que les monômes des polynômes $\gamma+\gamma g_i$ satisfont à l'hypothèse du lemme,
- que les $\gamma+\gamma g_i$ ne sont pas tous nuls,
- que si $\gamma \notin \mathcal{W}^\perp$, il existe $1 \le i \le k$ tel que $\gamma+\gamma g_i \notin \mathcal{W}^\perp$.

D'où le lemme se vérifie aisément par récurrence sur $i_k(\gamma)$. □

2.4 Démonstration du Théorème 1.1(i)

Soient
- $g_1, \dots, g_M \in \mathcal{GL}$ tels que les éléments $\widetilde{a}_\omega g_1, \dots, \widetilde{a}_\omega g_M$ forment une base de l'espace vectoriel $\mathcal{GL}\langle\widetilde{a}_\omega\rangle$,
- $h_1, \dots, h_N \in \mathcal{GL}$ tels que les classes modulo $\mathcal{GL}\langle\widetilde{a}_\omega\rangle \cap \mathcal{W}^\perp$ des éléments $\widetilde{a}_\omega h_1, \dots, \widetilde{a}_\omega h_N$ forment une base de l'espace vectoriel $\mathcal{GL}\langle\widetilde{a}_\omega\rangle/\mathcal{GL}\langle\widetilde{a}_\omega\rangle \cap \mathcal{W}^\perp$,
- $P_1, \dots, P_M \in \mathcal{P}^{\deg \widetilde{a}_\omega}$ tels que $\langle a_{\widetilde{\omega}} g_i, P_j\rangle = \delta_{ij}$ pour $1 \le i,j \le M$,
- $Q_1, \dots, Q_N \in \mathcal{W}^{\deg \widetilde{a}_\omega}$ (cf. le Lemme 2.1.2) tels que $\langle a_{\widetilde{\omega}} h_i, Q_j\rangle = \delta_{ij}$ pour $1 \le i,j \le N$.

Pour tout sous-ensemble $I = \{i_1 < \cdots < i_{k_1}\} \subset \{1, \dots, k_2\}$, soit $\tau_I \in \mathcal{GL}$ une matrice satisfaisant à

$$\begin{cases} (a_1\tau_I, \dots, a_{k_1}\tau_I) &= (a_{i_1}, \dots, a_{i_{k_1}}), \\ \{a_1\tau_I, \dots, a_{k_2}\tau_I\} &= \{a_1, \dots, a_{k_2}\}, \\ (a_{k_2+1}\tau_I, \dots, a_k\tau_I) &= (a_{k_2+1}, \dots, a_k). \end{cases}$$

Supposons d'abord $1 \le i,j \le M$, $I = \{i_1 < \cdots < i_{k_1}\} \subset \{1, \dots, k_2\}$ et $J = \{j_1 < \cdots < j_{k_1}\} \subset \{1, \dots, k_2\}$. Alors

$$\begin{aligned} & \langle a_\omega \tau_J g_j, P_i\big(g_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\big)^{2^{m_2}}\rangle \\ = \ & \langle (a_{\widetilde{\omega}} a_1^{(2^{m_2})} \cdots a_{k_1}^{(2^{m_2})})\tau_J g_j, P_i\big(g_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\big)^{2^{m_2}}\rangle \\ = \ & \langle a_{\widetilde{\omega}}\tau_J g_j, P_i\rangle \cdot \langle (a_1\cdots a_{k_1})\tau_J g_j, g_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\rangle \text{ d'après le Lemme 2.1.1} \\ = \ & \langle a_{\widetilde{\omega}} g_j, P_i\rangle \cdot \langle (a_{j_1}\cdots a_{j_{k_1}})g_j, g_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\rangle \\ = \ & \delta_{ij}\langle a_{j_1}\cdots a_{j_{k_1}}, g_j g_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\rangle \text{ d'après le Lemme 2.2.1(ii)} \\ = \ & \delta_{ij}\langle a_{j_1}\cdots a_{j_{k_1}}, x_{i_1}\cdots x_{i_{k_1}}\rangle = \delta_{ij}\delta_{IJ}. \end{aligned}$$

Ceci implique l'indépendance linéaire des éléments $a_\omega\tau_I g_i$. D'où

$$\dim \mathcal{GL}\langle a_\omega\rangle \ge \binom{k_2}{k_1} M = \binom{k_2}{k_1} \dim \mathcal{GL}\langle a_{\widetilde{\omega}}\rangle.$$

Supposons maintenant $1 \le i,j \le N$, $I = \{i_1 < \cdots < i_{k_1}\} \subset \{1, \dots, k_2\}$ et $J = \{j_1 < \cdots < j_{k_1}\} \subset \{1, \dots, k_2\}$. D'une manière analogue à ce qui était fait plus haut, on montre que $\langle a_\omega\tau_J h_j, Q_i\big(h_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\big)^{2^{m_2}}\rangle = \delta_{ij}\delta_{IJ}$. Puisque $Q_i\big(h_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\big)^{2^{m_2}} \in \mathcal{W}$, on a $\langle \gamma, Q_i\big(h_i^{-1}(x_{i_1}\cdots x_{i_{k_1}})\big)^{2^{m_2}}\rangle = 0$ pour tout $\gamma \in \mathcal{W}^\perp$. Il suit que les classes modulo $\mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp$ des éléments $a_\omega\tau_I h_i$ sont linéairement indépendantes dans $\mathcal{GL}\langle a_\omega\rangle/\mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp$. D'où

$$\dim \mathcal{GL}\langle a_\omega\rangle/\mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp \ge \binom{k_2}{k_1} N = \binom{k_2}{k_1} \dim \mathcal{GL}\langle\widetilde{a}_\omega\rangle/\mathcal{GL}\langle\widetilde{a}_\omega\rangle \cap \mathcal{W}^\perp.$$

2.5 Démonstration du Théorème 1.1(ii)

C'est à Crabb–Hubbuck [9, p. 150] que nous devons l'idée d'utiliser l'accouplement canonique entre Γ et $\mathcal{P}$ pour démontrer l'indépendance linéaire des éléments de $\mathcal{GL}\langle a_\omega\rangle$. Crabb–Hubbuck n'ont considéré que le cas $k_1 = 1$. Grâce à des techniques exposées dans les Sections 2.1, 2.2 et surtout 2.3, nous pouvons traiter le cas général.

Soient $\gamma := \prod_{i=1}^{s}\prod_{j=k_{i-1}+1}^{k_i} a_j^{(2^{m_i}-1)}$ et $\widetilde{\mathcal{GL}} \equiv \begin{pmatrix} \mathbb{I}_{k_s} & 0 \\ 0 & \mathcal{GL}_{k-k_s} \end{pmatrix} \subset \mathcal{GL}$. Étant donnés un sous-espace vectoriel $V \subset \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle$ et une matrice $g \in \mathcal{GL}$, notons $\gamma V g := \{(\gamma v)g \mid v \in V\}$. Il est clair que $\gamma V g$ est un sous-espace vectoriel de $\mathcal{GL}\langle a_\omega\rangle$ et $\dim \gamma V g = \dim V$. Soient $g_1, \ldots, g_M \in \mathcal{GL}$ des représentants des classes à gauche de $\mathcal{GL}/G_\omega^s$.

Supposons donnés $\gamma_1, \ldots, \gamma_M \in \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle$ avec $\gamma_1 \neq 0$. Comme $m_{s+1} - 1 \leq m_1 - k$, d'après le Lemme 2.3.4 il existe $h \in \widetilde{\mathcal{GL}}$ tel que $\gamma_1 h$ contienne au moins un monôme de la forme $a_{k_s+1}^{(i_{k_s+1})} \cdots a_k^{(i_k)}$ avec $i_k < 2^{m_1-k}$, monôme qui ne soit pas dans $\widetilde{\mathcal{W}}^\perp$ si $\gamma_1 \notin \widetilde{\mathcal{W}}^\perp$. Posons $\widetilde{P} := x_{k_s+1}^{i_{k_s+1}} \cdots x_k^{i_k}$ et $P := (x_1 \cdots x_{k_s})^{2^{m_1-k}-1}\widetilde{P}$. D'après le Corollaire 2.3.3, il existe $Q \in \mathcal{P}$ tel que pour tout $g = \begin{pmatrix} * & * \\ * & \widetilde{g} \end{pmatrix} \in \mathcal{M}$ avec $\widetilde{g} \in \mathcal{M}_{k-k_s,k-k_s}$, l'on ait

$$\langle a_\omega g, PQ^{2^{m_1-k}}\rangle = \begin{cases} \langle \widetilde{a}_\omega\widetilde{g}, \widetilde{P}\rangle & \text{si} \quad g \in G_\omega^s, \\ 0 & \text{si} \quad g \notin G_\omega^s. \end{cases}$$

Posons $\gamma_i := \sum_j \widetilde{a}_\omega h_{ij}$ avec $h_{ij} \in \widetilde{\mathcal{GL}}$, $1 \leq i \leq M$. Comme $h_{ij}g_ig_1^{-1}h \notin G_\omega^s$ si $i \neq 1$, en notant δ_{1i} le symbole de Kronecker on a

$$\begin{aligned} \langle(\gamma\gamma_i)g_ig_1^{-1}h, PQ^{2^{m_1-k}}\rangle &= \sum_j \langle(\gamma\widetilde{a}_\omega)h_{ij}g_ig_1^{-1}h, PQ^{2^{m_1-k}}\rangle \\ &= \sum_j \langle a_\omega h_{ij}g_ig_1^{-1}h, PQ^{2^{m_1-k}}\rangle = \delta_{1i}\sum_j \langle a_\omega h_{1j}h, PQ^{2^{m_1-k}}\rangle \\ &= \delta_{1i}\sum_j \langle \widetilde{a}_\omega h_{1j}h, \widetilde{P}\rangle = \delta_{1i}\langle\gamma_i h, \widetilde{P}\rangle = \delta_{1i}. \end{aligned}$$

Montrons que $\mathcal{GL}\langle a_\omega\rangle = \sum_{i=1}^{M} \gamma\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle g_i$. En effet, supposons $g \in \mathcal{GL}$ et $gg_1^{-1} \in G_\omega^s$. Alors $a_\omega gg_1^{-1} = (\gamma\widetilde{a}_\omega)gg_1^{-1} = \gamma\cdot\widetilde{a}_\omega gg_1^{-1}$ (cf. la démonstration du Lemme 2.2.2(iii)). Notons que $\widetilde{a}_\omega gg_1^{-1} \in \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle$. D'où $a_\omega g = (a_\omega gg_1^{-1})g_1 = (\gamma\cdot\widetilde{a}_\omega gg_1^{-1})g_1 \in \gamma\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle g_1$.

Montrons que $\mathcal{GL}\langle a_\omega\rangle = \bigoplus_{i=1}^{M} \gamma\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle g_i$. Supposons le contraire : il existe $\gamma_1, \ldots, \gamma_M \in \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle$ avec $\gamma_1 \neq 0$ tels que $\sum_{i=1}^{M}(\gamma\gamma_i)g_i = 0$. Par ce qui précède, il existe $h \in \widetilde{\mathcal{GL}}$, $P \in \mathcal{P}$ et $Q \in \mathcal{P}$ tels que $\langle(\gamma\gamma_i)g_ig_1^{-1}h, PQ^{2^{m_1-k}}\rangle = \delta_{1i}$ pour tout $1 \leq i \leq M$. D'où

$$0 = \langle\sum_{i=1}^{M}(\gamma\gamma_i)g_ig_1^{-1}h, PQ^{2^{m_1-k}}\rangle = \sum_{i=1}^{M}\langle(\gamma\gamma_i)g_ig_1^{-1}h, PQ^{2^{m_1-k}}\rangle = \sum_{i=1}^{M}\delta_{1i} = 1,$$

ce qui est une contradiction.

Montrons que $\mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp \supset \bigoplus_{i=1}^{M} \gamma(\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle \cap \widetilde{\mathcal{W}}^\perp)g_i$. En effet, ceci résulte de ce que $\mathcal{W}^\perp$ est stable sous l'action de $\mathcal{GL}$ (cf. le Lemme 2.2.2(i)).

Montrons que $\mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp = \bigoplus_{i=1}^M \gamma(\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle \cap \widetilde{\mathcal{W}}^\perp)g_i$. Supposons le contraire : il existe $\gamma_1, \ldots, \gamma_M \in \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle$ avec $\gamma_1 \notin \mathcal{W}^\perp$ tels que $\sum_{i=1}^M (\gamma\gamma_i)g_i \in \mathcal{W}^\perp$. Par ce qui précède $\langle(\gamma\gamma_i)g_i g_1^{-1}h, PQ^{2^{m_1}-k}\rangle = \delta_{1i}$ pour certains $h \in \widetilde{\mathcal{GL}}$, $P \in \mathcal{W}$, $Q \in \mathcal{P}$ et pour tout $1 \leq i \leq M$. D'où

$$0 = \langle\sum_{i=1}^M (\gamma\gamma_i)g_i g_1^{-1}h, PQ^{2^{m_1}-k}\rangle = \sum_{i=1}^M \langle(\gamma\gamma_i)g_i g_1^{-1}h, PQ^{2^{m_1}-k}\rangle = \sum_{i=1}^M \delta_{1i} = 1,$$

ce qui est une contradiction.

Pour résumer, on a

$$\begin{aligned}
\dim \mathcal{GL}\langle a_\omega\rangle &= \sum_{i=1}^M \dim \gamma\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle g_i = \sum_{i=1}^M \dim \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle \\
&= |\mathcal{GL}/G^s_\omega| \dim \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle, \\
\dim \mathcal{GL}\langle a_\omega\rangle \cap \mathcal{W}^\perp &= \sum_{i=1}^M \dim \gamma(\widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle \cap \widetilde{\mathcal{W}}^\perp)g_i = \sum_{i=1}^M \dim \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle \cap \widetilde{\mathcal{W}}^\perp \\
&= |\mathcal{GL}/G^s_\omega| \dim \widetilde{\mathcal{GL}}\langle\widetilde{a}_\omega\rangle \cap \widetilde{\mathcal{W}}^\perp.
\end{aligned}$$

C'est ce qu'il fallait démontrer.

3 Démonstration du Théorème 1.2

3.1 Préliminaires

Action de l'algèbre de Steenrod L'action naturelle à gauche de $\mathcal{A}$ sur $\mathcal{P}$ est définie par $Sq^q(x_i^j) = \binom{j}{q} x_i^{j+q}$. Elle vérifie la formule de Cartan [50]

$$Sq^q(PQ) = \sum_{r=0}^q Sq^r(P)Sq^{q-r}(Q),\ q \geq 0,\ P \in \mathcal{P},\ Q \in \mathcal{P}.$$

On transpose cette action en une $\mathcal{A}$-action à droite sur Γ en posant $\langle\gamma\theta, P\rangle := \langle\gamma, \theta P\rangle$, $\gamma \in \Gamma$, $\theta \in \mathcal{A}$, $P \in \mathcal{P}$. L'action à droite vérifie aussi la formule de Cartan.

Soit $\Gamma^{\mathcal{A}} \subset \Gamma$ le sous-espace vectoriel gradué engendré par les éléments $\gamma \in \Gamma$ vérifiant $\gamma\theta = 0$ pour tout $\theta \in \bar{\mathcal{A}}$. L'accouplement canonique entre Γ et $\mathcal{P}$ permet d'identifier $\Gamma^{\mathcal{A}}$ au dual de $\mathcal{P}_{\mathcal{A}}$. De plus, à cause de la formule de Cartan, $\Gamma^{\mathcal{A}}$ est une sous-algèbre de Γ. Cette sous-algèbre contient [49] le monôme $a_i^{(2^j-1)}$, donc le monôme a_ω mentionné dans la Section 1.1. On verra plus loin que $\Gamma^{\mathcal{A}}$ est un sous-$\mathcal{GL}$-module de Γ. Donc, le $\mathcal{GL}$-module $\Gamma^{\mathcal{A}}_{\deg a_\omega}$ contient $\mathcal{GL}\langle a_\omega\rangle$ comme sous-$\mathcal{GL}$-module. Dans la Section 3.4 on démontrera que $\Gamma^{\mathcal{A}}_{\deg a_\omega} = \mathcal{GL}\langle a_\omega\rangle$ dans le cas "générique". C'est en ce sens que l'espace vectoriel dual $\Gamma^{\mathcal{A}}_{\deg a_\omega} = (\mathcal{P}^{\deg a_\omega}_{\mathcal{A}})^*$ peut être approchée par $\mathcal{GL}\langle a_\omega\rangle$, qui en constitue une bonne approximation (cf. la Section 1.1).

Invariants et coinvariants Les actions de $\mathcal{A}$ et de $\mathcal{M}$ (le semigroupe des matrices $k \times k$) sur $\mathcal{P}$ commutent [56, 57]. Les espaces vectoriels gradués $\mathcal{P}_{\mathcal{A}}$

et $\Gamma^{\mathcal{A}}$ sont naturellement des $\mathcal{M}$-modules, donc des $\mathcal{GL}$-modules. La projection $\pi : \mathcal{P} \longrightarrow \mathcal{P}_{\mathcal{A}}$ est $\mathcal{M}$-linéaire.

Soit $(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}} \subset \mathcal{P}_{\mathcal{A}}$ le sous-espace vectoriel gradué engendré par les éléments $\pi(P)$ vérifiant $P \in \mathcal{P}$ et $g\pi(P) = \pi(gP) = \pi(P)$ pour tout $g \in \mathcal{GL}$. Notons $(\Gamma^{\mathcal{A}})_{\mathcal{GL}}$ le quotient de $\Gamma^{\mathcal{A}}$ par le sous-espace vectoriel gradué engendré par les éléments de la forme $\gamma g - \gamma$ avec $\gamma \in \Gamma^{\mathcal{A}}$ et $g \in \mathcal{GL}$. Les éléments de $(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$ s'appellent les $\mathcal{GL}$-invariants, ceux de $(\Gamma^{\mathcal{A}})_{\mathcal{GL}}$: les $\mathcal{GL}$-coinvariants. Les espaces vectoriels gradués $(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$ et $(\Gamma^{\mathcal{A}})_{\mathcal{GL}}$ sont en dualité.

Morphisme de Kameko Soit $\pi : \mathcal{P} \longrightarrow \mathcal{P}_{\mathcal{A}}$ la projection canonique. Un des outils dont s'est servi Kameko [19] pour une description récursive de $\mathcal{P}_{\mathcal{A}}$ est l'épimorphisme $\psi : \mathcal{P}_{\mathcal{A}}^{2d+k} \longrightarrow \mathcal{P}_{\mathcal{A}}^{d}$ défini par la formule

$$\psi(\pi(P)) = \begin{cases} \pi(Q) & \text{si} \quad P = x_1 \cdots x_k Q^2,\ Q \in \mathcal{P}^d, \\ 0 & \text{sinon.} \end{cases}$$

Le morphisme dual de ψ, noté $Sq^0 : \Gamma_d^{\mathcal{A}} \longrightarrow \Gamma_{2d+k}^{\mathcal{A}}$, est la restriction à $\Gamma^{\mathcal{A}}$ du morphisme linéaire $\Gamma_d^{\mathcal{A}} \longrightarrow \Gamma_{2d+k}^{\mathcal{A}}$, $a_1^{(i_1)} \cdots a_k^{(i_k)} \longmapsto a_1^{(2i_1+1)} \cdots a_k^{(2i_k+1)}$.

Lemme 3.1.1 *Si $\alpha(d+k-1) \geq k-1$, alors sont bijectifs les morphismes ψ, Sq^0, ainsi que les morphismes induits $\psi : (\mathcal{P}_{\mathcal{A}}^{2d+k})^{\mathcal{GL}} \longrightarrow (\mathcal{P}_{\mathcal{A}}^{d})^{\mathcal{GL}}$, $Sq^0 : (\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow (\Gamma_{2d+k}^{\mathcal{A}})_{\mathcal{GL}}$.*

Démonstration Puisque Sq^0 est le morphisme dual de ψ, il suffit de montrer le lemme pour ψ. Pour montrer l'injectivité de celui-ci, observons d'abord que $\pi(\mathcal{W}^{2d+k}) = 0$ (cf. la Section 2.1 pour $\mathcal{W}$). En effet, tout monôme de $\mathcal{W}^{2d+k}$ s'écrit sous la forme $P_0P_1^2$ pour certains $P_0, P_1 \in \mathcal{P}$ avec $\deg P_0 = k - 2r$, $r \geq 1$. Comme $\alpha(\deg(P_0P_1^2) + \deg P_0) = \alpha(d+k-r) \geq k-r > \deg P_0$ par hypothèse, on a $\pi(P_0P_1^2) = 0$ d'après un théorème de Wood [55] (rappelé dans le Théorème 4.1.1 du présent article).

Supposons que $P \in \mathcal{P}^{2d+k}$ et $\psi(\pi(P)) = 0$. Montrons que $\pi(P) = 0$. Ceci étant vrai si $P \in \mathcal{W}^{2d+k}$, on peut supposer que $P \notin \mathcal{W}^{2d+k}$, ce qui revient à dire que $P = x_1 \cdots x_k Q^2$ pour un certain $Q \in \mathcal{P}^d$. On a $\pi(Q) = \psi(\pi(P)) = 0$. Soient $Q_1, \ldots, Q_N \in \mathcal{P}^d$ des polynômes tels que $Q = Sq^1(Q_1) + \cdots + Sq^N(Q_N)$. D'après la formule de Cartan

$$\begin{aligned} P = x_1 \cdots x_k Q^2 &= \sum_{i=1}^{N} x_1 \cdots x_k Sq^{2i}(Q_i^2) \\ = \sum_{i=1}^{N} \big(Sq^{2i}(x_1 \cdots x_k Q^2) &+ \sum_{j=1}^{i} Sq^{2j}(x_1 \cdots x_k)(Sq^{2i-2j}(Q_i^2)) \big) \in \mathcal{W} + \bar{\mathcal{A}}\mathcal{P}. \end{aligned}$$

Comme $\pi(\mathcal{W} + \bar{\mathcal{A}}\mathcal{P})^{2d+k} = 0$, il suit que $\pi(P) = 0$.

La surjectivité de ψ étant claire, il reste à établir celle de la restriction $\psi : (\mathcal{P}_{\mathcal{A}}^{2d+k})^{\mathcal{GL}} \longrightarrow (\mathcal{P}_{\mathcal{A}}^{d})^{\mathcal{GL}}$. Soit $P \in \mathcal{P}^d$ un polynôme avec $\pi(P) \in (\mathcal{P}_{\mathcal{A}}^{d})^{\mathcal{GL}}$. Comme $\psi(\pi(x_1 \cdots x_k P^2)) = \pi(P)$, il suffit de montrer que $\pi(x_1 \cdots x_k P^2)$ est un $\mathcal{GL}$-invariant. Soit $g \in \mathcal{GL}$. Il est facile de voir que $g(x_1 \cdots x_k) + x_1 \cdots x_k \in W$, d'où $g(x_1 \cdots x_k)g(P)^2 + x_1 \cdots x_k g(P)^2 \in \mathcal{W}^{2d+k}$. Le fait $\pi(\mathcal{W}^{2d+k}) = 0$ implique que $g\pi(x_1 \cdots x_k P^2) = \pi(g(x_1 \cdots x_k)g(P)^2) = \pi(x_1 \cdots x_k g(P)^2)$. Comme

$$\psi(\pi(x_1 \cdots x_k g(P)^2)) = \pi(g(P)) = g\pi(P) = \pi(P) = \psi(\pi(x_1 \cdots x_k P^2))$$

par hypothèse, il suit de l'injectivité de ψ que

$$\pi(x_1 \cdots x_k g(P)^2) = \pi(x_1 \cdots x_k P^2).$$

D'où $g\pi(x_1 \cdots x_k P^2) = \pi(x_1 \cdots x_k P^2)$, ce qu'il fallait démontrer. □

3.2 Démonstration du Théorème 1.2(i)

Soient

- $\mathbb{Z}_+$ l'ensemble des entiers positifs ou nuls et $\mathbb{Z}_+^{k-1} = \overbrace{\mathbb{Z}_+ \times \cdots \times \mathbb{Z}_+}^{k-1}$,
- $E_1, \ldots, E_M \subset \mathbb{Z}_+^{k-1}$ tels que les polynômes $\sum_{(i_1,\ldots,i_{k-1})\in E_r} a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})}$ $(1 \leq r \leq M)$ forment une base de l'espace vectoriel $\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}$,
- $\gamma := a_1^{(2^m-1)} \cdots a_{k-1}^{(2^m-1)}$ et $g_1, \ldots, g_N \in \mathcal{GL}$ tels que $\gamma g_1, \ldots, \gamma g_N$ forment une base de l'espace vectoriel $\mathcal{GL}\langle\gamma\rangle$, où $N = \binom{k}{1} + \cdots + \binom{k}{m}$ d'après le Lemme 2.2.4(ii),
- $P_1, \ldots, P_N \in \mathcal{P}$ tels que $\langle ag_{s'}, P_s\rangle = \delta_{ss'}$ pour $1 \leq s, s' \leq N$,
- $Q_1, \ldots, Q_M \in \widetilde{\mathcal{P}}$ tels que $\langle \sum_{(i_1,\ldots,i_{k-1})\in E_{r'}} a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})}, Q_r\rangle = \delta_{rr'}$ pour $1 \leq r, r' \leq M$.

Montrons que les éléments $(\gamma \sum_{(i_1,\ldots,i_{k-1})\in E_r} a_1^{(2^m i_1)} \cdots a_{k-1}^{(2^m i_{k-1})})g_s$, où $1 \leq r \leq M$ et $1 \leq s \leq N$, sont linéairement indépendants dans Γ. En effet, on a

$$\begin{aligned}
&\langle(\gamma \sum_{E_{r'}} a_1^{(2^m i_1)} \cdots a_{k-1}^{(2^m i_{k-1})})g_{s'}, P_s(g_s^{-1}Q_r)^{2^m}\rangle \\
= \;& \langle\gamma g_{s'}, P_s\rangle \cdot \langle\sum_{E_{r'}} (a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})})g_{s'}, g_s^{-1}Q_r\rangle \text{ d'après le Lemme 2.1.1} \\
= \;& \delta_{ss'}\langle\sum_{E_{r'}} a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})}, g_{s'}g_s^{-1}Q_r\rangle \text{ d'après le Lemme 2.2.1(ii)} \\
= \;& \delta_{ss'}\langle\sum_{E_{r'}} a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})}, Q_r\rangle = \delta_{ss'}\delta_{rr'}.
\end{aligned}$$

Ceci donne l'indépendance linéaire voulue. De plus, du fait que

$$\gamma \sum_{E_r} a_1^{(2^m i_1)} \cdots a_{k-1}^{(2^m i_{k-1})} = (Sq^0)^m(\sum_{E_r} a_1^{(i_1)} \cdots a_{k-1}^{(i_{k-1})}) \in (Sq^0)^m(\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}) \subset \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d'}},$$

on a $(\gamma \sum_{E_r} a_1^{(2^m i_1)} \cdots a_{k-1}^{(2^m i_{k-1})})g_s \in \mathcal{GL}\langle\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d'}}\rangle \subset \Gamma^{\mathcal{A}}_{d'}$ pour tout $1 \leq r \leq M$ et $1 \leq s \leq N$. D'où $\dim \Gamma^{\mathcal{A}}_{d'} \geq \dim \mathcal{GL}\langle\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d'}}\rangle \geq MN = N \dim \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}} = (\binom{k}{1} + \cdots + \binom{k}{m}) \dim \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}$.

Supposons maintenant que $m \geq k$ et $\alpha(\widetilde{d} + k - 2) \geq k - 2$. Par ce qui précède $\dim \Gamma^{\mathcal{A}}_{d'} \geq \dim \mathcal{GL}\langle\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d'}}\rangle \geq (2^k - 1) \dim \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}$. D'autre part, d'après [40] on a $\dim \Gamma^{\mathcal{A}}_{d'} = \dim \mathcal{P}^{d'}_{\mathcal{A}} = (2^k - 1) \dim \widetilde{\mathcal{P}}^{\widetilde{d}}_{\mathcal{A}} = (2^k - 1) \dim \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}$. Il suit que $\dim \Gamma^{\mathcal{A}}_{d'} = \dim \mathcal{GL}\langle\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d'}}\rangle = (2^k - 1) \dim \widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}}$.

3.3 Démonstration du Théorème 1.2(ii)

La commutativité des carrés contenant $(Sq^0)^m$ et $(Sq^0)^n$ a été démontrée par Boardman [5]. Celle du carré contenant φ est un cas particulier d'un théorème de Singer [49] que nous rappelons ci-après.

Soient k_1, k_2, d_1, d_2 des entiers positifs ou nuls avec $k_1 + k_2 \leq k$. Posons

$$\begin{aligned} \Gamma(k_1)^{\mathcal{A}} &:= \Gamma(a_1, \ldots, a_{k_1}) \cap \Gamma^{\mathcal{A}}, \\ \Gamma(k_2)^{\mathcal{A}} &:= \Gamma(a_1, \ldots, a_{k_2}) \cap \Gamma^{\mathcal{A}}, \\ \Gamma(k_1+k_2)^{\mathcal{A}} &:= \Gamma(a_1, \ldots, a_{k_1+k_2}) \cap \Gamma^{\mathcal{A}}. \end{aligned}$$

Le morphisme bilinéaire

$$\begin{aligned} \Gamma(k_1)^{\mathcal{A}}_{d_1} \times \Gamma(k_2)^{\mathcal{A}}_{d_2} &\longrightarrow \Gamma(k_1+k_2)^{\mathcal{A}}_{d_1+d_2}, \\ (a_1^{(i_1)} \cdots a_{k_1}^{(i_{k_1})}, a_1^{(j_1)} \cdots a_{k_2}^{(j_{k_2})}) &\longmapsto a_1^{(i_1)} \cdots a_{k_1}^{(i_{k_1})} a_{k_1+1}^{(j_1)} \cdots a_{k_1+k_2}^{(j_{k_2})} \end{aligned}$$

se factorise par les coinvariants sous l'action des groupes linéaires et induit un morphisme linéaire

$$(\Gamma(k_1)^{\mathcal{A}}_{d_1})_{\mathcal{GL}_{k_1}} \otimes (\Gamma(k_2)^{\mathcal{A}}_{d_2})_{\mathcal{GL}_{k_2}} \longrightarrow (\Gamma(k_1+k_2)^{\mathcal{A}}_{d_1+d_2})_{\mathcal{GL}_{k_1+k_2}}.$$

D'autre part, la multiplication usuelle de l'anneau de cohomologie $H^*(\mathcal{A})$ fournit un morphisme linéaire

$$H^{k_1, d_1+k_1} \otimes H^{k_2, d_2+k_2} \longrightarrow H^{k_1+k_2, d_1+d_2+k_1+k_2}.$$

Le théorème de Singer [49] confirme la commutativité du carré

$$\begin{array}{ccc} (\Gamma(k_1)^{\mathcal{A}}_{d_1})_{\mathcal{GL}_{k_1}} \otimes (\Gamma(k_2)^{\mathcal{A}}_{d_2})_{\mathcal{GL}_{k_2}} & \longrightarrow & (\Gamma(k_1+k_2)^{\mathcal{A}}_{d_1+d_2})_{\mathcal{GL}_{k_1+k_2}} \\ \downarrow{\scriptstyle Tr_{k_1} \otimes Tr_{k_2}} & & \downarrow{\scriptstyle Tr_{k_1+k_2}} \\ H^{k_1, d_1+k_1} \otimes H^{k_2, d_2+k_2} & \longrightarrow & H^{k_1+k_2, d_1+d_2+k_1+k_2} \end{array}$$

(une petite remarque : l'attribut "algébrique" que nous donnons au morphisme Tr_k a pour origine ce carré commutatif). En choisissant $k_1 := k-1$, $k_2 := 1$, $d_1 := d'$ et $d_2 := 0$, on obtient le carré contenant φ dans le diagramme du Théorème 1.2(ii). Ainsi, la commutativité de ce diagramme est établie.

Les énoncés concernant les morphismes $(Sq^0)^m$ et $(Sq^0)^n$ de la première ligne résultent trivialement du Lemme 3.1.1.

Supposons $m \geq k$ et $\alpha(\widetilde{d} + k - 2) \geq k - 2$. Montrons que φ est surjectif. D'après le Théorème 1.2(i), on a $\dim \Gamma^{\mathcal{A}}_{d'} = \dim \mathcal{GL}\langle \widetilde{\Gamma}^{\mathcal{A}}_{d'} \rangle$, d'où $\Gamma^{\mathcal{A}}_{d'} = \mathcal{GL}\langle \widetilde{\Gamma}^{\mathcal{A}}_{d'} \rangle$. Il s'ensuit que la composée $\widetilde{\Gamma}^{\mathcal{A}}_{d'} \longrightarrow \Gamma^{\mathcal{A}}_{d'} \xrightarrow{\iota^*} (\Gamma^{\mathcal{A}}_{d'})_{\mathcal{GL}}$ est surjective, le premier morphisme étant l'inclusion. Comme cette composée est égale à la composée $\widetilde{\Gamma}^{\mathcal{A}}_{d'} \xrightarrow{\widetilde{\iota}^*} (\widetilde{\Gamma}^{\mathcal{A}}_{d'})_{\widetilde{\mathcal{GL}}} \xrightarrow{\varphi} (\Gamma^{\mathcal{A}}_{d'})_{\mathcal{GL}}$, on en déduit la surjectivité de φ.

L'égalité $(Sq^0)^n h_0 (Sq^0)^m = h_n (Sq^0)^{m+n}$ résulte du fait $(Sq^0)^n(h_0) = h_n$ et de ce que $Sq^0 : H^*(\mathcal{A}) \longrightarrow H^*(\mathcal{A})$ est un morphisme d'algèbres [25, 41].

Pour terminer, l'énoncé concernant $(\operatorname{Im} Tr_k)^d$ est une conséquence facile de la commutativité du diagramme et des énoncés qui précèdent.

3.4 Démonstration du Théorème 1.2(iii)

Ce théorème sera démontré par récurrence sur k. Sa validité pour $k = 1$ étant classique [43, 49], on suppose $k \geq 2$ et qu'il est vrai pour toute valeur inférieure de k.

Posons

$$\begin{aligned} d_1 &:= 2^{m_1-m_k} + \cdots + 2^{m_{k-1}-m_k} - (k-1), \\ d_2 &:= 2^{m_1-m_{k-1}} + \cdots + 2^{m_{k-2}-m_{k-1}} + 2^0 - (k-1). \end{aligned}$$

Puisque $d = 2^{m_{k-1}}(d_2 + k - 1) + 2^{m_k} - k$ et $m_{k-1} \geq m_k + k \geq k$, d'après le Théorème 1.2(i) on a $\Gamma^{\mathcal{A}}_{d_1} = \mathcal{GL}\langle\widetilde{\Gamma}^{\mathcal{A}}_{d_1}\rangle$. Par hypothèse de récurrence $\widetilde{\Gamma}^{\mathcal{A}}_{d_1} = \widetilde{\mathcal{GL}}\langle a_1^{(2^{m_1-m_k}-1)} \cdots a_{k-1}^{(2^{m_{k-1}-m_k}-1)}\rangle$. Il en résulte que

$$\Gamma^{\mathcal{A}}_{d_1} = \mathcal{GL}\langle a_1^{(2^{m_1-m_k}-1)} \cdots a_{k-1}^{(2^{m_{k-1}-m_k}-1)}\rangle.$$

D'autre part, du fait que $\alpha(d_1 + k - 1) = k - 1$, l'application itérative du Lemme 3.1.1 permet d'obtenir que

$$\begin{aligned} \Gamma^{\mathcal{A}}_d &= (Sq^0)^{m_k}(\Gamma^{\mathcal{A}}_{d_1}) = (Sq^0)^{m_k}(\mathcal{GL}\langle a_1^{(2^{m_1-m_k}-1)} \cdots a_{k-1}^{(2^{m_{k-1}-m_k}-1)}\rangle) \\ &= \mathcal{GL}\langle (Sq^0)^{m_k}(a_1^{(2^{m_1-m_k}-1)} \cdots a_{k-1}^{(2^{m_{k-1}-m_k}-1)})\rangle \\ &= \mathcal{GL}\langle a_1^{(2^{m_1}-1)} \cdots a_k^{(2^{m_k}-1)}\rangle. \end{aligned}$$

Observons que par hypothèse de récurrence, $(\operatorname{Im} Tr_{k-1})^{d_2}$ est le sous-espace vectoriel de H^{k-1,d_2+k-1} engendré par $h_{m_1-m_{k-1}} \cdots h_{m_{k-2}-m_{k-1}} h_0$. Il suit du Théorème 1.2(ii) et de la commutativité [1] de l'algèbre de cohomologie $H^*(\mathcal{A})$ que $(\operatorname{Im} Tr_k)^d$ est le sous-espace vectoriel de $H^{k,d+k}$ engendré par

$$h_{m_k}(Sq^0)^{m_{k-1}}(h_{m_1-m_{k-1}} \cdots h_{m_{k-2}-m_{k-1}} h_0) = h_{m_1} \cdots h_{m_k}.$$

Il reste à vérifier l'égalité concernant $(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}}$. Si $m_1 - m_2 = 1$, d'une part $(\widetilde{\Gamma}^{\mathcal{A}}_{d_1})_{\widetilde{\mathcal{GL}}} = 0$ par hypothèse de récurrence, de l'autre

$$(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = (Sq^0)^{m_k}\varphi((\widetilde{\Gamma}^{\mathcal{A}}_{d_1})_{\widetilde{\mathcal{GL}}})$$

d'après le Théorème 1.2(ii) ; cela implique $(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = 0$. Si $m_1 - m_2 \geq 2$, alors le $\mathcal{GL}$-module $\Gamma^{\mathcal{A}}_d = \mathcal{GL}\langle a_1^{(2^{m_1}-1)} \cdots a_k^{(2^{m_k}-1)}\rangle$ est isomorphe à $\mathbb{F}_2\langle\mathcal{GL}/G_0\rangle$ d'après le Théorème 1.1(i), où $G_0 \subset \mathcal{GL}$ désigne le sous-groupe de Borel des matrices supérieures inversibles. Il suit que $(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = \mathbb{F}_2$.

4 Démonstration du Théorème 1.3

4.1 Généralités

Rappelons d'abord les formules

$$\begin{array}{lll} \mathcal{P}^d_{\mathcal{A}} \cong \mathcal{P}^{(d-k)/2}_{\mathcal{A}} \oplus (\operatorname{Ker}\psi)^d & \text{si } d \equiv k \pmod 2, \\ \Gamma^{\mathcal{A}}_d = Sq^0(\Gamma^{\mathcal{A}}_{(d-k)/2}) \oplus (\operatorname{Coker} Sq^0)_d & \text{si } d \equiv k \pmod 2, \\ \mathcal{P}^d_{\mathcal{A}} = (\operatorname{Ker}\psi)^d,\ \Gamma^{\mathcal{A}}_d = (\operatorname{Coker} Sq^0)_d & \text{si } d \not\equiv k \pmod 2, \end{array}$$

qui ramènent la détermination de $\mathcal{P}_{\mathcal{A}}$, $\Gamma^{\mathcal{A}}$ à celle de $\operatorname{Ker}\psi$, $\operatorname{Coker} Sq^0$ respectivement. Pour déterminer $\operatorname{Ker}\psi$, notre méthode consiste à :

- en produire un système générateur et établir une borne supérieure de la dimension $\dim \operatorname{Ker}\psi$,

– faire appel au Théorème 1.1 qui fournit une borne inférieure de la dimension $\dim \mathrm{Coker}\, Sq^0 = \dim \mathrm{Ker}\, \psi$,
– effectuer des retouches nécessaires pour que ces bornes soient égales et obtenir la valeur exacte de $\dim \mathrm{Ker}\, \psi$.

D'après ce que nous en savons, cette méthode a été utilisée par Alghamdi–Crabb–Hubbuck [3] et Boardman [5], pour qui les travaux de Kameko [19] ont été une source de référence.

Théorème classique Soient $P, Q \in \mathcal{P}$. On note $P \equiv Q$ la relation $P + Q \in \bar{\mathcal{A}}\mathcal{P}$. Le théorème classique de cette branche de la topologie algébrique qui étudie la relation $P \equiv Q$ est le suivant :

Théorème 4.1.1 (Wood [55]) *Soient $P, Q \in \mathcal{P}$. Alors*

(i) *$\theta(P)Q \equiv P\chi(\theta)(Q)$ pour tout $\theta \in \mathcal{A}$, où $\chi : \mathcal{A} \longrightarrow \mathcal{A}$ désigne l'antiautomorphisme canonique de l'algèbre de Steenrod.*

(ii) *$PQ^2 \equiv 0$ si $\alpha(\deg(PQ^2) + \deg P) = \alpha(\deg P + \deg Q) > \deg P$.*

La première moitié du Théorème 4.1.1 est connue [55] sous le nom de χ-technique. La seconde (conséquence de la première) est la généralisation d'une conjecture de Peterson [43] dont elle était issue.

Décomposition Soient $1 \leq i_1 < \cdots < i_r \leq k$ des entiers. On note $\mathcal{P}_{x_{i_1}\ldots x_{i_r}}$ l'idéal engendré par $x_{i_1} \cdots x_{i_r}$ dans la sous-algèbre $\mathbb{F}_2[x_{i_1}, \ldots, x_{i_r}] \subset \mathcal{P}$. L'idéal $\mathcal{P}_{x_{i_1}\ldots x_{i_r}}$ est un sous-$\mathcal{A}$-module de $\mathcal{P}$. On a la somme directe de $\mathcal{A}$-modules

$$\mathcal{P} = \mathbb{F}_2 \bigoplus_{1 \leq i_1 < \cdots < i_r \leq k} \mathcal{P}_{x_{i_1}\ldots x_{i_r}}$$

et la somme directe d'espaces vectoriels gradués

$$\mathcal{P}_{\mathcal{A}} = \mathbb{F}_2 \bigoplus_{1 \leq i_1 < \cdots < i_r \leq k} \pi(\mathcal{P}_{x_{i_1}\ldots x_{i_r}}).$$

Système générateur Soit $\mathcal{B}_{x_1\ldots x_r}$ un système générateur minimal de $\mathcal{P}_{x_1\ldots x_r}$ en tant que $\mathcal{A}$-module, i.e. un sous-ensemble de $\mathcal{P}_{x_1\ldots x_r}$ tel que

$$\pi(\mathcal{P}_{x_1\ldots x_r}) \cong \mathbb{F}_2\, \langle \pi(\mathcal{B}_{x_1\ldots x_r})\rangle.$$

Notons $\mathcal{B}_{x_{i_1}\ldots x_{i_r}}$ l'image de $\mathcal{B}_{x_1\ldots x_r}$ par l'isomorphisme d'algèbres $\mathcal{P}_{x_1\ldots x_r} \longrightarrow \mathcal{P}_{x_{i_1}\ldots x_{i_r}}$ qui envoie x_s sur x_{i_s} pour tout $1 \leq s \leq r$. Il est clair que $\mathcal{B}_{x_{i_1}\ldots x_{i_r}}$ est un système générateur minimal de $\mathcal{P}_{x_{i_1}\ldots x_{i_r}}$ comme $\mathcal{A}$-module : $\pi(\mathcal{P}_{x_{i_1}\ldots x_{i_r}}) = \mathbb{F}_2\, \langle \pi(\mathcal{B}_{x_{i_1}\ldots x_{i_r}})\rangle$. On désigne par $\mathcal{B}^d_{x_{i_1}\ldots x_{i_r}}$ le sous-ensemble des éléments de degré d dans $\mathcal{B}_{x_{i_1}\ldots x_{i_r}}$.

Rappelons (cf. la Section 2.1) que $\mathcal{W} \subset \mathcal{P}$ désigne le sous-espace vectoriel gradué engendré par les monômes $x_1^{i_1} \cdots x_k^{i_k}$ avec $i_1 \cdots i_k$ pair. D'où $\pi(\mathcal{W}) = \mathrm{Ker}\, \psi$, et $\mathcal{W} \cap \mathcal{P}_{x_1\ldots x_k}$ est le sous-espace vectoriel gradué engendré par les monômes $x_1^{i_1} \cdots x_k^{i_k}$ avec $i_1 \cdots i_k$ positif et pair. Notons que l'image par $\pi : \mathcal{P} \longrightarrow \mathcal{P}_{\mathcal{A}}$ d'un système générateur minimal de $\mathcal{W} \cap \mathcal{P}_{x_1\ldots x_k}$ en tant que $\mathcal{A}$-module ne forme pas une base de $\pi(\mathcal{W} \cap \mathcal{P}_{x_1\ldots x_k})$. Théoriquement ce dernier

représente la partie la plus importante de $\operatorname{Ker}\psi$: celle qui concerne *toutes* les k variables $x_1 \ldots, x_k$. On a la formule

$$\begin{aligned}\operatorname{Ker}\psi &= \mathbb{F}_2 \oplus \pi(\mathcal{W} \cap \mathcal{P}_{x_1 \ldots x_k}) \bigoplus_{1 \le i_1 < \cdots < i_r,\ r<k} \pi(\mathcal{P}_{x_{i_1} \ldots x_{i_r}}) \\ &\cong \mathbb{F}_2 \oplus \pi(\mathcal{W} \cap \mathcal{P}_{x_1 \ldots x_k}) \oplus \mathbb{F}_2 \langle \pi(\bigcup_{1 \le i_1 < \cdots < i_r,\ r<k} \mathcal{B}_{x_{i_1} \ldots x_{i_r}}) \rangle.\end{aligned}$$

Ordre lexicographique Pour tout monôme non nul $P \in \mathcal{P}$ et tout $u \in \{x_1, \ldots, x_k\}$, notons $\deg_u P$ le degré de u dans P. L'ordre lexicographique sur l'ensemble des monômes de $\mathcal{P}$ est défini comme suit : pour $P \neq 0$, on a $0 < P$; pour $P, Q \neq 0$, on a $P < Q$ si et seulement s'il existe $1 \le i \le k$ tel que $\deg_{x_i} P < \deg_{x_i} Q$ et $\deg_{x_j} P = \deg_{x_j} Q$ pour tout $1 \le j < i$. Cet ordre est total.

Lemme 4.1.2 *Soit $E \subset \mathcal{P}_{x_1 \ldots x_k}$ un sous-ensemble. Supposons que $\mathcal{B}_{x_1 \ldots x_k} = \{Q_1 < \cdots < Q_N\}$ est un système générateur minimal ayant la propriété :*

- *chaque Q_i est un monôme de $\mathcal{P}_{x_1 \ldots x_k} \backslash E$,*
- *tout $P \in \mathcal{P}_{x_1 \ldots x_k} \backslash E$ s'écrit $P \equiv \sum Q$ pour certains $Q \in \mathcal{B}_{x_1 \ldots x_k}$ vérifiant $Q \le P$.*

Soit $\{Q'_1 < \cdots < Q'_N\}$ un système générateur minimal quelconque de $\mathcal{P}_{x_1 \ldots x_k}$ tel que chaque Q'_i est un monôme de $\mathcal{P}_{x_1 \ldots x_k} \backslash E$. Alors $Q_1 \le Q'_1, \ldots, Q_N \le Q'_N$. Par conséquent, il existe au plus un système générateur minimal $\mathcal{B}_{x_1 \ldots x_k}$ ayant la propriété mentionnée.

Démonstration Par hypothèse $Q'_1 \equiv \sum Q_i$ pour un certain $I \subset \{1, \ldots, N\}$ tel que $Q_i \le Q'_i$ pour tout $i \in I$. Puisque $Q'_1 \not\equiv 0$, l'ensemble I est non-vide. D'où $Q_1 \le Q'_1$.

Soit $1 < i \le N$. Si $Q_i > Q'_i$, alors les éléments $Q'_1, \ldots, Q'_i$ sont engendrés modulo $\bar{A}\mathcal{P}$ par les éléments $Q_1, \ldots, Q_{i-1}$. Il suit que $Q'_1, \ldots, Q'_i$ ne sont pas linéairement indépendants, ce qui est une contradiction. D'où $Q_i \le Q'_i$. □

À cause du Lemme 4.1.2, on peut dire que relativement au sous-ensemble E, le système générateur minimal qui vérifie l'hypothèse du lemme est le plus petit pour l'ordre lexicographique. Dans la Section 4.2, on explicitera un tel système générateur pour $k \le 3$.

Algorithme Inspiré du crible d'Eratosthène, l'algorithme que nous proposons pour construire $\mathcal{B}_{x_1 \ldots x_k}$ à partir de $\mathcal{B}_{x_1 \ldots x_{k-1}}$ consiste à :

0° Choisir un entier $d \ge 0$ et ordonner suivant l'ordre lexicographique les éléments Px_k^n de degré d, avec $P \in \mathcal{B}_{x_1 \ldots x_{k-1}}$ et $n > 0$, pour obtenir une suite croissante $P_1 < \cdots < P_N$.

1° Effacer P_N s'il existe une relation linéaire $P_N \equiv \sum_{1 \le i < N} \lambda_i P_i$ avec $\lambda_i \in \mathbb{F}_2$, et le garder sinon.

2° Effacer P_{N-1} s'il existe une relation linéaire $P_{N-1} \equiv \sum_{1 \le i < N-1} \lambda_i P_i$ avec $\lambda_i \in \mathbb{F}_2$, et le garder sinon.

.....

N° Effacer P_1 si $P_1 \equiv 0$, et le garder sinon.

Nous prenons pour $\mathcal{B}^d_{x_1\dots x_k}$ l'ensemble des éléments qui sont gardés après l'étape N°, et pour $\mathcal{B}_{x_1\dots x_k}$ la réunion $\bigcup_{d\geq 0}\mathcal{B}^d_{x_1\dots x_k}$.

Lemme 4.1.3 *L'ensemble $\mathcal{B}_{x_1\dots x_k}$ obtenu grâce à l'algorithme précédent est un système générateur minimal de $\mathcal{P}_{x_1\dots x_k}$.*

Démonstration Suivons de près l'algorithme. Soit $P \in \mathcal{P}_{x_1\dots x_k}$ un monôme quelconque. Posons $P = Q_1Q_2$ avec $Q_1 \in \mathcal{P}_{x_1\dots x_{k-1}}$ et $Q_2 \in \mathcal{P}_{x_k}$. Puisque $\mathcal{B}_{x_1\dots x_{k-1}}$ est un système générateur de $\mathcal{P}_{x_1\dots x_{k-1}}$ par définition, il existe des monômes $Q \in \mathcal{B}_{x_1\dots x_{k-1}}$, $R \in \mathcal{B}_{x_1\dots x_{k-1}}$ et des éléments $\theta \in \bar{\mathcal{A}}$ tels que $Q_1 = \sum Q + \sum \theta(R)$. D'où

$$P = Q_1Q_2 = \sum QQ_2 + \sum \theta(R)Q_2 \equiv \sum QQ_2 + \sum R\chi(\theta)(Q_2)$$

d'après le Théorème 4.2.1(i). Il suit que les éléments $P_1, \dots, P_N$ de l'étape 0° forment un système générateur de $\mathcal{P}_{x_1\dots x_k}$. D'autre part, il est clair que ces éléments sont engendrés modulo $\bar{\mathcal{A}}\mathcal{P}$ par ceux qui sont gardés, c'est-à-dire par $\mathcal{B}_{x_1\dots x_k}$. Comme on a effacé tout élément P_i susceptible d'engendrer une relation linéaire du type $P_i \equiv \sum_{1\leq j<i}\lambda_j P_j$ avec $\lambda_j \in \mathbb{F}_2$, il ne reste aucune relation linéaire parmi les éléments de $\mathcal{B}_{x_1\dots x_k}$. En d'autres termes, celui-ci est linéairement indépendant. □

Grâce au Lemme 4.1.3 et à l'algorithme précédent, la question d'une base explicite de $\mathcal{P}_{\mathcal{A}}$ est théoriquement résolue. En pratique, on est loin d'avoir une réponse satisfaisante à cette question. On ignore, par exemple, le cardinal $|\mathcal{B}_{x_1\dots x_k}|$ et la structure naturelle de $\mathcal{GL}$-module de $\mathcal{P}_{\mathcal{A}}$.

Notion d'étage Soit $P = x_1^{i_1}\cdots x_k^{i_k} \in \mathcal{P}$ un monôme quelconque. Soit $i_r = 2^0 i_{r,0} + 2^1 i_{r,1} + \cdots$ l'écriture binaire de i_r, avec $i_{r,s} = 0$ ou 1. Pour $s \geq 0$, l'étage s-ième de P, notée $P_{[s]}$, est définie comme étant le monôme $P_{[s]} := x_1^{i_{1,s}}\cdots x_k^{i_{k,s}}$. Chaque étage $P_{[s]}$ est un diviseur de $x_1\cdots x_k$. L'origine de cette appelation réside dans la décomposition $P = \prod_{s\geq 0} P_{[s]}^{2^s}$ (notons que toute décomposition $P = \prod_{s\geq 0} P_s^{2^s}$ vérifiant $P_s \mid x_1\cdots x_k$ pour $s \geq 0$ coïncide nécessairement avec celle-ci).

Lemme 4.1.4 (Nam [39]) *Soient N un entier positif, $P \in \mathcal{P}$ un monôme avec $\deg P_{[s]} \leq 2$ pour $0 \leq s < N$ et $P_{[s]} = 1$ pour $s \geq N$, et $Q \in \mathcal{P}$ un polynôme quelconque.*

(i) *Si $Q \equiv 0$, alors $PQ^{2^N} \equiv 0$.*

(ii) *Si $\deg P_{[s]} > \deg P_{[t]}$ pour certains $s > t \geq 0$, alors $PQ^{2^N} \equiv 0$.*

(iii) *Supposons $\deg P_{[s]} = \deg P_{[0]}$ pour tout $0 \leq s < N$. Alors*

$$PQ^{2^N} \equiv \prod_{s=0}^{N-1} P_{[\sigma(s)]}^{2^s} Q^{2^N}$$

pour toute permutation σ de l'ensemble $\{0, \dots, N-1\}$.

(iv) *Soit $R \in \mathcal{P}$ un monôme vérifiant $R_{[s]} = 1$ pour tout $s \geq N$ et*

$$\{R_{[0]}, \dots, R_{[N-1]}\} = \{P_{[0]}, \dots, P_{[N-1]}\}.$$

Supposons $\deg P_{[s]} = \deg P_{[0]}$ pour tout $0 \leq s < N$ et que, si $\deg P_{[0]} = 2$, l'ensemble $\{P_{[0]}, \dots, P_{[N-1]}, Q\}$ n'est pas composé de polynômes deux à deux premiers. Alors $PQ^{2^N} \equiv RQ^{2^N}$.

Démonstration (i) Il suffit de montrer le lemme pour $N = 1$, car le cas général s'en déduit facilement par récurrence. Supposons $Q = Sq^1(Q_1) + Sq^2(Q_2) + \cdots + Sq^M(Q_M)$. À cause de l'instabilité de $\mathcal{P}$ en tant que $\mathcal{A}$-module et la formule de Cartan, on a

$$\begin{aligned} PQ^2 &= \sum_{i=1}^{M} PSq^{2i}(Q_i^2) = \sum_{i=1}^{M} \big(Sq^{2i}(PQ_i^2) + Sq^2(P)Sq^{2i-2}(Q^2)\big) \\ &\equiv \sum_{i=1}^{M} Sq^2(P)Sq^{2i-2}(Q^2). \end{aligned}$$

Si $\deg P < 2$, alors $Sq^2(P) = 0$ à cause de l'instabilité de $\mathcal{P}$ en tant que $\mathcal{A}$-module. Si $\deg P = 2$, alors

$$Sq^2(P)Sq^{2i-2}(Q^2) = P^2Sq^{2i-2}(Q^2) = Sq^{i+1+\deg Q}(PSq^{i-1}(Q)) \equiv 0$$

à cause de l'instabilité de $\mathcal{P}$ en tant que $\mathcal{A}$-algèbre. Dans tous les cas $PQ^2 \equiv 0$.

(ii) Si $\deg P_{[s]} > \deg P_{[t]}$ pour certains $s > t \geq 0$, on peut supposer que $t = s - 1$. Posons $\bar{P} := \prod_{0 \leq r < s-1} P_{[r]}^{2^r}$ et $\bar{Q} := \prod_{s < r < N} P_{[r]}^{2^{r-s-1}} Q^{2^{N-s-1}}$. Si $\deg P_{[s]} = 1$, alors $P_{[s-1]} = 1$ et $P_{[s-1]}P_{[s]}^2\bar{Q}^4 = Sq^{1+2\deg \bar{Q}}(P_{[s]}\bar{Q}^2) \equiv 0$. Si $\deg P_{[s]} = 2$, alors

$$\begin{aligned} P_{[s-1]}P_{[s]}^2\bar{Q}^4 &= Sq^2(P_{[s-1]}P_{[s]}\bar{Q}^4) + Sq^1(P_{[s-1]})Sq^1(P_{[s]}\bar{Q}^4) \\ &= Sq^2(P_{[s-1]}P_{[s]}\bar{Q}^4) + Sq^1\big(P_{[s-1]}Sq^1(P_{[s]}\bar{Q}^4)\big) \equiv 0. \end{aligned}$$

Dans tous les cas, d'après le Lemme 4.1.4(i) on a

$$PQ^{2^N} = \bar{P}(P_{[s-1]}P_{[s]}^2\bar{Q}^4)^{2^{s-1}} \equiv 0.$$

(iii) Il suffit de considérer le cas où σ permute r et $r+1$ $(0 \leq r < N-1)$ en fixant le reste de l'ensemble $\{0, \ldots, N-1\}$. Posons $\bar{P} := \prod_{0 \leq s < r} P_{[s]}^{2^s}$ et $\bar{Q} := \prod_{r+2 \leq s < N} P_{[s]}^{2^{s-r-2}} Q^{2^{N-r-2}}$. Si $\deg P_{[r]} = 1$, alors

$$P_{[r]}P_{[r+1]}^2\bar{Q}^4 = Sq^1(P_{[r]}P_{[r+1]}\bar{Q}^4) + P_{[r+1]}P_{[r]}^2\bar{Q}^4 \equiv P_{[r+1]}P_{[r]}^2\bar{Q}^4.$$

Si $\deg P_{[r]} = 2$, alors

$$\begin{aligned} P_{[r]}P_{[r+1]}^2\bar{Q}^4 &= Sq^2(P_{[r]}P_{[r+1]}\bar{Q}^4) + Sq^1(P_{[r]})Sq^1(P_{[r+1]}\bar{Q}^4) + P_{[r+1]}P_{[r]}^2\bar{Q}^4 \\ &= Sq^2(P_{[r]}P_{[r+1]}\bar{Q}^4) + Sq^1\big(P_{[r]}Sq^1(P_{[r+1]}\bar{Q}^4)\big) + P_{[r+1]}P_{[r]}^2\bar{Q}^4 \\ &\equiv P_{[r+1]}P_{[r]}^2\bar{Q}^4. \end{aligned}$$

Dans tous les cas, d'après le Lemme 4.1.4(i) on a

$$PQ^{2^N} = \bar{P}(P_{[r]}P_{[r+1]}^2\bar{Q}^4)^{2^r} \equiv \bar{P}(P_{[r+1]}P_{[r]}^2\bar{Q}^4)^{2^r} \equiv \prod_{s=0}^{N-1} P_{[\sigma(s)]}^{2^s} Q^{2^N}.$$

(iv) Si $P_{[0]}, \ldots, P_{[N-1]}$ sont distincts, alors $(R_{[0]}, \ldots, R_{[N-1]})$ est une permutation de $(P_{[0]}, \ldots, P_{[N-1]})$, et le lemme résulte du Lemme 4.1.4(iii). Supposons

que $P_{[0]}, \ldots, P_{[N-1]}$ ne sont pas distincts. En utilisant le Lemme 4.1.4(iii), il suffit de considérer le cas où $N = 3$, $P_{[0]} = P_{[1]} = R_{[2]}$ et $R_{[0]} = R_{[1]} = P_{[2]}$.

Supposons $\deg P_{[0]} = 1$. Posons $P_{[0]} = x$, $R_{[0]} = y$. Il s'agit de montrer $x^3y^4Q^8 \equiv xy^6Q^8$. On a

$$\begin{aligned} x^3y^4Q^8 &= Sq^1(x^3y^3Q^8) + x^4y^3Q^8 \equiv x^4y^3Q^8 \equiv yy^2x^4Q^8 \\ &\equiv xy^6Q^8 \text{ d'après le Lemme 4.1.4(iii).} \end{aligned}$$

Supposons $\deg P_{[0]} = 2$. Posons $P_{[0]} = xy$, $R_{[0]} = zt$ avec x, y, z, t de degré 1. Il s'agit de montrer $(xy)^3(zt)^4Q^8 \equiv xy(zt)^6Q^8$. Comme les polynômes xy, zt, Q ne sont pas deux à deux premiers, on peut supposer que soit $x = z$, soit $x \mid Q$. Si $x = z$, on a

$$\begin{aligned} & (xy)^3(zt)^4Q^8 = Sq^1(x^7y^3t^3Q^8) + x^8y^3t^3Q^8 + x^7y^4t^3Q^8 \\ \equiv\ & x^8y^3t^3Q^8 + x^7y^4t^3Q^8 \\ \equiv\ & Sq^4(x^4y^3t^3Q^8) + x^4y^5t^5Q^8 + x^4y^4t^6Q^8 + x^4y^6t^4Q^8 + x^7y^4t^3Q^8 \\ \equiv\ & x^4y^5t^5Q^8 + x^7y^4t^3Q^8 \equiv Sq^2(x^2y^5t^5Q^8) + x^2y^6t^6Q^8 + x^7y^4t^3Q^8 \\ \equiv\ & x^7y^4t^3Q^8 \equiv (xt)^3(xy)^4Q^8 \equiv xy(xt)^6Q^8 \text{ d'après le Lemme 4.1.4(iii).} \end{aligned}$$

Si $x \mid Q$, on a $ztQ^2 = Sq^1(ztx(Q/x)^2) + z^2tx(Q/x)^2 + zt^2x(Q/x)^2$. Il s'ensuit d'après le Lemme 4.1.4(i) que

$$\begin{aligned} (xy)^3(zt)^4Q^8 &\equiv (xy)^3(z^2tx(Q/x)^2 + zt^2x(Q/x)^2)^4 \\ &\equiv (xy)^3(xt)^4(zQ/x)^8 + (xy)^3(xz)^4(tQ/x)^8. \end{aligned}$$

Puisque les polynômes xy, xz, xt ne sont pas deux à deux premiers, par ce qui précède on a $(xy)^3(xt)^4(zQ/x)^8 \equiv xy(xt)^6(zQ/x)^8$ et $(xy)^3(xz)^4(tQ/x)^8 \equiv xy(xz)^6(tQ/x)^8$. D'autre part, observons que

$$(xt)^3(zQ/x)^4 + (xz)^3(tQ/x)^4 = Sq^1(x^3z^3t^3(Q/x)^4) + x^4z^3t^3(Q/x)^4 \equiv (zt)^3Q^4.$$

D'où

$$\begin{aligned} (xy)^3(zt)^4Q^8 &\equiv xy(xt)^6(zQ/x)^8 + xy(xz)^6(tQ/x)^8 \\ &\equiv xy\big((xt)^3(zQ/x)^4 + (xz)^3(tQ/x)^4\big)^2 \\ &\equiv xy(zt)^6Q^8 \text{ d'après le Lemme 4.1.4(i).} \end{aligned}$$

Notons que le lemme n'est plus valable si l'ensemble $\{P_{[0]}, \ldots, P_{[N-1]}, Q\}$ est composé de polynômes deux à deux premiers. Les monômes $P := x_1x_2(x_3x_4)^6$, $Q := 1$, $R := (x_1x_2)^3(x_3x_4)^4$ constituent un bon contre-exemple. En effet, on a $d_0^* := P + R \not\equiv 0$ (voir l'Appendice 8.1). On verra par la Proposition 6.13 que $\pi(d_0^*)$ est l'unique élément $\mathcal{GL}$-invariant non nul de $\mathcal{P}^{14}_{\mathcal{A}}$ lorsque $k = 4$. □

4.2 Cas de trois variables

On écrira x, y, z respectivement à la place de x_1, x_2, x_3 dans cette section.

Alors que $\mathcal{B}_x$ est unique, les ensembles $\mathcal{B}_{xy}$ et $\mathcal{B}_{xyz}$ semblent varier selon les chercheurs. Les informations sur ces ensembles sont rassemblées dans le Théorème 4.2.1 suivant. La connaissance de $\mathcal{B}_x$, $\mathcal{B}_{xy}$ fournie par le Théorème 4.2.1(i) est due à Peterson [43]. Celle de $\mathcal{B}_{xyz}$ fournie par le Théorème 4.2.1(ii)

est due à Kameko [19] et à l'auteur [39] (indépendamment de Kameko). Notons que le système générateur minimal de Kameko presque coïncide avec celui de l'auteur (la seule différence se manifeste en un monôme de degré 8, qui est xzx^2y^4 pour Kameko et $xy(xyz)^2$ pour l'auteur). La description actuelle de $\mathcal{B}_{xy}$ et $\mathcal{B}_{xyz}$ est due à l'auteur [39, Proposition 3.2].

Théorème 4.2.1 (i) *$\mathcal{B}_x = \{x^{2^p-1} \mid p \geq 1\}$, tandis que $\mathcal{B}_{xy}$ est composé des monômes $x^{2^{p+q}-1}y^{2^{p+1}-1}$, $x^{2^{p+1}-1}y^{2^{p+q}-1}$, $x^{2^{p+1}-1}y^{2^{p+q+1}-2^p-1}$ avec $p \geq 1$, $q \geq 0$. D'une manière récursive, $\mathcal{B}_x = \{xP^2 \mid P \in \mathcal{B}_x \text{ ou } P = 1\}$ et $\mathcal{B}_{xy}$ se décrit comme étant l'ensemble des monômes*

$$\begin{cases} xP^2, & P \in \mathcal{B}_y, \\ xyP^2, & P \in \mathcal{B}_{xy} \cup \mathcal{B}_x \cup \mathcal{B}_y \cup \{1\}. \end{cases}$$

(ii) *D'une manière récursive, $\mathcal{B}_{xyz}$ se décrit comme étant l'ensemble des monômes*

$$\begin{cases} xyP^2, & P \in \mathcal{B}_{xz} \cup \mathcal{B}_{yz} \cup \mathcal{B}_z \cup \{xyz\}, \\ xzP^2, & P \in \mathcal{B}_{yz} \cup \mathcal{B}_y, \\ xy(xz)^2P^4, & P \in \mathcal{B}_{yz} \cup \mathcal{B}_y, \\ (xy)^3P^4, & P \in \mathcal{B}_z, \\ xy^2P^4, & P \in \mathcal{B}_z, \\ xyzP^2, & P \in \mathcal{B}_{xyz} \cup \mathcal{B}_{xy} \cup \mathcal{B}_{xz} \cup \mathcal{B}_{yz} \cup \mathcal{B}_x \cup \mathcal{B}_y \cup \mathcal{B}_z \cup \{1\}. \end{cases}$$

La propriété qui caractérise ces ensembles s'exprime dans le lemme suivant :

Lemme 4.2.2 (i) *Soit $P \in \mathcal{P}_{xy}$ un monôme. Alors $P = \sum Q + \sum \theta(R)$ pour certains $\theta \in \bar{\mathcal{A}}$ et certains monômes $Q, R \in \mathcal{B}_{xy}$ vérifiant $Q \leq P$ et $R \leq P$.*

(ii) *Soit $P \in \mathcal{P}_{xyz}$ un monôme. Si P n'est pas de la forme*

$$(xyz)^{2^m-1}z^{2^n-2^{m+1}}, \ n > m+1 \geq 2,$$

alors $P \equiv \sum Q$ pour certains $Q \in \mathcal{B}_{xyz}$ vérifiant $Q \leq P$. De plus

$$(xyz)^{2^m-1}z^{2^n-2^{m+1}} \equiv (xyz)^{2^{m-1}-1}x^{2^{m-1}}y^{2^m}z^{2^n-2^{m+1}}$$

pour tout $n > m+1 \geq 2$.

On peut donc dire, grâce à ce lemme et le Lemme 4.1.2, que pour l'ordre lexicographique

- $\mathcal{B}_{xy}$ est le système générateur minimal (de $\mathcal{P}_{xy}$) le plus petit,
- relativement à l'ensemble $\{(xyz)^{2^m-1}z^{2^n-2^{m+1}} \mid n > m+1 \geq 2\}$, $\mathcal{B}_{xyz}$ est le système générateur minimal (de $\mathcal{P}_{xyz}$) le plus petit.

Démonstration (i) Pour toute suite d'entiers positifs ou nuls $I = (i_1, \ldots, i_r)$, notons $2I := (2i_1, \ldots, 2i_r)$ et $Sq^I := Sq^{i_1} \cdots Sq^{i_r}$. Avant de montrer le lemme, montrons la remarque suivante : étant donnés des éléments $P_1, P_2 \in \mathcal{P}$ et une suite $I = (i_1, \ldots, i_r)$, on a

$$\begin{cases} P_1Sq^{2I}(P_2^2) &= \sum Sq^{2I_1}(Sq^{2I_2}(P_1)P_2^2), \\ xSq^{2I}(P_2^2) &= Sq^{2I}(xP_2^2), \\ xySq^{2I}(P_2^2) &= \sum Sq^{I_3}(xy^{2^i}P_2^2) \end{cases}$$

pour certains entiers $i \geq 0$ et certaines suites I_1, I_2, I_3 vérifiant : $I_3 \neq 0$ si $I \neq 0$. En effet, la première égalité résulte facilement de la formule de Cartan par récurrence sur $i_1 + \cdots + i_r$. La seconde est claire à cause de la formule de Cartan. Montrons la troisième par récurrence sur $i_1 + \cdots + i_r$. Il n'y a rien à faire si $i_1 + \cdots + i_r = 0$. Supposons $i_1 > 0$ et que cette égalité a lieu pour toute valeur inférieure de $i_1 + \cdots + i_r$. Posons $J := (i_2, \ldots, i_r)$. D'après la formule de Cartan on a

$$\begin{aligned} xySq^{2I}(P_2^2) &= xySq^{2i_1}Sq^{2J}(P_2^2) \\ &= Sq^{2i_1}\big(xySq^{2J}(P_2^2)\big) + x^2y^2Sq^{2i_1-2}Sq^{2J}(P_2^2) \\ &= Sq^{2i_1}\big(xySq^{2J}(P_2^2)\big) + Sq^1\big(xy^2Sq^{2i_1-2}Sq^{2J}(P_2^2)\big). \end{aligned}$$

Par hypothèse de récurrence $xySq^{2J}(P_2^2) = \sum Sq^{J_1}(xy^{2^j}P_2^2)$ pour certaines suites J_1 et certains entiers $j \geq 0$. D'autre part, d'après la première égalité $xy^2Sq^{2i_1-2}Sq^{2J}(P_2^2) = \sum Sq^{2J_2}(Sq^{2J_3}(xy^2)P_2^2)$ pour certaines suites J_2, J_3. Il est facile de vérifier que $Sq^{2J_3}(xy^2) = 0$ ou xy^{2^i} pour un certain entier $i > 0$. D'où

$$xySq^{2I}(P_2^2) = \sum Sq^{2i_1}Sq^{J_1}(xy^{2^j}P_2^2) + \sum Sq^1Sq^{2J_2}(xy^{2^i}P_2^2).$$

Revenons au lemme. Montrons-le par récurrence sur $\deg P$. Il n'y a rien à faire si $\deg P = 2$. Supposons $\deg P > 2$ et qu'il est vrai pour toute valeur inférieure de $\deg P$. Posons $\bar{P} := \sqrt{P/P_{[0]}}$. Observons que $\bar{P} = \sum \bar{Q} + \sum Sq^I(\bar{R})$ pour certaines suites $I \neq 0$ et certains monômes $\bar{Q}, \bar{R} \in \mathcal{B}_{xy} \cup \mathcal{B}_x \cup \mathcal{B}_y$ vérifiant $\bar{Q} \leq \bar{P}$ et $\bar{R} \leq \bar{P}$. En effet, ceci est facile si $\bar{P} \in \mathcal{B}_x \cup \mathcal{B}_y$, et vrai si $\bar{P} \in \mathcal{B}_{xy}$ par hypothèse de récurrence.

Supposons d'abord $P_{[0]} = xy$. D'après la remarque précédente on a

$$P = xy\bar{P}^2 = \sum xy\bar{Q}^2 + \sum xySq^{2I}(\bar{R}^2) = \sum xy\bar{Q}^2 + \sum Sq^{I_1}(xy^{2^i}\bar{R}^2)$$

pour certaines suites $I_1 \neq 0$ et certains entiers $i \geq 0$. Il est clair que $P \geq xy\bar{Q}^2 \in \mathcal{B}_{xy}$ et que $\deg_x xy^{2^i}\bar{R}^2 \leq \deg_x P$. Comme $\deg xy^{2^i}\bar{R}^2 = \deg P - \deg Sq^{I_1} < \deg P$, ceci implique que $xy^{2^i}\bar{R}^2 < P$. Par hypothèse de récurrence $xy^{2^i}\bar{R}^2 = \sum Q_1 + \sum \theta_1(R_1)$ pour certains $\theta_1 \in \bar{\mathcal{A}}$ et certains $Q_1, R_1 \in \mathcal{B}_{xy}$ vérifiant $Q_1 \leq xy^{2^i}\bar{R}^2 < P$ et $R_1 \leq xy^{2^i}\bar{R}^2 < P$. D'où $P = \sum xy\bar{Q}^2 + \sum Sq^{I_1}(Q_1) + \sum Sq^{I_1}\theta_1(R_1)$, ce qu'on cherchait.

Supposons ensuite $\deg P_{[0]} = 1$. D'après la remarque précédente on a

$$P = P_{[0]}\bar{P}^2 = \sum P_{[0]}\bar{Q}^2 + \sum P_{[0]}Sq^{2I}(\bar{R}^2) = \sum P_{[0]}\bar{Q}^2 + \sum Sq^{2I}(P_{[0]}\bar{R}^2).$$

Il est clair que $P_{[0]}\bar{Q}^2 \leq P$. Posons

$$(Q, R_1, R_2) := \begin{cases} (P_{[0]}\bar{Q}^2, 0, 0) \text{ si } xy \nmid P_{[0]}\bar{Q}^2, \\ (xy^{\deg P - 1}, 0, 0) \text{ si } xy \mid P_{[0]}\bar{Q}^2 \text{ et } \deg \bar{Q}_{[0]} = 1, \\ (0, \bar{Q}^4P_{[0]}^2/(x^3y^3), \bar{Q}^4P_{[0]}/(x^3y^3)) \text{ si } xy \mid \bar{Q}_{[0]}. \end{cases}$$

Il est facile de vérifier que $P \geq Q \in \mathcal{B}_{xy} \cup \{0\}$, $R_1 < P$, $R_2 < P$ et $P_{[0]}\bar{Q}^2 = Q + Sq^1(R_1) + Sq^2(R_2)$. Par hypothèse de récurrence on a $Sq^1(R_1) + Sq^2(R_2) + Sq^{2I}(P_{[0]}\bar{R}^2) = \sum Q_1 + \sum \theta_1(R_3)$ pour certains $\theta_1 \in \bar{\mathcal{A}}$ et certains monômes

$Q_1, R_3 \in \mathcal{B}_{xy}$ tels que $Q_1 \leq P$ et $R_3 \leq P$. D'où $P = Q + \sum Q_1 + \sum \theta_1(R_3)$, ce qu'on cherchait.

Supposons enfin $P_{[0]} = 1$. Alors $P = Sq^{\deg P/2}(\sqrt{P})$. Par hypothèse de récurrence $\sqrt{P} = \sum Q_1 + \sum \theta_1(R_1)$ pour certains $\theta_1 \in \bar{\mathcal{A}}$ et certains monômes $Q_1, R_1 \in \mathcal{B}_{xy}$ tels que $Q_1 \leq \sqrt{P} < P$ et $R_1 \leq \sqrt{P} < P$. D'où

$$P = \sum Sq^{\deg P/2}(Q_1) + \sum Sq^{\deg P/2}\theta_1(R_1),$$

ce qu'il fallait démontrer.

(ii) Montrons d'abord, par récurrence sur m, la deuxième partie du lemme. Si $m = 1$, celle-ci est vraie à cause du Lemme 4.3.1(i). Supposons $m > 1$ et qu'elle est vraie pour toute valeur inférieure de m. Par hypothèse de récurrence on a

$$(xyz)^{2^m-1}z^{2^n-2^{m+1}} \equiv (xyz)^{2^{m-1}-1}x^{2^{m-1}}y^{2^m}z^{2^n-2^{m+1}} + \sum_{i>0} Sq^i(P_i)$$

pour certains $P_i \in \mathcal{P}$. Notons que pout tout $i > 0$ on a

$$xyzSq^{2i}(P_i^2) = Sq^{2i}(xyzP_i^2) + Sq^1(x^2yzSq^{2i-2}(P_i^2)) + xy^2z^2Sq^{2i-2}(P_i^2).$$

Puisque $\alpha(1 + \deg xy^2z^2Sq^{2i-2}(P_i^2)) > 1$, d'après le Théorème 4.1.1(ii) on a $xy^2z^2Sq^{2i-2}(P_i^2) \equiv 0$. D'où

$$(xyz)^{2^m-1}z^{2^n-2^{m+1}} \equiv (xyz)^{2^{m-1}-1}x^{2^{m-1}}y^{2^m}z^{2^n-2^{m+1}}.$$

Montrons maintenant la première partie du lemme. Notons E l'ensemble des monômes $(xyz)^{2^m-1}z^{2^n-2^{m+1}}$ avec $n > m+1 \geq 2$. Raisonnons par l'absurde. Supposons qu'il existe des monômes de $\mathcal{P}\backslash E$ qui ne vérifient pas le lemme. Soit P le plus petit d'entre eux pour l'ordre lexicographique.

Montrons que P ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes de $\mathcal{P}_{xyz}$ qui lui sont inférieurs. Supposons le contraire $P \equiv Q + \sum R$ pour certains monômes $Q \in E \cup \{0\}$, $R \notin E$ vérifiant $\max(Q, R) < P$. Comme P est minimum, les monômes R vérifient le lemme. D'où $Q \in E$. Soit $Q = (xyz)^{2^m-1}z^{2^n-2^{m+1}}$ avec $n > m+1 \geq 2$. Par ce qui précède on a $Q \equiv (xyz)^{2^{m-1}-1}x^{2^{m-1}}y^{2^m}z^{2^n-2^{m+1}}$. Puisque $P > Q$, on vérifie aisément que $P \geq (xyz)^{2^{m-1}-1}x^{2^{m-1}}y^{2^m}z^{2^n-2^{m+1}}$. Comme ce dernier est dans $\mathcal{B}_{xyz}$, il suit que P vérifie le lemme, d'où une contradiction.

Montrons que $x^{\deg_x P}y^{\deg_y P} \in \mathcal{B}_{xy}$. Supposons le contraire. Alors, d'après le Lemme 4.2.2(i) on a $x^{\deg_x P}y^{\deg_y P} = \sum Q + \sum \theta(R)$ pour certains $Q \in \mathcal{B}_{xy}$, $R \in \mathcal{B}_{xy}$, $\theta \in \bar{\mathcal{A}}$ qui vérifient $\max(Q, R) < x^{\deg_x P}y^{\deg_y P}$. D'après le Théorème 4.1.1(i) on a

$$P = \sum Qz^{\deg_z P} + \sum \theta(R)z^{\deg_z P} \equiv \sum Qz^{\deg_z P} + \sum R\chi(\theta)(z^{\deg_z P}).$$

Ces monômes sont inférieurs à P, d'où une contradiction.

Montrons que $\deg P_{[0]} > 1$. Supposons le contraire. Alors $P = xy^{2^m-2}z^{\deg_z P}$ pour un certain $m \geq 2$. En utilisant le Lemme 4.1.4(ii), il suit que $\deg_z P = 2^n - 2^m$ pour un certain $n > m$. D'où $P \equiv xy^2z^{2^n-4}$ d'après le Lemme 4.1.4(iv). Ceci est une contradiction car $P \geq xy^2z^{2^n-4} \in \mathcal{B}_{xyz}$.

Montrons que $\deg P_{[0]} < 3$. Supposons le contraire. Alors $P_{[0]} = xyz$. Comme $\sqrt{P/xyz} < P$, par hypothèse et d'après le Lemme 4.2.2(i) on a $\sqrt{P/xyz} = \sum Q + \sum_{i>0} Sq^i(R_i)$ pour certains $R_i \in \mathcal{P}$ et $Q \in \mathcal{B}_{xyz} \cup \mathcal{B}_{xy} \cup \mathcal{B}_{xz} \cup \mathcal{B}_{yz} \cup \mathcal{B}_x \cup \mathcal{B}_y \cup \mathcal{B}_z \cup \{1\}$ qui vérifient $Q \leq \sqrt{P/xyz}$. Il suit que

$$P = \sum xyzQ^2 + \sum xyzSq^{2i}(R_i^2) \equiv \sum xyzQ^2 + \sum xy^2z^2Sq^{2i-2}(R_i^2).$$

En utilisant la χ-technique et les Lemmes 4.1.4(ii), 4.1.4(iv), on montre sans difficulté que $\sum xy^2z^2Sq^{2i-2}(R_i^2) \equiv \varepsilon xy^2z^{2^n-4}$ pour certains $n \geq 3$ et $\varepsilon \in \{0,1\}$. D'où $P \equiv \sum xyzQ^2 + \varepsilon xy^2z^{2^n-4}$. Notons que $P \geq xyzQ^2 \in \mathcal{B}_{xyz}$ et $P \geq xy^2z^{2^n-4} \in \mathcal{B}_{xyz}$. Ceci est une contradiction.

Montrons que $xy \mid P_{[1]}$. Supposons le contraire. Alors P est de la forme

$$P = \begin{cases} xyQ^2, & Q \in \mathbb{F}_2[x,z] \cup \mathbb{F}_2[y,z], \\ xzQ^2, & Q \in \mathbb{F}_2[y,z], \\ xy(xz)^2Q^4, & Q \in \mathbb{F}_2[y,z]. \end{cases}$$

Si $P = xyQ^2$ avec $Q \in \mathbb{F}_2[x,z]$, alors d'après le Lemme 4.2.2(i) $Q \equiv \sum R$ pour certains $R \in \mathcal{B}_{xz} \cup \mathcal{B}_z$ qui vérifient $R \leq Q$. D'après le Lemme 4.1.4(i) on a $P \equiv \sum xyR^2$. Comme $P \geq xyR^2 \in \mathcal{B}_{xyz}$, il suit que P vérifie le lemme, ce qui est une contradiction. De manière analogue, on aboutit également à une contradiction si $P = xyQ^2$, xzQ^2 ou $xy(xz)^2Q^4$ avec $Q \in \mathbb{F}_2[y,z]$.

Montrons que $P_{[1]} \neq xyz$. Supposons le contraire. Alors $P_{[0]} = xy$. Posant $P =: xy(xyz)^2Q^4$, on a

$$\begin{aligned} P &= Sq^1(x^3y^3zQ^4) + x^4y^3zQ^4 + x^3y^4zQ^4 \\ &\equiv x^2\chi(Sq^2)(y^3zQ^4) + xz(xy^2Q^2)^2 \text{ d'après le Théorème 4.1.1(i).} \end{aligned}$$

Il est facile de vérifier que $xy^2Q^2 \equiv \sum yx^2R^4$ pour certains $R \in \mathcal{B}_y \cup \mathcal{B}_z$ qui vérifient $R_{[0]}R^2 \leq Q$. D'où

$$\begin{aligned} & xz(xy^2Q^2)^2 \equiv \sum xz(yx^2R^4)^2 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & \sum \left(Sq^1(xyzx^4) + x^6yz + xyz^2x^4\right)R^8 \equiv yz(xR_{[0]}^2R^4)^2 + xy(xz^2R^4)^2 \end{aligned}$$

d'après les Lemmes 4.1.4(i) et 4.1.4(iv). Ces derniers monômes sont inférieurs à P. De plus $x^2\chi(Sq^2)(y^3zQ^4)$ est une somme de monômes inférieurs à P. Il suit que P vérifie le lemme, ce qui est une contradiction.

Jusqu'ici $P_{[0]} = P_{[1]} = xy$. Montrons que $x \nmid P_{[2]}$. Supposons le contraire. Posant $P =: (xy)^3(xzQ)^4$, on a

$$\begin{aligned} P &= Sq^1(x^7y^3z^3Q^4) + x^8y^3z^3Q^4 + x^7y^4z^3Q^4 \\ &\equiv x^8y^3z^3Q^4 + Sq^2(x^7y^2z^3Q^4) + x^9y^2z^3Q^4 + x^8y^2z^4Q^4 + x^7y^2z^5Q^4 \\ &\equiv x^8y^3z^3Q^4 + x^9y^2z^3Q^4 + xy(xz)^2(xzQ)^4 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv x^4\chi(Sq^4)(y^3z^3Q^4) + x^5\chi(Sq^4)(y^2z^3Q^4) + x^7yz^6Q^4 \end{aligned}$$

d'après le Théorème 4.1.1(i). Ces monômes sont inférieurs à P, d'où une contradiction.

Montrons que $P_{[2]} \neq yz$. Supposons le contraire. Posant $P =: (xy)^3(yz)^4Q^8$, on a $P \equiv xy(yz)^6Q^8$ d'après le Lemme 4.1.4(iv). Ce monôme est inférieur à P, d'où une contradiction.

Montrons que $P_{[2]} \neq y$. Supposons le contraire. Alors $P = (xy)^3y^4(zQ)^8$ pour un certain $Q \in \mathbb{F}_2[z]$. On a

$$\begin{aligned} P &= Sq^1(x^3y^7z^7Q^8) + x^4y^7z^7Q^8 + x^3y^8z^7Q^8 \\ &\equiv x^4y^7z^7Q^8 + (xz)^3y^4(zQ)^8 \text{ d'après les Lemmes 4.1.4(i) et 4.1.4(iii)} \\ &\equiv x^2\chi(Sq^2)(y^7z^7Q^8) + x^3y^4z^{11}Q^8 \text{ d'après le Théorème 4.1.1(i).} \end{aligned}$$

Ces monômes sont inférieurs à P, d'où une contradiction.

Jusqu'ici $P_{[0]} = P_{[1]} = xy$ et $P = (xy)^3Q^4$ pour un certain $Q \in \mathbb{F}_2[z]$. Par hypothèse on a $Q \notin \mathcal{B}_z$. Il suit que $Q \equiv 0$. D'où $P \equiv 0$ d'après le Lemme 4.1.4(i). Ceci est une contradiction. □

4.3 Lemmes principaux

À partir d'ici jusqu'à la fin de la Section 4, on travaillera uniquement avec $k = 4$ et écrira x, y, z, t respectivement à la place de x_1, x_2, x_3, x_4.

Notons

- $\mathcal{W}_1 \subset \mathcal{P}_{xyzt}$ le sous-espace vectoriel gradué engendré par les monômes P vérifiant $\deg P_{[0]} = 2 > \deg P_{[s]}$ pour tout $s \geq 1$,
- $\mathcal{W}_2 \subset \mathcal{P}_{xyzt}$ le sous-espace vectoriel gradué engendré par les monômes P vérifiant $\deg P_{[0]} = \deg P_{[1]} = 2 > \deg P_{[s]}$ pour tout $s \geq 2$,
- $\mathcal{W}_3 \subset \mathcal{P}_{xyzt}$ le sous-espace vectoriel gradué engendré par les monômes P vérifiant $\deg P_{[0]} = \deg P_{[1]} = \deg P_{[2]} = 2 \geq \deg P_{[s]}$ pour tout $s \geq 3$.

On montrera que $\pi(\mathcal{W}_1 \cup \mathcal{W}_2 \cup \mathcal{W}_3) = \pi(\mathcal{W} \cap \mathcal{P}_{xyzt})$ en degré pair supérieur à 16, et on explicitera une base de $\pi(\mathcal{W}_1 \cup \mathcal{W}_2 \cup \mathcal{W}_3)$ en degré pair supérieur à 22.

Lemme 4.3.1 (i) *Soit $P \in \mathcal{P}$. Alors*

$$\begin{array}{llllllll} x(xyz)^2P^4 & \equiv & y(xyz)^2P^4 & \equiv & z(xyz)^2P^4 & \equiv & xy^2z^4P^4, \\ xyzx^4P^4 & \equiv & xyzy^4P^4 & \equiv & xyzz^4P^4 & \equiv & xy^2z^4P^4. \end{array}$$

(ii) *Supposons que $P \in \mathcal{P}$ est un monôme et $\deg P_{[0]} = 1$.*

- *Si $P \in \mathcal{P}_{xy}$, alors $P \equiv \sum Q$ pour certains $Q \leq P$ de la forme xy^{2^n-2} avec $n \geq 2$.*
- *Si $P \in \mathcal{P}_{xyz}$, alors $P \equiv \sum Q$ pour certains $Q \leq P$ de la forme $xy^2z^{2^n-4}$ avec $n \geq 3$.*
- *Si $P \in \mathcal{P}_{xyzt}$ est différent de $x(yzt)^2t^{2^n-8}$ pour tout $n \geq 3$, alors $P \equiv \sum Q$ pour certains $Q \leq P$ qui sont de la forme*

$$x(yzt)^2,\ xy^2z^4t^{2^n-8}\ (n \geq 4).$$

De plus $x(yzt)^2t^{2^n-8} \equiv xy^2z^4t^{2^n-8}$ pour tout $n \geq 4$.

Démonstration (i) Ce lemme résulte des égalités

$$\begin{aligned} x(xyz)^2 &= Sq^2(x^2yz^2) + Sq^1(x^3yz^2 + xyz^4) + xy^2z^4, \\ xyzx^4 &= Sq^2(x^3yz + x^2yz^2) + Sq^1(x^4yz + x^3yz^2 + xyz^4) + xy^2z^4. \end{aligned}$$

(ii) Les deux premières affirmations résultent du Lemme 4.2.2. L'égalité $x(yzt)^2t^{2^n-8} \equiv xy^2z^4t^{2^n-8}$ résultent des Lemmes 4.2.2(ii) et 4.1.4(i).

Raisonnons par l'absurde pour ce qui reste de la troisième affirmation. Supposons qu'il existe des monômes de $\mathcal{P}_{xyzt}$, différents de $x(yzt)^2t^{2^n-8}$ $(n \geq 3)$, qui

ne vérifient pas cette affirmation. Soit P le plus petit d'entre eux pour l'ordre lexicographique. Il est clair que P ne peut s'écrire modulo $\bar{A}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs.

Montrons que $P_{[0]} = x$. Supposons le contraire. Alors $m = \deg_x P$ est pair. Posant $Q := P/x^m$, on a $P = Sq^1(x^{m-1})Q \equiv x^{m-1}Sq^1(Q) < P$. D'où une contradiction.

Montrons que $x^3 \mid P$. Supposons le contraire. Alors $\sqrt{P/x} \in \mathbb{F}_2[y,z,t]$. D'après le Lemme 4.2.2 on a $\sqrt{P/x} \equiv \sum Q$ pour certains monômes $Q \in \mathcal{B}_{yzt}$ vérifiant $Q \leq \sqrt{P/x}$. Par hypothèse sur P, les monômes Q satisfont à $\deg Q_{[0]} = 2$. D'après les Lemmes 4.1.4(i) et 4.1.4(ii) on a $P = x(\sqrt{P/x})^2 \equiv \sum xQ^2 \equiv 0$. D'où une contradiction.

Montrons que $x \mid P_{[1]}$. Supposons le contraire. Alors $m := \deg_x \sqrt{P/x}$ est pair. Posant $Q := \sqrt{P/x}/x^m$, on a $\sqrt{P/x}P = Sq^1(x^{m-1})Q \equiv x^{m-1}Sq^1(Q)$. D'après le Lemme 4.1.4(i) on a $P = x(\sqrt{P/x})^2 \equiv x(x^{m-1}Sq^1(Q))^2 < P$. D'où une contradiction.

Montrons que $\deg P_{[1]}$ est impair. Supposons le contraire. Alors $\alpha(\deg P + \deg P_{[0]}) > \deg P_{[0]} = 1$. D'après le Théorème 4.1.1(ii) on a $P \equiv 0$. D'où une contradiction.

Jusqu'ici $P_{[1]} = x$ ou $P_{[1]} = xuv$ pour certains $u, v \in \{y,z,t\}$. Posons $P =: xP_{[1]}^2y^4Q^4$. Si $P_{[1]} = x$, d'après le Théorème 4.1.1(i) on a $P = Sq^1(x^3Q/y) + x^4Q/y \equiv x^2Sq^2(Q/y) < P$, ce qui est une contradiction. Si $P_{[1]} = xuv$, d'après le Lemme 4.3.1(i) on a $P \equiv xu^2v^4Q^4 < P$, ce qui est une contradiction. □

Lemme 4.3.2 (i) *Soit $P \in \mathcal{P}$ un monôme de degré 8 qui vérifie :* $\deg P_{[0]} \neq 4$ *ou* $\deg P_{[1]} \neq 2$. *Alors, pour tout $u, v, Q \in \mathcal{P}$ tels que* $\deg u = \deg v = 1$, *on a* $Pu^{12}v^4Q^8 \equiv Pu^8v^8Q^8$.

(ii) *Soit* $16 < d \equiv 0 \pmod 4$. *Tout monôme $P \in \mathcal{W}^d \cap \mathcal{P}_{xyzt}$ qui n'est pas de la forme*

$$xy(xzt)^2t^{2^n-8},\ P_{[0]}(yzt)^2t^{2^n-8}\ (n > 4,\ P_{[0]} \in \{xy, xz, xt\})$$

peut s'écrire $P \equiv \sum Q$ pour certains $Q \leq P$ qui sont parmi les suivants :

$$\begin{array}{llll} xyx^2z^4t^{2^n-8}, & xyy^2z^4t^{2^n-8}, & xyz^2t^{2^n-4}, & \\ xzy^2z^4t^{2^n-8}, & xzy^2t^{2^n-4}, & xty^2z^4t^{2^n-8}, & xty^2z^{2^n-4}. \end{array}$$

De plus $xy(xzt)^2t^{2^n-8} \equiv xyx^2z^4t^{2^n-8}$ et $P_{[0]}(yzt)^2t^{2^n-8} \equiv P_{[0]}y^2z^4t^{2^n-8}$ pour tout $n \geq 4$.

Démonstration (i) Supposons d'abord que $P = P_1P_2^4$ pour certains $P_1, P_2 \in \mathcal{P}$ vérifiant $\deg P_1 = 4$. Alors

$$\begin{aligned} Pu^{12}v^4Q^8 &= Sq^4(Pu^{10}v^2Q^8) + Sq^4(P)u^{10}v^2Q^8 + Sq^2(P)Sq^2(u^{10}v^2Q^8) \\ &\equiv (P_1^2P_2^4 + P_1P_2^8)u^{10}v^2Q^8 + PSq^2Sq^2(u^{10}v^2Q^8) \equiv P_1P_2^8u^{10}v^2Q^8 \\ &\equiv Sq^4(P_1P_2^8u^6v^2Q^8) + Sq^4(P_1u^2v^2)P_2^8u^4Q^8 \\ &\equiv \left(P_1^2u^2v^2 + Sq^2(P_1)u^2v^4 + Sq^2(P_1)u^4v^2 + P_1u^4v^4\right)P_2^8u^4Q^8 \\ &\equiv P_1P_2^8u^8v^4Q^8 \equiv \left(Sq^4(P) + P_1^2P_2^4\right)u^8v^4Q^8 \equiv Pu^8v^8Q^8. \end{aligned}$$

Le lemme étant clair si $P_{[0]} = 1$, il reste deux cas à considérer : $\deg P_{[0]} = 4$ ou 2. Si $\deg P_{[0]} = 4$, alors $P_{[1]} = 1$, $\deg P_{[2]} = 1$ et $P = P_{[0]}P_{[2]}^4$ par hypothèse.

Par ce qui précède on a $Pu^{12}v^4Q^8 \equiv Pu^8v^8Q^8$. Si $\deg P_{[0]} = 2$, alors $P_{[0]}$ et $P/P_{[0]}$ ne sont pas premiers entre eux. Pour fixer les idées, supposons $P_{[0]} = xy$ et $\sqrt{P/P_{[0]}} = xR$ avec $\deg R = 2$. Alors $P = Sq^2(x^3yR) + Sq^1(Sq^1(x^3y)R) + (x^4y^2 + x^5y)R$. Ceci implique que

$$P(u^{12}v^4Q^8 + u^8v^8Q^8) \equiv (x^4y^2 + x^5y)R(u^{12}v^4Q^8 + u^8v^8Q^8).$$

On a montré plus haut que $x^4y^2R(u^{12}v^4Q^8 + u^8v^8Q^8) \equiv 0$ et $x^5yR(u^{12}v^4Q^8 + u^8v^8Q^8) \equiv 0$. D'où $Pu^{12}v^4Q^8 \equiv Pu^8v^8Q^8$.

(ii) La deuxième partie du lemme résulte des Lemmes 4.2.2 et 4.1.4(i).

Montrons la première partie. Raisonnons par l'absurde. Supposons qu'il existe des monômes qui ne la vérifient pas. Soit P le plus petit d'entre eux pour l'ordre lexicographique. Il est clair que P ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs.

Montrons que $x^{\deg_x P}y^{\deg_y P} \in \mathcal{B}_{xy}$. Supposons le contraire. Puisque P est minimum, par la χ-technique on a $\deg_x P \equiv 1 \pmod 2$.

- Si $\deg_y P \equiv 0 \pmod 2$, alors d'après le Lemme 4.2.2(i) $x^{\deg_x P}y^{\deg_y P} = \sum Q + \sum \theta(R)$ pour certains $\theta \in \bar{\mathcal{A}}$ et certains $Q, R \in \mathcal{B}_{xy}$ vérifiant $\max(Q,R) < x^{\deg_x P}y^{\deg_y P}$. D'après le Théorème 4.1.1 on a

$$\begin{aligned} P &= \sum Qz^{\deg_z P}t^{\deg_t P} + \sum \theta(R)z^{\deg_z P}t^{\deg_t P} \\ &\equiv \sum Qz^{\deg_z P}t^{\deg_t P} + \sum R\chi(\theta)(z^{\deg_z P}t^{\deg_t P}). \end{aligned}$$

  Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, ce qui est une contradiction.
- Si $\deg_y P \equiv 1 \pmod 2$, alors d'après le Lemme 4.2.2(i)

$$Q_{xy} := \sqrt{x^{\deg_x P - 1}y^{\deg_y P - 1}} = \sum Q + \sum \theta(R)$$

  pour certains $\theta \in \bar{\mathcal{A}}$ et certains $Q, R \in \mathcal{B}_{xy}$ vérifiant $\max(Q,R) \leq Q_{xy}$. Notons que $\deg_z P \equiv \deg_t P \equiv 0 \pmod 2$. En posant $Q_{zt} := \sqrt{z^{\deg_z P}t^{\deg_t P}}$, on a

$$\begin{aligned} P &= xy(Q_{xy}Q_{zt})^2 = xy(\sum QQ_{zt} + \sum \theta(R)Q_{zt})^2 \\ &\equiv xy\big(\sum QQ_{zt} + \sum R\chi(\theta)(Q_{zt})\big)^2 \end{aligned}$$

  d'après le Lemme 4.1.4(i) et le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, ce qui est une contradiction.

Montrons que $\deg P = 2^{n+1}$ pour un certain $n \geq 4$. Supposons le contraire. Alors $\alpha(\deg P + \deg P_{[0]}) > \deg P_{[0]} = 2$. D'après le Théorème 4.1.1(ii) on a $P \equiv 0$. D'où une contradiction.

Posons $P =: P_{[0]}P_{[1]}^2Q^4$. Montrons que $\deg P_{[1]} = 3$. Supposons le contraire. Alors $P_{[1]} = x$ et $P_{[0]} = xy$. Comme P est minimum, d'après les Lemmes 4.3.1 et 4.1.4(i) on a $Q = yz^2t^{2^{n-1}-4}$. Il est facile de vérifier que

$$P = xy(xy^2z^4t^{2^n-8})^2 \equiv xy(xz^2t^{2^n-4} + yz^2t^{2^n-4} + zt^{2^n-2})^2.$$

Ces monômes sont inférieurs à P, d'où une contradiction.

Montrons que $Q \not\equiv 0$. Supposons le contraire $Q = \sum_{i>0} Sq^i(Q_i)$ pour certains $Q_i \in \mathcal{P}$. Alors

$$\begin{aligned} P_{[1]}Q^2 &= \sum_{i>0} P_{[1]}Sq^{2i}(Q_i^2) = \sum_{i>0} \left(Sq^{2i}(P_{[1]}Q_i^2) + Sq^2(P_{[1]})Sq^{2i-1}(Q_i^2)\right) \\ &\equiv \sum_{i>0} Sq^2(P_{[1]})Sq^{2i-1}(Q_i^2). \end{aligned}$$

La 0-ième étage des monômes de cette somme est degré 1. D'après le Lemme 4.3.1(ii), cela implique que $P_{[1]}Q^2 \equiv \sum R$ pour certains $R \leq P_{[1]}Q^2$ qui sont de la forme

$$yz^2t^{2^n-4}, xz^2t^{2^n-4}, xy^2t^{2^n-4}, xy^2z^{2^n-4}, xy^2z^4t^{2^n-8}.$$

Par hypothèse sur P, on vérifie sans difficulté que $R < P_{[1]}Q^2$. D'après le Lemme 4.1.4(i) on a $P = P_{[0]}(P_{[1]}Q^2)^2 \equiv \sum P_{[0]}R^2$. Ces monômes sont inférieurs à P, d'où une contradiction.

Jusqu'ici $\deg P_{[1]} = 3$, $\deg Q_{[0]} = 2$ et $\deg Q_{[1]} \geq 2$. D'où l'existence d'une variable u qui divise $Q_{[0]}$ et $Q_{[1]}$. Posons $Q =: uv(uR)^2$. D'après le Lemme 4.3.2(i) on a $P = P_{[0]}P_{[1]}^2u^{12}v^4R^8 \equiv P_{[0]}P_{[1]}^2u^8v^8Q^8$. Comme $u^2v^2R^2 \equiv 0$, par des arguments analogues à ceux présentés plus haut, on a $P \equiv \sum P_{[0]}R^2$ pour certains $R < P_{[1]}Q^2$ qui sont de la forme

$$yz^2t^{2^n-4}, xz^2t^{2^n-4}, xy^2t^{2^n-4}, xy^2z^{2^n-4}, xy^2z^4t^{2^n-8}.$$

Comme $P_{[0]}R^2 < P$, on aboutit à une contradiction. □

Lemme 4.3.3 *Soit* $16 < d \equiv 2 \pmod 4$. *Tout monôme* $P \in \mathcal{W}^d$ *qui n'est pas de la forme*

$$xy(xz)^2(yzt)^4,\ xy(xyzt)^2t^{2^n-8}\ (n \geq 4),$$

peut s'écrire $P \equiv \sum Q$ *pour certains monômes* $Q \in \mathcal{W}_2 \cup \mathcal{W}_3$ *vérifiant* $Q \leq P$. *De plus* $xy(xyzt)^2t^{2^n-8} \equiv (xy)^3z^4t^{2^n-8} + \sum Q$ *pour certains monômes* $Q \in \mathcal{W}_2 \cup \mathcal{W}_3$ *vérifiant* $Q < xy(xyzt)^2t^{2^n-8}$.

Démonstration La deuxième partie du lemme résulte de l'égalité

$$xy(xyzt)^2t^{2^n-8} \equiv xy(xyz^2 + xzt^2 + xz^2t + yzt^2 + yz^2t + zt^3)^2t^{2^n-8},$$

dont la preuve est laissée au lecteur.

Montrons la première partie. Raisonnons par l'absurde. Supposons qu'il existe des monômes dans $\mathcal{W}^d$, différents de $xy(xz)^2(yzt)^4$ et $xy(xyzt)^2t^{2^n-8}$ $(n > 3)$, qui ne vérifient pas le lemme. Soit P le plus petit d'entre eux pour l'ordre lexicographique. Il est clair que P ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes de $\mathcal{W}$ qui lui sont inférieurs. Par un argument analogue à celui de la démonstration du Lemme 4.3.2(ii), on a $x^{\deg_x P}y^{\deg_y P} \in \mathcal{B}_{xy}$. Soit $s \geq 1$ le plus petit entier vérifiant $\deg P_{[s]} \geq 3$. Posons $Q := \prod_{r>s} P_{[r]}^{2^{r-s-1}}$. À cause du Lemme 4.1.4(i), aucun élément parmi

$$P_{[s]}Q^2,\ P_{[s-1]}P_{[s]}^2Q^4,\ P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8\ (\text{si } s \geq 2)$$

ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes de $\mathcal{W}$ qui lui sont inférieurs.

Cas 1 $s \geq 2$ *et* $x \mid P_{[s]}Q^2$.

Il est clair que $x \mid P_{[r]}$ pour tout $0 \leq r \leq s$.

Montrons que $y \nmid P_{[s-1]}$. Supposons le contraire. Alors $P_{[s-1]} = P_{[s-2]} = xy$. Soit $u \in \{z, t\}$ une variable qui divise $P_{[s]}$. Posant $Q_1 := \prod_{r \geq s} P_{[r]}^{2^{r-s}}/(xu)$, on a

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = Sq^1(x^7y^3u^3Q_1^4) + x^8y^3u^3Q_1^4 + x^7y^4u^3Q_1^4 \\ \equiv\ & x^4\chi(Sq^4)(y^3u^4Q_1^4) + Sq^2(x^7y^2u^3Q_1^4) + x^9y^2u^3Q_1^4 \\ \equiv\ & x^4\chi(Sq^4)(y^3u^4Q_1^4) + x^5\chi(Sq^4)(y^2u^3Q_1^4) \text{ d'après le Théorème 4.1.1(i).} \end{aligned}$$

Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Puisque $y \nmid P_{[s-1]}$, on a $xy \nmid P_{[s]}$. À cause de l'hypothèse $\deg P_{[s]} \geq 3$ on a $P_{[s]} = xzt$.

Montrons que $P_{[s-1]} = xz$. Supposons le contraire. Alors $P_{[s-1]} = xt$ ou x. En posant $Q_1 := \prod_{r \geq s} P_{[r]}^{2^{r-s}}/(xz)$, on a

$$\begin{aligned} & P_{[s-1]}P_{[s]}^2Q^4 = P_{[s-1]}x^2z^2Q_1^2 \\ =\ & Sq^1(x^3(P_{[s-1]}/x)zQ_1^2) + x^4(P_{[s-1]}/x)zQ_1^2 + x^3\,Sq^1(P_{[s-1]}/x)zQ_1^2 \\ \equiv\ & x^2\chi(Sq^2)(P_{[s-1]}zQ_1^2/x) + x^3\,Sq^1(P_{[s-1]}/x)zQ_1^2 \end{aligned}$$

d'après le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-1]}P_{[s]}^2Q^4$, d'où une contradiction.

Montrons que $P_{[s-2]} = xy$. Supposons le contraire. Comme $P \not\equiv 0$, on a $\deg P_{[s-2]} = 2$ d'après le Lemme 4.1.4(ii). D'après le Lemme 4.1.4(iii) la permutation des étages $P_{[s-2]}$ et $P_{[s-1]}$ ne change pas la classe modulo $\bar{A}\mathcal{P}$ de P. Puisque P est minimum, on a $P_{[s-2]} \geq P_{[s-1]} = xz$. D'où $P_{[s-2]} = xz$. Observons que

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = Sq^1(x^7z^7t^3Q^8) + x^8y^7u^3Q^8 + x^7z^8t^3Q^8 \\ \equiv\ & x^8y^7u^3Q^8 + (xt)^3(xz^2Q^2)^4 \equiv x^8y^7u^3Q^8 + (xt)^3\big(Sq^1(xzQ^2) + x^2zQ^2\big)^4 \\ \equiv\ & x^8y^7u^3Q^8 + x^{11}z^4t^3Q^8 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & x^8y^7u^3Q^8 + Sq^1(x^{11}z^3t^3Q^8) + x^{12}z^3t^3Q^8 + x^{11}z^3t^4Q^8 \\ \equiv\ & x^4\chi(Sq^4)(z^7t^3Q^8) + x^6\chi(Sq^6)(z^3t^3Q^8) + x^7\chi(Sq^4)(z^3t^4Q^8), \end{aligned}$$

ceci d'après le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Jusqu'ici $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4 = xy(xz)^2(xzt)^4$. On a

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 \equiv xz(xy)^2(xztQ^2)^4 \text{ d'après le Lemme 4.1.4(iii)} \\ \equiv\ & xz\big(Sq^1(x^3yzt^2Q^4) + x^4yzt^2Q^4 + x^3y^2zt^2Q^4\big)^2 \\ \equiv\ & (x^9y^2z^3t^4 + x^7y^4z^3t^4)Q^8 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & \big(x^9y^2z^3t^4 + Sq^1(x^7y^4z^3t^3) + x^8y^4z^3t^3 + x^7y^4z^4t^3\big)Q^8 \\ \equiv\ & \big(x^9y^2z^3t^4 + x^8y^4z^3t^3 + Sq^2(x^7y^2z^4t^3) + x^9y^2z^4t^3 + x^7y^2z^4t^5\big)Q^8 \\ \equiv\ & \big(x^5\chi(Sq^4)(y^2z^3t^4 + y^2z^4t^3) + x^4\chi(Sq^4)(y^4z^3t^3) + xy(xt)^2(xzt)^4\big)Q^8 \end{aligned}$$

ceci d'après le Théorème 4.1.1(i) et le Lemme 4.1.4(iii). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Cas 2 $s \geq 2$, $x \nmid P_{[s]}Q^2$ *et* $x \mid P_{[s-1]}$.

Il est clair que $P_{[s]} = yzt$ et que $x \mid P_{[r]}$ pour $0 \leq r < s$.

Montrons que $y \nmid P_{[s-1]}$. Supposons le contraire. Alors $P_{[s-1]} = xy$, ce qui implique $P_{[s-2]} = xy$. On a

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = Sq^1(x^3y^7z^3t^4Q^8) + x^4y^7z^3t^4Q^8 + x^3y^8z^3t^4Q^8 \\ \equiv\ & x^2\chi(Sq^2)(y^7z^3t^4Q^8) + (xz)^3(y^2tQ^2)^4 \text{ d'après le Théorème 4.1.1(i)} \\ \equiv\ & x^2\chi(Sq^2)(y^7z^3t^4Q^8) + (xz)^3\big(Sq^1(ytQ^2) + yt^2Q^2\big)^4 \\ \equiv\ & x^2\chi(Sq^2)(y^7z^3t^4Q^8) + (xz)^3(yt^2Q^2)^4 \text{ d'après le Lemme 4.1.4(i).} \end{aligned}$$

Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Montrons que $y \mid P_{[s-2]}$. Supposons le contraire. Posant $\prod_{r\geq s-2} P_{[r]}^{2^{r-s+2}} =: x^3y^4Q_1$, on a

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = Sq^1(x^3y^3Q_1) + x^4y^3Q_1 + x^3y^3Sq^1(Q_1) \\ \equiv\ & x^2\chi(Sq^2)(y^3Q_1) + x^3y^3Sq^1(Q_1) \text{ d'après le Théorème 4.1.1(i).} \end{aligned}$$

Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Montrons que $P_{[s-1]} \neq xt$. Supposons le contraire. On a

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = xy(xy^2z^2t^3Q^4) = xy\big(Sq^1(xy^2zt^3Q^4) + x^2y^2zt^3Q^4\big)^2 \\ \equiv\ & xy(x^2y^2zt^3Q^4)^2 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & xy(zt)^2(xytQ^2)^4 \equiv zt(x^3y^3t^2Q^4)^2 \text{ d'après le Lemme 4.1.4(iii)} \\ \equiv\ & zt\big(Sq^1(x^3y^3tQ^4) + x^4y^3tQ^4 + x^3y^4tQ^4\big)^2 \\ \equiv\ & x^8y^6zt^3Q^8 + x^6y^8zt^3Q^8 \equiv x^2\chi(Sq^4Sq^2)(y^6zt^3Q^8) + x^3y^4\chi(Sq^7)(zt^3Q^8), \end{aligned}$$

ceci d'après le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Montrons que $P_{[s-1]} \neq x$. Supposons le contraire. On a

$$\begin{aligned} & P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = xy(xy^2z^2t^2Q^4) \\ \equiv\ & xy(zx^2y^2t^2Q^4)^2 \text{ d'après les Lemmes 4.3.1(i) et 4.1.4(i)} \\ \equiv\ & \big(Sq^1(xyz) + xzy^2 + yzx^2\big)x^2y^2t^2Q^4 \equiv xz(xy^2t^4Q^4)^2 + yz(xy^2t^4Q^4)^2 \end{aligned}$$

d'après les Lemmes 4.3.1 et 4.1.4(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Jusqu'ici $P_{[s-2]} = xy$ et $P_{[s-1]} = xz$. Montrons que $s = 2$. Supposons le contraire $s \geq 3$. On a montré que $P_{[s-1]} = xz$. Il est clair que $P_{[s-3]} = xy$. Il s'ensuit d'après le Lemme 4.1.4(iv) que

$$P \equiv \prod_{0\leq r<s-3} P_{[r]}^{2^r} \cdot (xy)^{2^{s-3}} \cdot (xz)^{2^{s-2}+2^{s-1}} \cdot \prod_{r\geq s} P_{[r]}^{2^r}.$$

Ce monôme est dans $\mathcal{W}$ et inférieur à P, d'où une contradiction.

On vient d'établir $P = xy(xz)^2(yzt)^4Q^8$. Observons que

$$\begin{aligned}
& P = xy\big(Sq^1(xy^2z^3tQ^4) + x^2y^2z^3tQ^4 + xy^2z^4tQ^4\big)^2\\
\equiv\ & xy(zt)^2(xyzQ^2)^4 + xy(xt)^2(yz^2Q^2)^4 \text{ d'après le Lemme 4.1.4(i)}\\
\equiv\ & zt(xy)^2(xyzQ^2)^4 + xy(xt)^2(yz^2Q^2)^4 \text{ d'après le Lemme 4.1.4(iii)}\\
\equiv\ & zt\big(Sq^1(x^3y^3zQ^4) + x^4y^3zQ^4 + x^3y^4zQ^4\big)^2 + xy(xt)^2(yzQ^2)^4\\
\equiv\ & x^8y^6z^3tQ^8 + x^6y^8z^3tQ^8 + xy(xt)^2(yz^2Q^2)^4 \text{ d'après le Lemme 4.1.4(i)}\\
\equiv\ & x^2\chi(Sq^4Sq^2)(y^6z^3tQ^8) + x^3y^4\chi(Sq^7)(z^3tQ^8) + xy(xt)^2(yz^2Q^2)^4,
\end{aligned}$$

ceci d'après le Théorème 4.1.1(i). Les monômes des deux premiers termes de cette somme sont dans $\mathcal{W}$ et inférieurs à P. Il suit que yz^2Q^2 ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs. D'après le Lemme 4.3.1, cela implique que $Q = z^{2^n-2}$ pour un certain $n \geq 2$. Puisque

$$P = xy(xz)^2(yztz^{2^{n+1}-4})^4 \equiv xy(xz)^2(yz^2t^{2^{n+1}-4})^4$$

d'après les Lemmes 4.3.1(i), 4.1.4(i), et que ce dernier monôme est dans $\mathcal{W}$, inférieur à P, on aboutit à une contradiction.

Cas 3 *$s \geq 2$, $x \nmid P_{[s]}Q^2$ et $x \nmid P_{[s-1]}$.*

Il est clair que $P_{[s]} = yzt$. Comme $P_{[s-1]}P_{[s]}^2Q^4$ ne peut être engendré modulo $\bar{\mathcal{A}}\mathcal{P}$ par les monômes de $\mathcal{W}$ qui lui sont inférieurs, il suit du Lemme 4.2.2(ii) que $Q = 1$ et $P_{[s-1]} = yz$. Comme $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$ ne peut être engendré modulo $\bar{\mathcal{A}}\mathcal{P}$ par les monômes de $\mathcal{W}$ qui lui sont inférieurs, il suit des Lemmes 4.2.2(ii) et 4.1.4(ii) que $x \mid P_{[s-2]}$ et $\deg P_{[s-2]} = 2$.

Montrons que $P_{[s-2]} \neq xt$. Supposons le contraire. On a

$$P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 = xt(yz)^2(yzt)^4 \equiv xy(zt)^2(yzt)^4 + xt(yz)^2(yzt)^4.$$

Ces monômes sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$, d'où une contradiction.

Montrons que $P_{[s-2]} \neq xz$. Supposons le contraire. On a

$$\begin{aligned}
P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8 \equiv\ & yz(xz)^2(yzt)^4 \text{ d'après le Lemme 4.1.4(i)}\\
\equiv\ & yz\big(Sq^1(xyz^3t^2) + x^2yz^3t^2 + xyz^4t^2\big)^2\\
\equiv\ & x^4y^3z^7t^4 + yz(xy)^2(z^2t)^4 \text{ d'après le Lemme 4.1.4(i)}\\
\equiv\ & Sq^1(x^4y^3z^7t^3) + x^4y^4z^7t^3 + x^4y^3z^8t^3 + xy(yz)^2(z^2t)^4\\
\equiv\ & xy^4\chi(Sq^2Sq^1)((z^7t^3) + x^4y^3z^8t^3 + xy^3z^{10}t^4,
\end{aligned}$$

ceci d'après le Lemme 4.1.4(iii) et le Théorème 4.1.1(i). Les monômes de cette somme sauf $x^4y^3z^8t^3$ sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P_{[s-1]}^2P_{[s]}^4Q^8$. Quant à celui-ci, on a

$$\begin{aligned}
& x^4y^3z^8t^3 = yt\big(Sq^1(y^3z^3t) + y^4z^3t + y^3z^3t^2\big)^2\\
\equiv\ & xy(yt)^2t^4z^8 + xt(yt)^2y^4z^8 \text{ d'après les Lemmes 4.1.4(i) et 4.1.4(iii)}\\
\equiv\ & xy^3z^8t^6 + xt\big(Sq^1(y^3z^3t) + y^4z^3t + y^3z^3t^2\big)^2\\
\equiv\ & xy^3z^8t^6 + xy^8z^6t^3 + xy^6z^6t^5 \text{ d'après le Lemme 4.1.4(i)}\\
\equiv\ & xy^3z^8t^6 + xy^4\chi(Sq^4)(z^6t^3) + xy^6z^6t^5 \text{ d'après le Théorème 4.1.1(i).}
\end{aligned}$$

Ces monômes sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P^2_{[s-1]}P^4_{[s]}Q^8$, d'où une contradiction.

Jusqu'ici $P_{[s-2]} = xy$. Observons que

$$\begin{aligned} & P_{[s-2]}P^2_{[s-1]}P^4_{[s]}Q^8 \equiv yz(xy)^2(yzt)^4 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & yz\big(Sq^1(xy^3zt^2) + x^2y^3zt^2 + xy^4zt^2\big)^2 \equiv x^4y^7z^3t^4 + yz(xz)^2(ty^2)^4 \\ \equiv\ & Sq^1(x^4y^7z^3t^3) + x^4y^8z^3t^3 + x^4y^7z^4t^3 + xz(yz)^2(yt^2)^4 \\ \equiv\ & xy^2\chi(Sq^6Sq^3)(z^3t^3) + x^4y^7z^4t^3 + xy^6z^3t^8, \end{aligned}$$

ceci d'après les Lemmes 4.1.4(i), 4.1.4(iii) et le Théorème 4.1.1(i). Les monômes de cette somme sauf $x^4y^7z^4t^3$ sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P^2_{[s-1]}P^4_{[s]}Q^8$. Quant à celui-ci, il s'écrit

$$\begin{aligned} & x^4y^7z^4t^3 = yt\big(Sq^1(xy^3z^2t) + xy^4z^2t + xy^3z^2t^2\big)^2 \\ \equiv\ & yt(xt)^2(zy^2)^4 + yt(xy)^2(yzt)^4 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & xt(yt)^2(yz^2)^4 + xy(yt)^2(yzt)^4 \text{ d'après le Lemme 4.1.4(i) et 4.1.4(iii).} \end{aligned}$$

Ces monômes sont dans $\mathcal{W}$ et inférieurs à $P_{[s-2]}P^2_{[s-1]}P^4_{[s]}Q^8$, d'où une contradiction.

Cas 4 $s = 1$.

Par hypothèse sur $d = \deg P$, on a $3 \leq \deg P_{[1]} \equiv 0 \pmod 2$. D'où $P_{[1]} = xyzt$. Il s'ensuit que $P_{[0]} = xy$. Observons que

$$\begin{aligned} & P = x^3y^3z^2t^2Q^4 = Sq^1(x^3y^3zt^2Q^4) + x^4y^3zt^2Q^4 + x^3y^4zt^2Q^4 \\ \equiv\ & x^2\chi(Sq^2)(y^3zt^2Q^4) + x^3y^4zt^2Q^4 \text{ d'après le Théorème 4.1.1(i).} \end{aligned}$$

Puisque $x^2\chi(Sq^2)(y^3zt^2Q^4) < P$, le monôme $x^3y^4zt^2Q^4$ ne peut être engendré modulo $\bar{\mathcal{A}}\mathcal{P}$ par les monômes de $\mathcal{W}$ inférieurs à P.

Montrons que $x \nmid Q_{[0]}$. Supposons le contraire. On a

$$\begin{aligned} & x^3y^4zt^2Q^4 = xz\big(Sq^1(xytQ^2) + x^2ytQ^2 + xyt^2Q^2\big)^2 \\ \equiv\ & xz(x^4ytQ^2/x^2)^2 + xy(xz)^2(tQ)^4 \text{ d'après les Lemmes 4.1.4(i) et 4.1.4(iii)} \\ \equiv\ & xz\big(x\chi(Sq^2Sq^1)(ytQ^2/x^2)\big)^2 + x^3yz^2t^4Q^4, \end{aligned}$$

ceci d'après le Lemme 4.1.4(i) et le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Montrons que $y \nmid Q_{[0]}$. Supposons le contraire. On a

$$x^3y^4zt^2Q^4 = x^3y^8zt^2Q^4/y^4 \equiv x^3y^4\chi(Sq^4)(zt^2Q^4/y^4)$$

d'après le Théorème 4.1.1(i). Les monômes de celui-ci sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Montrons que $z \nmid Q_{[0]}$ et $t \nmid Q_{[0]}$. Supposons le contraire. Soient u, v des variables telles que $u \mid Q_{[0]}$ et $\{u, v\} = \{z, t\}$. On a

$$\begin{aligned} & x^3y^4zt^2Q^4 = xz(xt)^2(yQ)^4 \equiv xu(xv)^2(yQ)^4 \text{ d'après le Lemme 4.1.4(iii)} \\ \equiv\ & xu\big(Sq^1(xvy^2Q^2/u) + x^2y^2vQ^2/u + xy^2v^2Q^2/u\big)^2 \\ \equiv\ & xu\big(xy\chi(Sq^2)(vQ^2/u)\big)^2 + Sq^1(x^3y^3v^4Q^4/u) + x^4y^3v^4Q^4/u + x^3y^3v^4Q^4 \\ \equiv\ & xu\big(xy\chi(Sq^2)(vQ^2/u)\big)^2 + x^2\chi(Sq^2)(y^3v^4Q^4/u) + x^3y^3v^4Q^4, \end{aligned}$$

ceci d'après le Théorème 4.1.1(i) et le Lemme 4.1.4(i). Les monômes de cette somme sauf $x^3y^3v^4Q^4$ sont dans $\mathcal{W}$ et inférieurs à P. Si $(u,v) = (z,t)$, alors $x^3y^3v^4Q^4$ est également dans $\mathcal{W}$ et inférieur à P, ce qui est une contradiction. D'où $(u,v) = (t,z)$. D'après le Lemme 4.1.4(iv) on a

$$x^3y^3v^4Q^4 = (xy)^3(zt)^4(\sqrt{Q/t})^8 \equiv xy(zt)^6(\sqrt{Q/t})^8 \equiv xyz^6t^2Q^4.$$

Ce monôme est dans $\mathcal{W}$ et inférieur à P, d'où une contradiction.

Puisque $x^{4\deg_x Q+3}y^{4\deg_y Q+3} \in \mathcal{B}_{xy}$, le monôme Q appartient à $\mathbb{F}_2[z,t]$.

Montrons que $z \nmid Q$. Supposons le contraire. On a

$$\begin{aligned}
& P = xz(xy^2tQ^2)^2 = xz\big(Sq^1(xy^2tQ^2/z) + x^2y^2tQ^2/z + xy^2t^2Q^2/z\big)^2 \\
\equiv\ & zt(xz)^2(xyQ/z)^4 + x^3y^4t^4Q^4/z \text{ d'après les Lemmes 4.1.4(i) et 4.1.4(iii)} \\
\equiv\ & zt\big(Sq^1(x^3yQ^2/z) + x^4yQ^2/z + x^3yQ^2\big)^2 \\
& + Sq^1(x^3y^3t^4Q^4/z) + x^4y^3t^4Q^4/z + x^3y^3t^4Q^4 \\
\equiv\ & x^8y^2tQ^4/z + x^6y^2ztQ^4 + x^4y^3t^4Q^4/z + x^3y^3t^4Q^4 \\
\equiv\ & x^2\chi(Sq^4Sq^2)(y^2tQ^4/z) + x^3y\chi(Sq^4)(ztQ^4) + x^2\chi(Sq^2)(y^3t^4Q^4/z) \\
& + x^3y^3t^4Q^4 \text{ d'après le Lemme 4.1.4(i) et le Théorème 4.1.1(i).}
\end{aligned}$$

Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Jusqu'ici $\sqrt{Q} \in \mathbb{F}_2[t]$. Puisque $\sqrt{Q} \notin \mathcal{B}_t$ par hypothèse, on a $\sqrt{Q} \equiv 0$. Il s'ensuit d'après le Lemme 4.1.4(i) que $x^3y^4zt^2Q^4 = xz(xt)^2y^4(\sqrt{Q})^8 \equiv 0$. Ceci est une contradiction. □

Lemme 4.3.4 *Soit $22 < d \equiv 2 \pmod 8$. Tout monôme $P \in \mathcal{W}_2^d$ peut s'écrire $P \equiv \sum Q$ pour certains monômes $Q \leq P$ qui sont de la forme*

$$\begin{cases}
xyR^2, & R \in \mathcal{B}_{xzt} \cup \mathcal{B}_{yzt} \cup \mathcal{B}_{zt}, \\
xzR^2, & R \in \mathcal{B}_{yzt} \cup \mathcal{B}_{yt}, \\
xt(yt)^2z^4R^8, & R \in \mathcal{B}_z \cup \mathcal{B}_t, \\
xy(xz)^2y^4R^8, & R \in \mathcal{B}_t, \\
(xy)^3z^4R^8, & R \in \mathcal{B}_t.
\end{cases}$$

Démonstration Raisonnons par l'absurde. Supposons qu'il existe des monômes de $\mathcal{W}_2^d$ qui ne vérifient le lemme. Soit P le plus petit d'entre eux pour l'ordre lexicographique. Observons que P ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes de $\mathcal{W}$ qui lui sont inférieurs. En effet, ceci résulte du Lemme 4.3.3 et de la minimalité de P. D'où $x^{\deg_x P}y^{\deg_y P} \in \mathcal{B}_{xy}$ par un argument analogue à celui de la démonstration du Lemme 4.3.2(ii).

Posons $Q := \prod_{s>1} P_{[s]}^{2^s}$. D'après le Lemme 4.1.4(i) ni Q, ni $P_{[1]}Q^2$ ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs. Or, à cause de l'hypothèse sur d, on a $\deg Q_{[0]} = 1$. Il s'ensuit d'après le Lemme 4.3.1 que $\deg Q_{[1]} = 1$ et que $Q = Q_{[0]}Q_{[1]}^{2^n-2}$ pour un certain $n \geq 3$.

Supposons $x \mid P_{[1]}$. Alors $P_{[0]} = xy$. Il suit que $P_{[1]}Q^2 \in \mathcal{P}_{xyzt}$. La seule valeur possible de $P_{[1]}$ est $P_{[1]} = xt$. D'où les seules valeurs possibles de $Q_{[0]}, Q_{[1]}$ sont $Q_{[0]} = y$ et $Q_{[1]} = z$. Posant $R := z^{2^{n-1}-2}$, on a

$$\begin{aligned}
P &= xy(xy^2z^4tR^4)^2 = xy\big(Sq^1(xy^2z^3tR^4) + x^2y^2z^3tR^4 + xy^2z^3t^2R^4\big)^2 \\
&\equiv xy\big(xy\chi(Sq^2)(z^3tR^4)\big)^2 + x^3y^5z^6t^4R^8
\end{aligned}$$

d'après le Théorème 4.1.1(i) et le Lemme 4.1.4(i). Ces monômes sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Supposons $x \nmid P_{[1]}$. Alors $P_{[1]}Q^2 \in \mathbb{F}_2[y,z,t]$. La seule valeur possible de $P_{[0]}$ est $P_{[0]} = xt$. Comme $P_{[1]}Q^2$ ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs, d'après le Lemme 4.2.2 la seule valeur possible de $P_{[1]}$ est $P_{[1]} = yz$. On a $P = xt(yz)^2Q^4 \equiv xy(zt)^2Q^4 + xz(yt)^2Q^4$. Ces deux monômes sont dans $\mathcal{W}_2$ et inférieurs à P, d'où une contradiction. □

Lemme 4.3.5 *Soit* $22 < d \equiv 6 \pmod 8$. *Tout monôme* $P \in \mathcal{W}_3^d$ *peut s'écrire* $P \equiv \sum Q$ *pour certains monômes* $Q \leq P$ *qui sont de la forme*

$$\begin{cases} xyR^2, & R \in \mathcal{B}_{zt}, \\ xy(xz)^2R^4, & R \in \mathcal{B}_{xt} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}, \\ xy(xt)^2R^4, & R \in \mathcal{B}_{zt}, \\ xy(yz)^2R^4, & R \in \mathcal{B}_{yt} \cup \mathcal{B}_{zt}, \\ xy(yt)^2R^4, & R \in \mathcal{B}_{zt}, \\ xz(yz)^2R^4, & R \in \mathcal{B}_{zt}, \\ xz(yt)^2R^4, & R \in \mathcal{B}_{yt} \cup \mathcal{B}_{zt}, \\ xt(yt)^2R^4, & R \in \mathcal{B}_{zt}, \\ xy(xz)^2(yt)^4R^8, & R \in \mathcal{B}_{zt} \cup \mathcal{B}_z, \\ xy(xz)^2(yz)^4R^8, & R \in \mathcal{B}_t. \end{cases}$$

Démonstration Appelons "bon" tout monôme qui peut s'écrire de la manière décrite dans l'énoncé du lemme. Appelons "mauvais" tout monôme qui n'est pas "bon". Raisonnons par l'absurde. Supposons qu'il existe des monômes "mauvais" dans $\mathcal{W}_3^d$. Soit P le plus petit d'entre eux pour l'ordre lexicographique. Observons que P ne peut s'écrire modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme des monômes de $\mathcal{W}$ qui lui sont inférieurs. En effet, ceci résulte du Lemme 4.3.3 et de la minimalité de P. D'où $x^{\deg_x P}y^{\deg_y P} \in \mathcal{B}_{xy}$ par un argument analogue à celui de la démonstration du Lemme 4.3.2(ii).

Montrons que $xy \nmid P_{[1]}$. Supposons le contraire. Alors $P_{[0]} = xy$. Puisque P est minimum et que $P = (xy)^3P_{[2]}^4\prod_{s>2}P_{[s]}^{2^s} \equiv xyP_{[2]}^6\prod_{s>2}P_{[s]}^{2^s}$ d'après le Lemme 4.1.4(iv), on a $P_{[2]} \geq xy$. D'où $P_{[2]} = xy$. Posons $zQ := \prod_{s>2}P_{[s]}^{2^{s-3}}$, on obtient que

$$\begin{aligned} P &= Sq^1(x^7y^7z^7Q^8) + x^7y^8z^7Q^8 + x^8y^7z^7Q^8 \\ &\equiv (xz)^3\left(Sq^2(xyzQ^2) + x^2yzQ^2 + xyz^2Q^2\right)^4 + x^8y^7z^7Q^8 \\ &\equiv xz(yz)^6(xQ)^8 + xy(xz)^6(zQ)^8 + x^4\chi(Sq^4)(y^7z^7Q^8) \\ &\equiv x^5\chi(Sq^4)(y^6z^7Q^8) + x^7yz^{14}Q^8 + x^4\chi(Sq^4)(y^7z^7Q^8), \end{aligned}$$

ceci d'après le Théorème 4.1.1(i) et les Lemmes 4.1.4(i), 4.1.4(iv). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Cas 1 $\alpha(\deg_x P) = 1$.

Dans ce cas $P_{[0]} \in \{xy, xz, xt\}$. Comme P est minimum, d'après les Lemmes 4.2.2 et 4.1.4(i) le monôme $Q := \prod_{s>0}P_{[s]}^{2^{s-1}}$ est un élément de $\mathcal{B}_{yzt} \cup \mathcal{B}_{yz} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}$.

Si $P_{[0]} = xy$, en renvoyant au Théorème 4.2.1 pour la forme explicite de $\mathcal{B}_{yzt} \cup \mathcal{B}_{yz} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}$, il suit que les seuls monômes Q qui puissent rendre "mauvais" $P = xyQ^2$ sont ceux de la forme

$$Q = \begin{cases} yz(yt)^2(zR)^4, & R \in \mathbb{F}_2[z,t], \\ (yz)^3(tR)^4, & R \in \mathbb{F}_2[t]. \end{cases}$$

Examinons ces monômes en détail :

(1) Pour $Q = yz(yt)^2(zR)^4$ avec $R \in \mathbb{F}_2[z,t]$, on a

$$\begin{aligned} P &\equiv yz(xy)^2(yt)^4(zR)^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv yz\big(Sq^1(xy^3z^3t^2R^4) + x^2y^3z^3t^2R^4 + xy^4z^3t^2R^4\big)^2 \\ &\equiv x^4y^7z^7t^4R^8 + yz(xz)^2(y^2ztR^2)^4 \text{ d'après le Lemme 4.1.4(i)} \\ &\equiv Sq^1(x^4y^7z^7t^3R^8) + x^4y^8z^7t^3R^8 + x^4y^7z^8t^3R^8 \\ &\quad + xz(yz)^2(y^2ztR^2)^4 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv xy^2\chi(Sq^6Sq^3)(z^7t^3R^8) + xy(yt)^6(zR)^8 + xy^6\chi(Sq^4)(z^7t^4R^8), \end{aligned}$$

ceci d'après le Lemme 4.1.4(iv) et le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

(2) Pour $Q = (yz)^3(tR)^4$ avec $R \in \mathbb{F}_2[t]$, on a

$$\begin{aligned} P &\equiv (yz)^3(xy)^4(tR)^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv Sq^1(x^4y^7z^3t^7R^8) + x^4y^8z^3t^7R^8 + x^4y^7z^4t^7R^8 \\ &\equiv x^4y^8z^3t^7R^8 + Sq^2(x^2y^7z^4t^7R^8) + x^2y^9z^4t^7R^8 + x^2y^7z^4t^9R^8 \\ &\equiv xy^2\chi(Sq^6Sq^3)(z^3t^7R^8) + xt(yt)^2(y^2ztR^2)^4 + xy(yz)^2(yt)^4(tR)^8 \\ &\equiv xy^2\chi(Sq^6Sq^3)(z^3t^7R^8) + xy^6\chi(Sq^4)(z^4t^7R^8) + xy^7z^2t^{12}R^8, \end{aligned}$$

ceci d'après le Lemme 4.1.4(iii) et le Théorème 4.1.1(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Si $P_{[0]} = xz$, en renvoyant au Théorème 4.2.1 pour la forme explicite de $\mathcal{B}_{yzt} \cup \mathcal{B}_{yz} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}$, il suit que les seuls Q qui puissent rendre "mauvais" $P = xzQ^2$ sont ceux de la forme

$$Q = \begin{cases} yz(yt)^2R^4, & R \in \mathbb{F}_2[y,z,t], \\ (yz)^3(tR)^4, & R \in \mathbb{F}_2[t]. \end{cases}$$

En examinant de près, on s'aperçoit que

(1) Pour $Q = yz(yt)^2R^4$ avec $R \in \mathbb{F}_2[y,z,t]$, on a

$$\begin{aligned} P &\equiv xz(yt)^2(yz)^4R^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv (xy(zt)^2 + xt(yz)^2)(yz)^4R^8 \\ &\equiv xy(yz)^2(zt)^4R^8 + (yz)^3(xt)^4R^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv xy(yz)^2(zt)^4R^8 + \big(Sq^1(x^4y^3z^3t^3) + x^4y^4z^3t^3 + x^4y^3z^4t^3\big)R^8 \\ &\equiv xy(yz)^2(zt)^4R^8 + xy(zt)^6R^8 + xz(yt)^6R^8, \end{aligned}$$

ceci d'après le Lemme 4.1.4(iv). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

(2) Pour $Q = (yz)^3(tR)^4$ avec $R \in \mathbb{F}_2[t]$, on a

$$\begin{aligned} P &\equiv (yz)^3(xz)^4(tR)^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv Sq^1(x^4y^3z^7t^7R^8) + x^4y^4z^7t^7R^8 + x^4y^3z^8t^7R^8 \\ &\equiv x^4y^4z^7t^7R^8 + xt(yt)^6(zR)^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv x^4y^4z^7t^7R^8 + xt\big(Sq^1(y^3z^3t^3R^4) + y^4z^3t^3R^4 + y^3z^3t^4R^4\big)^2 \\ &\equiv xy^4\chi(Sq^2Sq^1)(z^7t^7R^8) + xy^4\chi(Sq^4)(z^6t^7R^8) + xy^6z^6t^9R^8, \end{aligned}$$

ceci d'après le Théorème 4.1.1(i) et le Lemme 4.1.4(i). Ces monômes sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Si $P_{[0]} = xt$, en renvoyant encore au Théorème 4.2.1 pour la forme explicite de $\mathcal{B}_{yzt} \cup \mathcal{B}_{yz} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}$, il suit que les seuls Q qui puissent rendre "mauvais" $P = xtQ^2$ sont ceux de la forme $Q = yzR^2$ avec $R \in \mathbb{F}_2[y,z,t]$ et $\deg R_{[0]} = 2$. On a $P = xt(yz)^2R^4 \equiv xy(zt)^2R^4 + xz(yt)^2R^4$. Ces monômes sont inférieurs à P, d'où une contradiction.

Cas 2 $\alpha(\deg_x P) = 2$.

Dans ce cas $P_{[0]}P_{[1]}^2 \in \{xy(xz)^2, xy(xt)^2\}$. Comme P est minimum, d'après les Lemmes 4.2.2 et 4.1.4(i) le monôme $Q := \prod_{s>1} P_{[s]}^{2^{s-1}} \in \mathbb{F}_2[y,z,t]$ est un élément de $\mathcal{B}_{yzt} \cup \mathcal{B}_{yz} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}$.

Si $P_{[0]}P_{[1]}^2 = xy(xz)^2$, en renvoyant au Théorème 4.2.1 pour la forme explicite de $\mathcal{B}_{yzt} \cup \mathcal{B}_{yz} \cup \mathcal{B}_{yt} \cup \mathcal{B}_{zt}$, il suit que les seuls Q qui puissent rendre "mauvais" $P = xy(xz)^2Q^4$ sont ceux de la forme

$$Q = \begin{cases} yz(yt)^2R^4, & R \in \mathbb{F}_2[y,z,t], \\ (yz)^3(tR)^4, & R \in \mathbb{F}_2[t], \\ yzy^2(tR)^4, & R \in \mathbb{F}_2[t], \\ yz(yzt)^2, & \\ yz(zt)^2R^4, & R \in \mathbb{F}_2[z,t], \\ yzz^2(tR)^4, & R \in \mathbb{F}_2[t]. \end{cases}$$

Examinons ces éléments en détail :

(1) Pour $Q = yz(yt)^2R^4$ avec $R \in \mathbb{F}_2[y,z,t]$, ou $Q = (yz)^3(tR)^4$ avec $R \in \mathbb{F}_2[t]$, on a montré plus haut que xzQ^2 s'écrit modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs. D'après le Lemme 4.1.4(i), cela implique que $P = xy(xz)^2Q^4$ s'écrit modulo $\bar{\mathcal{A}}\mathcal{P}$ comme somme de monômes qui lui sont inférieurs. D'où une contradiction.

(2) Pour $Q = yzy^2(tR)^4$ avec $R \in \mathbb{F}_2[t]$, on a

$$\begin{aligned} & P = xy\big(Sq^1(xy^6z^3t^7R^8) + xy^6z^4t^7R^8 + x^2y^6z^3t^7R^8\big)^2 \\ \equiv\ & xy(xt)^2(y^3z^2t^3R^4)^4 + xy(x^2y^6z^3t^7R^8)^2 \text{ d'après le Lemme 4.1.4(i)} \\ \equiv\ & xy(xt)^2\big(Sq^1(y^3zt^3R^4) + y^4zt^3R^4 + y^3zt^4R^4\big)^4 + xy(x^2y^6z^3t^7R^8)^2 \\ \equiv\ & R^{16}\big(x^3yt^2(y^2\chi(Sq^2)(zt^3))^4 + x^3y^{13}z^4t^{18} + xy(xy^3\chi(Sq^4)(z^3t^7))^2\big) \end{aligned}$$

d'après le Théorème 4.1.1(i) et le Lemme 4.1.4(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

(3) Pour $Q = yz(yzt)^2$ on a

$$\begin{aligned} P &= xy\big(Sq^1(xy^6z^7t^3) + xy^6z^8t^3 + x^2y^6z^7t^3\big)^2 \\ &\equiv xy(xt)^2(y^3z^4t)^4 + xy\big(x^2y^6z^7t^3\big)^2 \\ &\equiv xy(xt)^2\big(Sq^1(y^3z^3t) + y^4z^3t + y^3z^3t^2\big)^4 + xy\big(xy^3\chi(Sq^4)(z^7t^3)\big)^2 \\ &\equiv xy(xt)^2\big(y^2\chi(Sq^2)(z^3t)\big)^4 + x^3y^{13}z^{12}t^{10} + x^3y^7\big(\chi(Sq^4)(z^7t^3)\big)^2 \end{aligned}$$

d'après le Théorème 4.1.1 et le Lemme 4.1.4(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

(4) Pour $Q = yz(zt)^2R^4$ avec $R \in \mathbb{F}_2[z,t]$, on a

$$\begin{aligned} & P \equiv xy(zt)^2(xz)^4(yz)^8R^{16} \text{ d'après le Lemme 4.1.4(iii)} \\ \equiv\ & \big(xz(yt)^2 + xt(yz)^2\big)(xz)^4(yz)^8R^{16} \\ \equiv\ & xz(yz)^2(y^3t^3R^4)^4 + (yz)^3(xt)^4(xz)^8R^{16} \text{ d'après le Lemme 4.1.4(iv)} \\ \equiv\ & xy^{14}z^3t^{12}R^{16} + \big(Sq^1(x^{11}y^3z^{11}t^4) + x^{11}y^4z^{11}t^4 + x^{11}y^3z^{12}t^4\big)R^{16} \\ \equiv\ & xz(yz)^2(yt)^{12}R^{16} + xz(yt)^{14}R^{16} + xy(xz)^2(zt)^{12}R^{16}, \end{aligned}$$

ceci d'après le Lemme 4.1.4(iv). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

(5) Pour $Q = yzz^2(tR)^4$ avec $R \in \mathbb{F}_2[t]$, on a

$$\begin{aligned} P &= xy\big(Sq^1(xy^2z^7t^7R^8) + xy^2z^8t^7R^8 + x^2y^2z^7t^7R^8\big)^2 \\ &\equiv xy(xt)^2(yt)^4(z^2tR^2)^8 + xy\big(x^2y^2z^7t^7R^8\big)^2 \\ &\equiv xy(xt)^2(yt)^4\big(Sq^1(ztR^2) + zt^2R^2\big)^8 + xy\big(xy\chi(Sq^2)(z^7t^7R^8)\big)^2 \\ &\equiv xy(xt)^2(yt)^4(zt^2R^2)^8 + x^3y^3\big(\chi(Sq^2)(z^7t^7R^8)\big)^2 \end{aligned}$$

d'après le Lemme 4.1.4(i) et le Théorème 4.1.1. Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Si $P_{[0]}P^2_{[1]} = xy(xt)^2$, alors les seuls monômes Q qui puissent rendre "mauvais" $P = xy(xt)^2Q^4$ sont ceux de la forme

$$Q = \begin{cases} yzR^2, & R \in \mathbb{F}_2[y,z,t], \\ yt(zR)^2, & R \in \mathbb{F}_2[z,t]. \end{cases}$$

Examinons ces éléments en détail :

(1) Pour $Q = yzR^2$ avec $R \in \mathbb{F}_2[y,z,t]$, on a

$$\begin{aligned} P &\equiv xt(yz)^2(xy)^4R^8 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv \big(xy(zt)^2 + xz(yt)^2\big)(xy)^4R^8 \equiv xy(zt)^6R^8 + xy(xz)^2(yt)^4R^8 \end{aligned}$$

d'après le Lemme 4.1.4(iv). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

(2) Pour $Q = yt(zR)^2$ avec $R \in \mathbb{F}_2[z,t]$, on a

$$\begin{aligned} P &= xy\big(Sq^1(xy^2z^3t^3R^4) + x^2y^2z^3t^3R^4 + xy^2z^3t^4R^4\big)^2 \\ &\equiv x^3y^5z^6t^6R^8 + xy(zt)^2(xyztR^2)^4 \text{ d'après le Lemme 4.1.4(i)} \\ &\equiv x^3y^5z^6t^6R^8 + zt(xy)^2(xyztR^2)^4 \text{ d'après le Lemme 4.1.4(iii)} \\ &\equiv x^3y^5z^6t^6R^8 + zt\big(Sq^1(x^3y^3z^2tR^4) + x^4y^3z^2tR^4 + x^3y^4z^2tR^4\big)^2 \\ &\equiv x^3y^5z^6t^6R^8 + x^2\chi(Sq^4Sq^2)(y^6z^5t^3R^8) + x^3y^4\chi(Sq^7)(z^5t^3R^8), \end{aligned}$$

ceci d'après le Théorème 4.1.1(i) et le Lemme 4.1.4(i). Les monômes de cette somme sont dans $\mathcal{W}$ et inférieurs à P, d'où une contradiction.

Cas 3 $\alpha(\deg_x P) \geq 3$.

Comme $xy \nmid P_{[1]}$ et $x^{\deg_x P} y^{\deg_y P} \in \mathcal{B}_{xy}$, on a $P_{[0]} = xy$ et $Q := \prod_{s>0} P_{[s]}^{2^s} \in \mathbb{F}_2[x,z,t]$. Puisque P est minimum, d'après les Lemmes 4.2.2 et 4.1.4(i) on a $Q \in \mathcal{B}_{xzt} \cup \mathcal{B}_{xz} \cup \mathcal{B}_{xt} \cup \mathcal{B}_{zt}$. Les seuls monômes Q qui puissent rendre "mauvais" $P = xyQ^2$ sont ceux de la forme

$$Q = \begin{cases} xz(xt)^2(zR)^4, & R \in \mathbb{F}_2[z,t], \\ (xz)^3(tR)^4, & R \in \mathbb{F}_2[t]. \end{cases}$$

L'examen de ces éléments étant analogue à celui qui était fait au début du Cas 1 (avec les rôles de x et y échangés), on aboutit aussi à une contradiction. □

4.4 Démonstration du Théorème 1.3

(i) Ce théorème résulte trivialement du Théorème 4.1.1(ii).

(ii) Rappelons que

$$\begin{aligned}(\operatorname{Ker}\psi)^d &= \pi(\mathcal{W}^d \cap \mathcal{P}_{xyzt}) \oplus \mathbb{F}_2\langle \pi(\mathcal{B}^d_{xyz} \cup \mathcal{B}^d_{xyt} \cup \mathcal{B}^d_{xzt} \cup \mathcal{B}^d_{yzt} \\ &\quad \cup \mathcal{B}^d_{xy} \cup \mathcal{B}^d_{xz} \cup \mathcal{B}^d_{xt} \cup \mathcal{B}^d_{yz} \cup \mathcal{B}^d_{yt} \cup \mathcal{B}^d_{zt} \cup \mathcal{B}^d_{x} \cup \mathcal{B}^d_{y} \cup \mathcal{B}^d_{z} \cup \mathcal{B}^d_{t})\rangle.\end{aligned}$$

L'ensemble $\mathcal{B}^d_x$ étant vide, cette formule implique que

$$\dim(\operatorname{Ker}\psi)^d = \dim \pi(\mathcal{W}^d \cap \mathcal{P}_{xyzt}) + 4|\mathcal{B}^d_{xyz}| + 6|\mathcal{B}^d_{xy}|.$$

D'après les Lemmes 4.3.2 et 4.3.3, on a $\pi(\mathcal{W}^d \cap \mathcal{P}_{xyzt}) = \pi(\mathcal{W}^d_{\min(p,3)})$. Les Lemmes 4.3.2, 4.3.4, 4.3.5 fournissent un système générateur de $\pi(\mathcal{W}^d_{\min(p,3)})$. En renvoyant au Théorème 4.2.1 pour le cardinal des ensembles $\mathcal{B}_x$, $\mathcal{B}_{xy}$, $\mathcal{B}_{xyz}$, on obtient que

$$\dim(\operatorname{Ker}\psi)^d \leq \begin{cases} 35 & \text{si} \quad p \geq 4 \quad \text{et} \quad q = 0, \\ 70 & \text{si} \quad p \geq 4 \quad \text{et} \quad q = 1, \\ 105 & \text{si} \quad p \geq 3 \quad \text{et} \quad q \geq 2, \\ 90 & \text{si} \quad p = 2 \quad \text{et} \quad q \geq 3, \\ 45 & \text{si} \quad p = 1 \quad \text{et} \quad q \geq 4. \end{cases}$$

D'autre part, observons que

$$\begin{aligned} & \dim(\operatorname{Ker}\psi)^d = \dim(\operatorname{Coker} Sq^0)_d = \dim \Gamma^{\mathcal{A}}_d - \dim Sq^0(\Gamma^{\mathcal{A}}_{d/2-2}) \\ \geq\ & \dim\left(\mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle + Sq^0(\Gamma^{\mathcal{A}}_{d/2-2})\right) - \dim Sq^0(\Gamma^{\mathcal{A}}_{d/2-2}) \\ =\ & \dim \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle - \dim \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle \cap Sq^0(\Gamma^{\mathcal{A}}_{d/2-2}) \\ \geq\ & \dim \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle - \dim \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle \cap \mathcal{W}^{\perp} \\ =\ & \dim \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle / \mathcal{GL}\langle a_1^{(2^{p+q}-1)} a_2^{(2^p-1)}\rangle \cap \mathcal{W}^{\perp}, \end{aligned}$$

et que, d'après le Théorème 1.1 et le Lemme 2.2.4 :

$$\begin{aligned}
&\dim \mathcal{GL}\langle a_1^{(2^{p+q}-1)}a_2^{(2^p-1)}\rangle/\mathcal{GL}\langle a_1^{(2^{p+q}-1)}a_2^{(2^p-1)}\rangle \cap \mathcal{W}^\perp \\
\geq &\begin{cases}
35 & \text{si} \quad p\geq 4 \quad \text{et} \quad q=0,\\
70 & \text{si} \quad p\geq 4 \quad \text{et} \quad q=1,\\
105 & \text{si} \quad p\geq 3 \quad \text{et} \quad q\geq 2,\\
90 & \text{si} \quad p=2 \quad \text{et} \quad q\geq 3,\\
45 & \text{si} \quad p=1 \quad \text{et} \quad q\geq 4.
\end{cases}
\end{aligned}$$

Par ces inégalités, les affirmations concernant $\dim(\operatorname{Ker}\psi)^d$ et $\Gamma_d^{\mathcal{A}}$ sont justifiées. Montrons l'affirmation qui concerne $(\Gamma_d^{\mathcal{A}})_{\mathcal{GL}}$. Si $q\neq 1$ et $p\geq 3$, alors par ce qui précède on a

$$\mathcal{GL}\langle a_1^{(2^{p+q}-1)}a_2^{(2^p-1)}\rangle = \mathbb{F}_2\langle \mathcal{GL}/G_0\rangle,\ \Gamma_d^{\mathcal{A}} = \mathbb{F}_2\langle \mathcal{GL}/G_0\rangle \oplus Sq^0(\Gamma_{d/2-2}^{\mathcal{A}}),$$

où $G_0\subset \mathcal{GL}$ désigne le stabilisateur de $a_1^{(2^{p+q}-1)}a_2^{(2^p-1)}$ pour l'action de $\mathcal{GL}$. Notons que cette somme-ci est une somme directe de $\mathcal{GL}$-modules. D'où

$$(\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} = \mathbb{F}_2\langle \iota^*(a_1^{(2^{p+q}-1)}a_2^{(2^p-1)})\rangle \oplus Sq^0(\Gamma_{d/2-2}^{\mathcal{A}})_{\mathcal{GL}}.$$

Supposons que $q=1$ ou $p\leq 2$. En notant $\gamma := a_1^{(2^{p+q}-1)}a_2^{(2^p-1)}$, montrer $(\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} = Sq^0(\Gamma_{d/2-2}^{\mathcal{A}})_{\mathcal{GL}}$ revient à vérifier que $\iota^*(\gamma)\in Sq^0(\Gamma_{d/2-2}^{\mathcal{A}})_{\mathcal{GL}}$. Soient $g_1,g_2\in\mathcal{GL}$ des matrices satisfaisant à $(a_1g_1,a_2g_1)=(a_2,a_1)$ et $(a_1g_2,a_2g_2)=(a_1+a_2,a_2)$. Pour tout $0\neq v\in\mathbb{F}_2\langle a_2,a_3,a_4\rangle$, soit $g_v\in\mathcal{GL}$ une matrice vérifiant $(a_1g_v,a_2g_v)=(a_1,v)$. Si $q=1$, on a

$$\begin{aligned}
&\iota^*(\gamma) = \iota^*(\gamma+\gamma g_1+\gamma g_2)\\
= \ &\iota^*(a_1^{(2^{p+1}-1)}a_2^{(2^p-1)} + (a_1+a_2)^{(2^{p+1}-1)}a_2^{(2^p-1)} + a_2^{(2^{p+1}-1)}a_1^{(2^p-1)}) = 0.
\end{aligned}$$

Si $p=1$, on a

$$\begin{aligned}
\iota^*(\gamma) &= \iota^*(\gamma+\gamma g_{a_3}+\gamma g_{a_2+a_3})\\
&= \iota^*(a_1^{(2^{q+1}-1)}a_2 + a_1^{(2^{q+1}-1)}a_3 + a_1^{(2^{q+1}-1)}(a_2+a_3)) = 0.
\end{aligned}$$

Si $p=2$, comme $|\mathbb{F}_2\langle a_2,a_3,a_4\rangle|=8$, on a

$$\begin{aligned}
\iota^*(\gamma) &= \iota^*\Big(\sum_{0\neq v\in\mathbb{F}_2\langle a_2,a_3,a_4\rangle}\gamma g_v\Big) = \iota^*\Big(a_1^{(2^{q+2}-1)}\sum_{v\in\mathbb{F}_2\langle a_2,a_3,a_4\rangle}v^{(3)}\Big)\\
&= \iota^*(a_1^{(2^{q+2}-1)}a_2a_3a_4) = Sq^0(\iota^*(a_1^{(2^{q+1}-1)})) \in Sq^0(\Gamma_{d/2-2}^{\mathcal{A}})_{\mathcal{GL}}.
\end{aligned}$$

Ceci achève la démonstration du théorème.

5 Démonstration du Théorème 1.4

5.1 Autour des espaces vectoriels

Somme et produit Soit $(U_i)_{i\in I}$ une famille d'espaces vectoriels. Il existe un morphisme linéaire $\bigoplus_{i\in I}U_i \longrightarrow \prod_{i\in I}U_i$ qui, à chaque somme finie $\sum_{i\in I}u_i$ avec $u_i\in U_i$, fait correspondre $(u_i)_{i\in I}$. Ce morphisme naturel étant injectif (bijectif si I est fini), $\bigoplus_{i\in I}U_i$ s'identifie à un sous-espace vectoriel de $\prod_{i\in I}U_i$.

Structure multiplicative Soient $(U_i)_{i\in I}$, $(V_j)_{j\in J}$, $(W_\ell)_{\ell\in K}$ des familles d'espaces vectoriels. Supposons donnés une fonction $\mu : I \times J \longrightarrow K$ et des morphismes linéaires $f_{ij} : U_i \otimes V_j \longrightarrow W_{\mu(i,j)}$ pour tout $(i,j) \in I \times J$. Pour chaque $\ell \in K$, les f_{ij} avec $(i,j) \in \mu^{-1}(\ell)$ induisent un morphisme linéaire

$$f_\ell^\oplus := \sum_{(i,j)\in\mu^{-1}(\ell)} f_{ij} : \bigoplus_{(i,j)\in\mu^{-1}(\ell)} U_i \otimes V_j \longrightarrow W_\ell.$$

Les $f_\ell^\oplus$ induisent à leur tour un morphisme linéaire

$$f^\oplus = \sum_{\ell\in K} f_\ell^\oplus : (\bigoplus_{i\in I} U_i) \bigotimes (\bigoplus_{j\in J} V_j) = \bigoplus_{\ell\in K} \bigoplus_{(i,j)\in\mu^{-1}(\ell)} U_i \otimes V_j \longrightarrow \bigoplus_{\ell\in K} W_\ell.$$

Les projections canoniques $\prod_{i\in I} U_i \longrightarrow U_i$ et $\prod_{j\in J} V_j \longrightarrow V_j$ forment un morphisme linéaire $(\prod_{i\in I} U_i) \otimes (\prod_{j\in J} V_j) \longrightarrow \prod_{(i,j)\in\mu^{-1}(\ell)} U_i \otimes V_j$ pour tout $\ell \in K$. Supposons, pour chaque $\ell \in K$, qu'il n'y a qu'un nombre fini de couples $(i,j) \in \mu^{-1}(\ell)$ vérifiant $U_i \otimes V_j \neq 0$. Les sommes et produits finis étant les mêmes, on obtient un morphisme linéaire

$$f_\ell^\Pi : (\prod_{i\in I} U_i) \bigotimes (\prod_{j\in J} V_j) \longrightarrow \prod_{(i,j)\in\mu^{-1}(\ell)} U_i \otimes V_j = \bigoplus_{(i,j)\in\mu^{-1}(\ell)} U_i \otimes V_j \longrightarrow W_\ell,$$

où la seconde flèche est $f_\ell^\oplus$. Les f_ℓ^Π forment un morphisme linéaire

$$f^\Pi = (f_\ell^\Pi)_{\ell\in K} : (\prod_{i\in I} U_i) \bigotimes (\prod_{j\in J} V_j) \longrightarrow \prod_{\ell\in K} W_\ell.$$

Le lien entre f^Π et $f^\oplus$ est le suivant : sous l'hypothèse qu'il n'y a qu'un nombre fini de couples $(i,j) \in \mu^{-1}(\ell)$ vérifiant $U_i \otimes V_j \neq 0$ (ceci pour tout $\ell \in K$), on le diagramme commutatif

$$\begin{array}{ccc} (\bigoplus_{i\in I} U_i) \bigotimes (\bigoplus_{j\in J} V_j) & \xrightarrow{f^\oplus} & \bigoplus_{\ell\in K} W_\ell \\ \downarrow & & \downarrow \\ (\prod_{i\in I} U_i) \bigotimes (\prod_{j\in J} V_j) & \xrightarrow{f^\Pi} & \prod_{\ell\in K} W_\ell \end{array}$$

où les flèches verticales sont les inclusions.

Voici un exemple de structure multiplicative. Soient $(U_i)_{i\geq N}$ une famille d'espaces vectoriels indexée par les entiers $i \geq N$, et $f_{ij} : U_i \otimes U_j \longrightarrow U_{i+j}$ des morphismes linéaires. Les f_{ij} induisent un morphisme linéaire

$$f^\oplus : (\bigoplus_{i\geq N} U_i) \bigotimes (\bigoplus_{i\geq N} U_i) \longrightarrow \bigoplus_{i\geq N} U_i.$$

Par ce qui précède, il existe un morphisme linéaire

$$f^\Pi : (\prod_{i\geq N} U_i) \bigotimes (\prod_{i\geq N} U_i) \longrightarrow \prod_{i\geq N} U_i$$

qui rend commutatif le diagramme

$$\begin{array}{ccc} (\bigoplus_{i\geq N} U_i)\bigotimes(\bigoplus_{i\geq N} U_i) & \xrightarrow{f^{\oplus}} & \bigoplus_{i\geq N} U_i \\ \downarrow & & \downarrow \\ (\prod_{i\geq N} U_i)\bigotimes(\prod_{i\geq N} U_i) & \xrightarrow{f^{\Pi}} & \prod_{i\geq N} U_i \end{array}$$

Si $\bigoplus_{i\geq N} U_i$ est un anneau avec $f^{\oplus}$ comme multiplication, alors $\prod_{i\geq N} U_i$ est un anneau avec f^{Π} comme multiplication, et $\bigoplus_{i\geq N} U_i \longrightarrow \prod_{i\geq N} U_i$ est une inclusion d'anneaux. L'anneau $\prod_{i\geq N} U_i$ est unitaire ou commutatif (ou les deux) suivant que l'est l'anneau $\bigoplus_{i\geq N} U_i$. L'exemple le plus familier de cette généralité est l'inclusion $\mathbb{F}_2[X] = \bigoplus_{i\geq 0} \mathbb{F}_2 X^i \longrightarrow \mathbb{F}_2[[X]] = \prod_{i\geq 0} \mathbb{F}_2 X^i$ de l'anneau des polynômes dans l'anneau des séries formelles.

Un autre exemple de structure multiplicative s'obtient comme suit. Soient $(U_i)_{i\in\mathbb{Z}}$, $(V_j)_{j\in\mathbb{Z}}$ des familles d'espaces vectoriels avec $U_i = V_j = 0$ si $\max(i,j) < N$ pour un certain $N \in \mathbb{Z}$, et $f_{ij}^U : U_i \otimes U_j \longrightarrow U_{i+j}$, $f_{ij}^V : V_i \otimes V_j \longrightarrow V_{i+j}$ des morphismes linéaires. Soient $(E_\ell)_{\ell\in\mathbb{Z}}$ une famille de sous-ensembles de $\mathbb{Z}\times\mathbb{Z}$ qui vérifient : si $(i_1,j_1) \in E_{\ell_1}$ et $(i_2,j_2) \in E_{\ell_2}$, alors $(i_1+i_2, j_1+j_2) \in E_{\ell_1+\ell_2}$ (exemple : prenons pour E_ℓ l'ensemble des couples d'entiers (i,j) vérifiant $j-i=\ell$). Les f_{ij}^U, f_{ij}^V induisent un morphisme linéaire $f_{\ell_1\ell_2}^{\oplus} : (\bigoplus_{(i_1,j_1)\in E_{\ell_1}} U_{i_1}\otimes V_{j_1})\bigotimes(\bigoplus_{(i_2,j_2)\in E_{\ell_2}} U_{i_2}\otimes V_{j_2}) \longrightarrow \bigoplus_{(i,j)\in E_{\ell_1+\ell_2}} U_i\otimes V_j$ pour chaque $(\ell_1,\ell_2) \in \mathbb{Z}\times\mathbb{Z}$. Par ce qui précède, il existe pour chaque $(\ell_1,\ell_2) \in \mathbb{Z}\times\mathbb{Z}$ un morphisme linéaire

$$f_{\ell_1\ell_2}^{\Pi} : (\prod_{E_{\ell_1}} U_{i_1}\otimes V_{j_1})\bigotimes(\prod_{E_{\ell_2}} U_{i_2}\otimes V_{j_2}) \longrightarrow \prod_{E_{\ell_1+\ell_2}} U_i\otimes V_j$$

qui rend commutatif le diagramme

$$\begin{array}{ccc} (\bigoplus_{E_{\ell_1}} U_{i_1}\otimes V_{j_1})\bigotimes(\bigoplus_{E_{\ell_2}} U_{i_2}\otimes V_{j_2}) & \xrightarrow{f_{\ell_1\ell_2}^{\oplus}} & \bigoplus_{E_{\ell_1+\ell_2}} U_i\otimes V_j \\ \downarrow & & \downarrow \\ (\prod_{E_{\ell_1}} U_{i_1}\otimes V_{j_1})\bigotimes(\prod_{E_{\ell_2}} U_{i_2}\otimes V_{j_2}) & \xrightarrow{f_{\ell_1\ell_2}^{\Pi}} & \prod_{E_{\ell_1+\ell_2}} U_i\otimes V_j \end{array}$$

En notant $f^{\oplus} = \bigoplus_{\ell_1,\ell_2} f_{\ell_1\ell_2}^{\oplus}$ et $f^{\Pi} = \bigoplus_{\ell_1,\ell_2} f_{\ell_1\ell_2}^{\Pi}$, on obtient le diagramme commutatif

$$\begin{array}{ccc} (\bigoplus_\ell \bigoplus_{E_\ell} U_i\otimes V_j)\bigotimes(\bigoplus_\ell \bigoplus_{E_\ell} U_i\otimes V_j) & \xrightarrow{f^{\oplus}} & \bigoplus_\ell \bigoplus_{E_\ell} U_i\otimes V_j \\ \downarrow & & \downarrow \\ (\bigoplus_\ell \prod_{E_\ell} U_i\otimes V_j)\bigotimes(\bigoplus_\ell \prod_{E_\ell} U_i\otimes V_j) & \xrightarrow{f^{\Pi}} & \bigoplus_\ell \prod_{E_\ell} U_i\otimes V_j \end{array}$$

Si $(\bigoplus_\ell \bigoplus_{E_\ell} U_i\otimes V_j, f^{\oplus})$ est un anneau, alors $(\bigoplus_\ell \prod_{E_\ell} U_i\otimes V_j, f^{\Pi})$ est un anneau, et $\bigoplus_\ell \bigoplus_{E_\ell} U_i\otimes V_j \longrightarrow \bigoplus_\ell \prod_{E_\ell} U_i\otimes V_j$ est une inclusion d'anneaux. L'anneau $\bigoplus_\ell \prod_{E_\ell} U_i\otimes V_j$ est unitaire ou commutatif (ou les deux) suivant que l'est l'anneau $\bigoplus_\ell \bigoplus_{E_\ell} U_i\otimes V_j$. L'exemple typique que nous voulons signaler à

ce propos est l'inclusion d'anneaux

$$\mathcal{P} \otimes \mathcal{A}^* = \bigoplus_{\ell} \bigoplus_{j-i=\ell} \mathcal{P}^j \otimes \mathcal{A}_i^* \longrightarrow \bigoplus_{\ell} \prod_{j-i=\ell} \mathcal{P}^j \otimes \mathcal{A}_i^*,$$

avec $\mathcal{P}$ pour l'algèbre polynomiale mentionnée dans le Section 1, et $\mathcal{A}^*$ pour l'algèbre de Steenrod duale. Cet exemple surgit de notre étude de la coaction de Milnor. Nous y reviendrons au paragraphe sur le produit tensoriel complété.

Dual et accouplement canonique Soit V un espace vectoriel. Son dual V^* est, par définition, l'espace vectoriel des formes linéaires $V \longrightarrow \mathbb{F}_2$. L'accouplement canonique etre V et V^* est la fonction $\langle *, * \rangle : V^* \times V \longrightarrow \mathbb{F}_2$ qui fait correspondre à chaque couple $(f_V, v) \in V^* \times V$ le scalaire $\langle f_V, v \rangle := f_V(v)$.

Soient U, V des espaces vectoriels et $f : U \longrightarrow V$ un morphisme linéaire. Le morphisme dual $f^* : V^* \longrightarrow U^*$ fait correspondre à chaque $f_V \in V^*$ la forme linéaire $U \longrightarrow \mathbb{F}_2$, $u \longmapsto \langle f_V, f(u) \rangle$.

Soit $(U_i)_{i \in I}$ une famille d'espaces vectoriels. Les morphismes duaux des inclusions $U_i \longrightarrow \bigoplus_{i \in I} U_i$ forment un morphisme linéaire

$$(\bigoplus_{i \in I} U_i)^* \longrightarrow \prod_{i \in I} U_i^*.$$

Celui-ci est un isomorphisme. Par contre, il en est tout autrement de son analogue $\bigoplus_{i \in I} U_i^* \longrightarrow (\prod_{i \in I} U_i)^*$, induit par les morphismes duaux des projections canoniques $\prod_{i \in I} U_i \longrightarrow U_i$. Cet analogue est injectif, voire bijectif si I est fini, mais n'est pas surjectif en général.

Cas gradué On définit un espace vectoriel gradué comme étant la somme directe d'une famille d'espaces vectoriels indexée par l'ensemble des entiers $\mathbb{Z}$. Si $V = \bigoplus_{n \in \mathbb{Z}} V^n$ est un espace vectoriel gradué dont la graduation s'écrit traditionellement en haut (comme la cohomologie), on peut également écrire celle-ci en bas en posant $V_n := V^{-n}$ pour tout $n \in \mathbb{Z}$. Inversement, si $V = \bigoplus_{n \in \mathbb{Z}} V_n$ est un espace vectoriel gradué dont la graduation s'écrit traditionellement en bas (comme l'homologie), on peut également écrire celle-ci en haut en posant $V^n := V_{-n}$ pour tout $n \in \mathbb{Z}$. Suivant le contexte, le degré des éléments de $V_n = V^{-n}$ est n ou $-n$.

Soit $V = \bigoplus_{n \in \mathbb{Z}} V^n$ un espace vectoriel gradué. Son dual $V^* = \bigoplus_{n \in \mathbb{Z}} (V^*)^n$ est défini par $(V^*)^n := (V^{-n})^*$ pour tout $n \in \mathbb{Z}$. Si l'on veut écrire la graduation en bas, on aura $(V^*)_n = (V^*)^{-n} = (V^n)^*$. L'accouplement canonique entre V^* et V est défini par

$$\langle f, v \rangle = \begin{cases} 0 & \text{si} \quad f \in (V^*)_m,\ v \in V^n,\ m \neq n, \\ f(v) & \text{si} \quad f \in (V^*)_n,\ v \in V^n,\ n \in \mathbb{Z}. \end{cases}$$

Dual du dual Soit V un espace vectoriel (gradué ou non). Il existe un morphisme linéaire $V \longrightarrow (V^*)^*$ qui envoie $v \in V$ sur la forme linéaire $V^* \longrightarrow \mathbb{F}_2$, $f \longmapsto \langle f, v \rangle$. Ce morphisme naturel est injectif, mais n'est pas surjectif en général. Il est bijectif si V est de dimension finie, ou de type fini (i.e. gradué et de dimension finie en chaque degré).

Dual d'un produit tensoriel Soient U, V des espaces vectoriels (gradués ou non). Il existe un morphisme linéaire $U^* \otimes V^* \longrightarrow (U \otimes V)^*$ qui envoie $f_U \otimes f_V \in U^* \otimes V^*$ sur la forme linéaire $U \otimes V \longrightarrow \mathbb{F}_2$, $u \otimes v \longmapsto \langle f_U, u\rangle \cdot \langle f_V, v\rangle$. Ce morphisme naturel est injectif, mais n'est pas surjectif en général. Il est bijectif si U et V sont de dimension finie, ou de type fini.

Produit tensoriel complété Soient U, V des espaces vectoriels (gradués ou non). On définit le produit tensoriel complété $U \widehat{\otimes} V$ comme étant $(U^* \otimes V^*)^*$. Il existe un morphisme linéaire $U \otimes V \longrightarrow U \widehat{\otimes} V$ qui envoie $u \otimes v \in U \otimes V$ sur la forme linéaire $U^* \otimes V^* \longrightarrow \mathbb{F}_2$, $f_U \otimes f_V \longmapsto \langle f_U, u\rangle \cdot \langle f_V, v\rangle$. Ce morphisme naturel est injectif et coïncide avec la composée $U \otimes V \longrightarrow ((U \otimes V)^*)^* \longrightarrow (U^* \otimes V^*)^*$ des morphismes mentionnés plus haut. Dans le cas non gradué, il est bijectif si U et V sont de dimension finie, mais n'est pas surjectif en général. Dans le cas gradué, il n'est même pas bijectif lorsque U et V sont de type fini. L'exemple suivant élucide ce point.

Soient $U = \bigoplus_{n\in\mathbb{Z}} U^n$ et $V = \bigoplus_{n\in\mathbb{Z}} V_n$ des espaces vectoriels gradués de type fini. Alors $(U \otimes V)^n = \bigoplus_{i\in\mathbb{Z}} U^{i+n} \otimes V^{-i} = \bigoplus_{i\in\mathbb{Z}} U^{i+n} \otimes V_i$, tandis que

$$\begin{aligned}
(U \widehat{\otimes} V)^n &= ((U^* \otimes V^*)^*)^n = ((U^* \otimes V^*)^{-n})^* \\
&= \Big(\bigoplus_{i\in\mathbb{Z}} (U^*)^{-i-n} \otimes (V^*)^i\Big)^* = \Big(\bigoplus_{i\in\mathbb{Z}} (U^{i+n})^* \otimes (V^{-i})^*\Big)^* \\
&= \prod_{i\in\mathbb{Z}} ((U^{i+n})^*)^* \otimes ((V^{-i})^*)^* = \prod_{i\in\mathbb{Z}} U^{i+n} \otimes V_i.
\end{aligned}$$

Voici un cas particulier de cette situation. Soit $\mathcal{A} \otimes \mathcal{P} \longrightarrow \mathcal{P}$ l'action de l'algèbre de Steenrod sur l'algèbre polynomiale $\mathcal{P}$ (cf. la Section 3.1). Cette action se transpose en un morphisme linéaire $\lambda^* : \mathcal{P}^* \otimes \mathcal{A} \longrightarrow \mathcal{P}^*$ qui vérifie $\langle \lambda^*(P^* \otimes \theta), P\rangle = \langle P^*, \theta(P)\rangle$ pour tout $P^* \in \mathcal{P}^*$, $\theta \in \mathcal{A}$ et $P \in \mathcal{P}$. En dualisant, on obtient un morphisme linéaire $\lambda : P \longrightarrow (\mathcal{P}^* \otimes \mathcal{A})^* = \mathcal{P} \widehat{\otimes} \mathcal{A}^*$ qui s'appelle la coaction de Milnor [33, 46]. Rappelons

- que $\mathcal{P} \otimes \mathcal{A}^* = \bigoplus_{n\in\mathbb{Z}} \bigoplus_{i\in\mathbb{Z}} \mathcal{P}^{i+n} \otimes \mathcal{A}_i^*$ est naturellement un anneau,
- que, par ce qui précède, $\mathcal{P} \widehat{\otimes} \mathcal{A}^* = \bigoplus_{n\in\mathbb{Z}} \prod_{i\in\mathbb{Z}} \mathcal{P}^{i+n} \otimes \mathcal{A}_i^*$ est naturellement un anneau, et que $\mathcal{P} \otimes \mathcal{A}^* \longrightarrow \mathcal{P} \widehat{\otimes} \mathcal{A}^*$ est une inclusion d'anneaux.

Étant donné $P \in \mathcal{P}^n$, en notant $\lambda(P) = \sum_{i\in\mathbb{Z}} P_{i+n} \otimes \theta_i^*$ avec $P_{i+n} \in \mathcal{P}^{i+n}$ et $\theta_i^* \in \mathcal{A}_i^*$ (ceci est un abus de notation, car il s'agit d'une somme infinie), on a la formule $\langle P^*, \theta(P)\rangle = \langle P^* \otimes \theta, \lambda(P)\rangle = \sum_{i\in\mathbb{Z}} \langle P^*, P_{i+n}\rangle \cdot \langle \theta, \theta_i^*\rangle$ pour tout $P^* \in \mathcal{P}^*$ et $\theta \in \mathcal{A}$ (cette somme est bien finie). Grâce à cette formule, on peut montrer que $\lambda : \mathcal{P} \longrightarrow \mathcal{P} \widehat{\otimes} \mathcal{A}^*$ est un morphisme d'anneaux. En effet, soient $P_1 \in \mathcal{P}^{n_1}$, $P_2 \in \mathcal{P}^{n_2}$, $P^* \in \mathcal{P}^*$ et $\theta \in \mathcal{A}$. Notons Δ, $\delta_{\mathcal{P}^*}$ la comultiplication de $\mathcal{A}$, $\mathcal{P}^*$ respectivement. Supposons que

$$\left\{\begin{array}{lcllll}
\Delta(\theta) & = & \sum_{\theta_1,\theta_2} \theta_1 \otimes \theta_2, & \theta_1 \in \mathcal{A}, & & \theta_2 \in \mathcal{A}, \\
\delta_{\mathcal{P}^*}(P^*) & = & \sum_{P_1^*,P_2^*} P_1^* \otimes P_2^*, & P_1^* \in \mathcal{P}^*, & & P_2^* \in \mathcal{P}^*, \\
\lambda(P_1) & = & \sum_{i_1\in\mathbb{Z}} P_{1,i_1+n_1} \otimes \theta_{1,i_1}^*, & P_{1,i_1+n_1} \in \mathcal{P}^{i_1+n_1}, & \theta_{1,i_1}^* \in \mathcal{A}_{i_1}^*, \\
\lambda(P_2) & = & \sum_{i_2\in\mathbb{Z}} P_{2,i_2+n_2} \otimes \theta_{2,i_2}^*, & P_{2,i_2+n_2} \in \mathcal{P}^{i_2+n_2}, & \theta_{2,i_2}^* \in \mathcal{A}_{i_2}^*.
\end{array}\right.$$

D'après la formule de Cartan on a

$$\begin{aligned}
&\langle P^* \otimes \theta, \lambda(P_1P_2)\rangle = \langle P^*, \theta(P_1P_2)\rangle = \langle P^*, \sum_{\theta_1,\theta_2} \theta_1(P_1)\theta_2(P_2)\rangle \\
= \;& \langle \delta_{\mathcal{P}^*}(P^*), \sum_{\theta_1,\theta_2} \theta_1(P_1)\otimes\theta_2(P_2)\rangle = \sum_{P_1^*,P_2^*}\sum_{\theta_1,\theta_2} \langle P_1^*, \theta_1(P_1)\rangle \cdot \langle P_2^*, \theta_2(P_2)\rangle \\
= \;& \sum_{P_1^*,P_2^*}\sum_{\theta_1,\theta_2}\sum_{i_1\in\mathbb{Z}}\sum_{i_2\in\mathbb{Z}} \langle P_1^*, P_{1,i_1+n_1}\rangle \cdot \langle \theta_1, \theta_{1,i_1}^*\rangle \cdot \langle P_2^*, P_{2,i_2+n_2}\rangle \cdot \langle \theta_2, \theta_{2,i_2}^*\rangle \\
= \;& \sum_{i_1\in\mathbb{Z}}\sum_{i_2\in\mathbb{Z}}\sum_{P_1^*,P_2^*}\sum_{\theta_1,\theta_2} \langle P_1^*\otimes P_2^*, P_{1,i_1+n_1}\otimes P_{2,i_2+n_2}\rangle \cdot \langle \theta_1\otimes\theta_2, \theta_{1,i_1}^*\otimes\theta_{2,i_2}^*\rangle \\
= \;& \sum_{i_1\in\mathbb{Z}}\sum_{i_2\in\mathbb{Z}} \langle \delta_{\mathcal{P}^*}(P^*), P_{1,i_1+n_1}\otimes P_{2,i_2+n_2}\rangle \cdot \langle \Delta(\theta), \theta_{1,i_1}^*\otimes\theta_{2,i_2}^*\rangle \\
= \;& \sum_{i_1\in\mathbb{Z}}\sum_{i_2\in\mathbb{Z}} \langle P^*, P_{1,i_1+n_1}P_{2,i_2+n_2}\rangle \cdot \langle \theta, \theta_{1,i_1}^*\theta_{2,i_2}^*\rangle \\
= \;& \sum_{i_1\in\mathbb{Z}}\sum_{i_2\in\mathbb{Z}} \langle P^*\otimes\theta, P_{1,i_1+n_1}P_{2,i_2+n_2}\otimes\theta_{1,i_1}^*\theta_{2,i_2}^*\rangle = \langle P^*\otimes\theta, \lambda(P_1)\lambda(P_2)\rangle.
\end{aligned}$$

D'où $\lambda(P_1P_2) = \lambda(P_1)\lambda(P_2)$, ce qu'il fallait démontrer.

Pour résumer, disons

- que $\mathcal{P}\widehat{\otimes}\mathcal{A}^* = \bigoplus_{n\in\mathbb{Z}}\prod_{i\in\mathbb{Z}}\mathcal{P}^{i+n}\otimes\mathcal{A}_i^*$ admet une structure naturelle d'anneau qui étend celle de $\mathcal{P}\otimes\mathcal{A}^* = \bigoplus_{n\in\mathbb{Z}}\bigoplus_{i\in\mathbb{Z}}\mathcal{P}^{i+n}\otimes\mathcal{A}_i^*$,
- que tout élément $(P_{i+n}\otimes\theta_i^*)_{i\in\mathbb{Z}} \in (\mathcal{P}\widehat{\otimes}\mathcal{A}^*)^n = \prod_{i\in\mathbb{Z}}\mathcal{P}^{i+n}\otimes\mathcal{A}_i^*$ est noté $\sum_{i\in\mathbb{Z}} P_{i+n}\otimes\theta_i^*$ par abus de notation,
- que $\lambda : P \longrightarrow \mathcal{P}\widehat{\otimes}\mathcal{A}^*$ est un morphisme d'anneaux,
- que si $P^* \in \mathcal{P}^*$, $\theta\in\mathcal{A}$, $P\in\mathcal{P}^n$ et $\lambda(P) = \sum_{i\in\mathbb{Z}} P_{i+n}\otimes\theta_i^*$ avec $P_{i+n}\in\mathcal{P}^{i+n}$ et $\theta_i^*\in\mathcal{A}_i^*$, alors

$$\langle P^*, \theta(P)\rangle = \langle P^*\otimes\theta, \lambda(P)\rangle = \sum_{i\in\mathbb{Z}}\langle P^*, P_{i+n}\rangle\cdot\langle\theta,\theta_i^*\rangle.$$

Des exemples de calcul avec la coaction de Milnor seront donnés dans la Section 5.2. C'était Schwartz [46] qui nous a signalé le point "subtil" des arguments utilisant la coaction de Milnor (il s'agit des sommes infinies), point non élucidé dans l'article original de Milnor [33].

Suspension Soit $V = \bigoplus_{n\in\mathbb{Z}} V_n$ un espace vectoriel gradué. Pour $m\in\mathbb{Z}$, la suspension m-ième de V, noté $\Sigma^m V$, est l'espace vectoriel gradué défini par $(\Sigma^m V)_n := V_{n-m}$ $(n\in\mathbb{Z})$. Si $v\in V_{n-m}$, l'élément dans $(\Sigma^m V)_n$ qui lui correspond est noté $\Sigma^m v$.

Soient U, V des espaces vectoriels gradués et $f : U\longrightarrow V$ un morphisme. On note $\Sigma^m f$ le morphisme $\Sigma^m U\longrightarrow\Sigma^m V$, $\Sigma^m u\longmapsto\Sigma^m f(u)$.

Soit V est un $\mathcal{A}$-module à gauche. Alors $\Sigma^m V$ l'est également. L'action de $\mathcal{A}$ sur $\Sigma^m V$ est définie par la formule $\theta(\Sigma^m v) := \Sigma^m(\theta v)$, $v\in V$, $\theta\in\mathcal{A}$.

5.2 Transfert et bar-résolution

Extensions Soient $\mathcal{P}_1 = \mathbb{F}_2[x_1]$ et $\mathcal{L}_1 := x_1^{-1}\mathcal{P}_1 \subset \mathbb{F}_2[x_1^{\pm 1}]$. D'après [54], l'action naturelle de $\mathcal{A}$ sur $\mathcal{P}_1$ s'étend à $\mathcal{L}_1$ et fait de ce dernier un $\mathcal{A}$-module.

On a la suite exacte courte de $\mathcal{A}$-modules

$$0 \longrightarrow \Sigma\mathcal{P}_1 \xrightarrow{\iota_1} \Sigma\mathcal{L}_1 \xrightarrow{\pi_1} \mathbb{F}_2 \longrightarrow 0,$$

où ι_1 est l'inclusion et $\pi_1(\Sigma x_1^{i_1}) = \begin{cases} 1 & \text{si } i_1 = -1, \\ 0 & \text{si } i_1 \geq 0. \end{cases}$

Singer [49] et Lannes–Zarati [23] considèrent l'élément $e_1 \in Ext_{\mathcal{A}}(\mathbb{F}_2, \Sigma\mathcal{P}_1)$ correspondant à cette courte suite. Observant l'isomorphisme de $\mathcal{A}$-modules $(\Sigma\mathcal{P}_1)^{\otimes k} \cong \Sigma^k\mathcal{P}$, ils définissent $e_k := e_1^{\otimes k} \in Ext_{\mathcal{A}}(\mathbb{F}_2, \Sigma^k\mathcal{P})$. En termes de la bar-résolution [26] de l'algèbre de Steenrod, e_k est représenté par un certain morphisme $\mathcal{A}$-linéaire $e_k : \mathcal{A} \otimes \bar{\mathcal{A}}^{\otimes k} \longrightarrow \Sigma^k\mathcal{P}$. Dans ce qui suit, on se propose d'exhiber ce morphisme à l'aide des produits de Yoneda [26, 58] des suites exactes de $\mathcal{A}$-modules.

Soient $\mathcal{P}_2 = \mathbb{F}_2[x_1, x_2]$, $\mathcal{L}_2 := x_2^{-1}\mathcal{P}_2 \subset \mathbb{F}_2[x_1, x_2^{\pm 1}]$ et $\pi_2 : \Sigma^2\mathcal{L}_2 \longrightarrow \Sigma\mathcal{P}_1$ le morphisme $\mathcal{A}$-linéaire défini par

$$\pi_2(\Sigma^2 x_1^{i_1} x_2^{i_2}) = \begin{cases} \Sigma x_1^{i_1} & \text{si } i_2 = -1, \\ 0 & \text{si } i_2 \geq 0. \end{cases}$$

La suite exacte précédente donne naissance au diagramme commutatif

$$\begin{array}{ccccccc} \mathcal{A} \otimes \bar{\mathcal{A}} & & \xrightarrow{\quad\partial\quad} & & \mathcal{A} & \xrightarrow{\varepsilon} & \mathbb{F}_2 \\ \downarrow{\scriptstyle \varphi_1} & \searrow^{e_1} & & & \downarrow{\scriptstyle \varphi_0} & & \| \\ \Sigma^2\mathcal{L}_2 & \xrightarrow{\pi_2} & \Sigma\mathcal{P}_1 & \xrightarrow{\iota_1} & \Sigma\mathcal{L}_1 & \xrightarrow{\pi_1} & \mathbb{F}_2 \end{array}$$

où ε est l'augmentation, $\partial(\theta[\theta_1]) = \theta\theta_1$, $\varphi_0(\theta) := \Sigma\theta(x_1^{-1})$ et

$$\begin{aligned} e_1(\theta[\theta_1]) &= \Sigma\theta\theta_1(x_1^{-1}), \\ \varphi_1(\theta[\theta_1]) &:= \Sigma\theta\big(x_2^{-1}e_1(1[\theta_1])\big) = \Sigma^2\theta(x_2^{-1}\theta_1(x_1^{-1})). \end{aligned}$$

Pour tout $r > 1$, notons

$$\mathcal{P}_r = \mathbb{F}_2[x_1, \ldots, x_r],\ \mathcal{L}_r := x_r^{-1}\mathcal{P}_r \subset \mathbb{F}_2[x_1, \ldots, x_{r-1}, x_r^{\pm 1}].$$

On a la suite exacte courte de $\mathcal{A}$-modules

$$0 \longrightarrow \Sigma^r\mathcal{P}_r \xrightarrow{\iota_r} \Sigma^r\mathcal{L}_r \xrightarrow{\pi_r} \Sigma^{r-1}\mathcal{P}_{r-1} \longrightarrow 0,$$

où ι_r est l'inclusion et pour tout $P \in \mathcal{P}_{r-1} = \mathbb{F}_2[x_1, \ldots, x_{r-1}] \subset \mathcal{P}_r$:

$$\pi_r(\Sigma^r P x_r^{i_r}) = \begin{cases} \Sigma^{r-1}P & \text{si } i_r = -1, \\ 0 & \text{si } i_r \geq 0. \end{cases}$$

Supposons que φ_{r-1} et e_{r-1} sont connus. Alors cette suite donne naissance au diagramme commutatif

$$\begin{array}{ccccccc} \mathcal{A} \otimes \bar{\mathcal{A}}^{\otimes r} & & \xrightarrow{\quad\partial\quad} & & \mathcal{A} \otimes \bar{\mathcal{A}}^{\otimes(r-1)} & & \\ \downarrow{\scriptstyle \varphi_r} & \searrow^{e_r} & & & \downarrow{\scriptstyle \varphi_{r-1}} & \searrow^{e_{r-1}} & \\ \Sigma^{r+1}\mathcal{L}_{r+1} & \xrightarrow{\pi_{r+1}} & \Sigma^r\mathcal{P}_r & \xrightarrow{\iota_r} & \Sigma^r\mathcal{L}_r & \xrightarrow{\pi_r} & \Sigma^{r-1}\mathcal{P}_{r-1} \end{array}$$

où $\partial(\theta[\theta_r|\cdots|\theta_1]) = \theta\theta_r[\theta_{r-1}|\cdots|\theta_1] + \sum_{i=1}^{r-1}\theta[\theta_r|\cdots|\theta_{i+1}\theta_i|\cdots|\theta_1]$ et

$$\begin{aligned} e_r(\theta[\theta_r|\cdots|\theta_1]) &= \varphi_{r-1}\partial(\theta[\theta_r|\cdots|\theta_1]), \\ \varphi_r(\theta[\theta_r|\cdots|\theta_1]) &:= \Sigma\theta\big(x_{r+1}^{-1}e_r(1[\theta_r|\cdots|\theta_1])\big). \end{aligned}$$

Transfert Soit $\cap : Tor_k^{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) \otimes Ext_{\mathcal{A}}^k(\mathbb{F}_2, \Sigma^k\mathcal{P}) \longrightarrow Tor_0^{\mathcal{A}}(\mathbb{F}_2, \Sigma^k\mathcal{P}) = \Sigma^k\mathcal{P}_{\mathcal{A}}$ le cap-produit [26]. Le transfert est défini comme suit : $Tor_k^{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) \longrightarrow \Sigma^k\mathcal{P}_{\mathcal{A}}$, $z \longmapsto z \cap e_k$. En utilisant la bar-résolution de $\mathcal{A}$, ce morphisme est représenté par un morphisme $\bar{\mathcal{A}}^{\otimes k} \longrightarrow \Sigma^k\mathcal{P}_{\mathcal{A}}$ que nous identifions ci-après.

Pour tout $\mathcal{A}$-module V, notons $1 \otimes V$ le morphisme linéaire $V \longrightarrow \mathbb{F}_2 \otimes_{\mathcal{A}} V$ qui envoie v sur $1 \otimes v$. Le morphisme $\mathcal{A}$-linéaire e_k induit un morphisme linéaire

$$Tr_k^* : \bar{\mathcal{A}}^{\otimes k} \longrightarrow \Sigma^k\mathcal{P}_{\mathcal{A}}$$

qui rend commutatif le diagramme

$$\begin{array}{ccc} \mathcal{A} \otimes \bar{\mathcal{A}}^{\otimes k} & \xrightarrow{1\otimes(\mathcal{A}\otimes\bar{\mathcal{A}}^{\otimes k})} & \mathbb{F}_2 \otimes_{\mathcal{A}} (\mathcal{A} \otimes \bar{\mathcal{A}}^{\otimes k}) \cong \bar{\mathcal{A}}^{\otimes k} \\ \downarrow{\scriptstyle e_k} & & \downarrow{\scriptstyle Tr_k^*} \\ \Sigma^k\mathcal{P}_k = \Sigma^k\mathcal{P} & \xrightarrow{\Sigma^k\pi = 1\otimes\Sigma^k\mathcal{P}_k} & \mathbb{F}_2 \otimes_{\mathcal{A}} \Sigma^k\mathcal{P}_k \cong \Sigma^k\mathcal{P}_{\mathcal{A}} \end{array}$$

La restriction de Tr_k^* au noyau du bord $\partial : \bar{\mathcal{A}}^{\otimes k} \longrightarrow \bar{\mathcal{A}}^{\otimes(k-1)}$ de la bar-construction de l'algèbre de Steenrod est précisément le morphisme représentant du transfert qu'ont défini Singer [49] et Lannes–Zarati [23]. Pour nous, cette restriction n'est pas nécessaire et Tr_k^* sera défini sur $\bar{\mathcal{A}}^{\otimes k}$ tout entier. On a ainsi la formule

$$Tr_k^*([\theta_k|\cdots|\theta_1]) = \Sigma^k\pi e_k(1[\theta_k|\cdots|\theta_1]).$$

Signalons [23, 49] que Tr_k^* applique $\operatorname{Ker}\partial$ dans $\Sigma^k(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$ et non pas dans $\Sigma^k(\mathcal{P}^{\mathcal{GL}})_{\mathcal{A}} := \Sigma^k(\mathbb{F}_2 \otimes_{\mathcal{A}} \mathcal{P}^{\mathcal{GL}})$ (l'article [10] contient une erreur de ce genre, nous semble-t-il). Bien au contraire, c'est le morphisme naturel $\Sigma^k(\mathcal{P}^{\mathcal{GL}})_{\mathcal{A}} \longrightarrow \Sigma^k(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$ qui se factorise par le transfert [16]. En effet, ce morphisme est égal à la composée $Tr_k^* \circ \mathcal{LZ}^*$, où $\mathcal{LZ}^*$ désigne le dual du morphisme de Lannes–Zarati (voir la Section 1.4). Cette composée est nulle en vérité [18].

Notons également que pour ne pas compliquer les choses, nous avons supprimé tout symbole de suspension dans l'écriture de Tr_k^* dans les sections qui précèdent.

Formule récursive Soient $\theta_1, \ldots, \theta_k \in \bar{\mathcal{A}}$. Par définition

$$e_1(1[\theta_1]) = \Sigma\theta_1(x_1^{-1}).$$

Notons $\Delta : \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$ la comultiplication de l'algèbre de Steenrod et supposons que

$$\Delta(\theta_k) := 1 \otimes \theta_k + \sum_{\deg\theta'_k > 0} \theta'_k \otimes \theta''_k.$$

On veut démontrer la formule suivante pour $k > 1$:

$$e_k(1[\theta_k|\cdots|\theta_1]) = \sum_{\deg\theta'_k>0} \Sigma\theta'_k(x_k^{-1})\theta''_k e_{k-1}(1[\theta_{k-1}|\cdots|\theta_1]).$$

Posons $u := [\theta_k|\cdots|\theta_1]$ et $v := [\theta_{k-1}|\cdots|\theta_1]$. On a

$$\begin{aligned} & e_k(1[\theta_k|\cdots|\theta_1]) = e_k(1 \otimes u) = \varphi_{k-1}(\partial(1 \otimes u)) \\ = \;& \varphi_{k-1}(u) + \varphi_{k-1}(1 \otimes \partial u) = \Sigma\theta_k\big(x_k^{-1}e_{k-1}(1 \otimes v)\big) + \Sigma x_k^{-1}e_{k-1}(1 \otimes \partial u) \\ = \;& \sum_{\deg\theta'_k>0} \Sigma\theta'_k(x_k^{-1})\theta''_k e_{k-1}(1 \otimes v) + \Sigma x_k^{-1}\big(\theta_k e_{k-1}(1 \otimes v) + e_{k-1}(1 \otimes \partial u)\big), \end{aligned}$$

ceci d'après la formule de Cartan. La formule désirée résulte de ce que le second terme de cette somme est nul. En effet :

$$\begin{aligned} & \theta_k e_{k-1}(1\otimes v) + e_{k-1}(1\otimes \partial u) = e_{k-1}(\theta_k \otimes v + 1\otimes \partial u) \\ = \quad & e_{k-1}(u + 1\otimes \partial u) = e_{k-1}(\partial(1\otimes u)) = \varphi_{k-2}(\partial\partial(1\otimes u)) = 0. \end{aligned}$$

Afin d'éviter des complications inutiles, à partir d'ici nous supprimons à nouveau tout symbole de suspension dans les formules concernant le transfert.

Base de Milnor L'algèbre de Steenrod duale $\mathcal{A}^*$ est isomorphe [33, 50] à l'algèbre polynomiale graduée $\mathbb{F}_2[\xi_1, \xi_2, \dots]$, où $\deg \xi_i = 2^i - 1$. Étant donnée une suite d'entiers positifs ou nuls $I = (i_1, \dots, i_t)$, on note $Sq(I) \in \mathcal{A}$ l'élément dual de $\xi^I := \xi_1^{i_1} \cdots \xi_t^{i_t}$ par rapport à la base formée des monômes en $\xi_1, \xi_2, \dots$ de $\mathcal{A}^*$. Si $i_1 = \cdots = i_{t-1} = 0$ et $i_t = 2^s$, l'élément $Sq(I)$ se note également P_t^s selon l'usage [30, 46]. Lorsque I parcourt toutes les suites d'entiers positifs ou nuls, les éléments $Sq(I)$ forment une base de l'espace vectoriel gradué $\mathcal{A}$. Cette base est baptisée d'après Milnor.

L'action de la comultiplication de $\mathcal{A}$ sur la base de Milnor est donnée par la formule $\Delta(Sq(I)) = \sum_{I'+I''=I} Sq(I') \otimes Sq(I'')$. D'où P_t^0 est primitif. Les P_t^0 sont les seuls éléments primitifs de l'algèbre de Hopf $\mathcal{A}$.

Dans l'algèbre $\mathcal{A}$, l'élément P_t^s est engendré par $Sq^1, \dots, Sq^{2^{s+t-1}}$. Si $s < t$, on a $(P_t^s)^2 = 0$ (voir [33]).

Le primitif P_t^0 commute [32] avec $Sq^1, \dots, Sq^{2^t-1}$. Ceci résulte de ce que l'action de $\mathcal{A}$ sur $\bigoplus_{n>0} H^*((\mathbb{R}P^\infty)^n; \mathbb{F}_2)$ est fidèle [50] et que le commutateur $[Sq^i, P_t^0] = Sq^i P_t^0 + P_t^0 Sq^i$ s'annule sur $\bigoplus_{n>0} H^*((\mathbb{R}P^\infty)^n; \mathbb{F}_2)$ pour tout $i < 2^t$.

Coaction de Milnor L'action de la base de Milnor sur les polynômes peut être calculée à l'aide de la coaction de Milnor $\lambda : \mathcal{P} \longrightarrow \mathcal{P}\widehat{\otimes}\mathcal{A}^*$ introduite dans la Section 5.1. Le morphisme λ est un morphisme d'algèbres et vérifie les formules

$$\begin{cases} \lambda(u) = u\otimes 1 + \sum_{i>0} u^{2^n} \otimes \xi_i & \text{si} \quad u \in \mathcal{P},\ \deg u = 1, \\ \lambda(P) = \sum_I Sq(I)(P) \otimes \xi^I & \text{si} \qquad\qquad P \in \mathcal{P}. \end{cases}$$

D'où l'on déduit, par exemple, que $P_t^s(u^{2^s}) = u^{2^{s+t}}$ si $u \in \mathcal{P}$ et $\deg u = 1$.

Shuffle-produit Soient $\gamma' := [\theta_1|\cdots|\theta_r]$ et $\gamma'' := [\theta_{r+1}|\cdots|\theta_{r+s}]$ des éléments de la bar-construction [26] de l'algèbre de Steenrod. Le shuffle-produit de γ' et γ'' est défini [1, 13, 26] comme étant

$$\gamma' * \gamma'' := \sum_{\sigma \in \mathfrak{S}_{r+s}/\mathfrak{S}_r\times\mathfrak{S}_s} [\theta_{\sigma^{-1}(1)}|\cdots|\theta_{\sigma^{-1}(r+s)}],$$

où $\mathfrak{S}_{r+s}/\mathfrak{S}_r\times\mathfrak{S}_s$ désigne l'ensemble des permutations $\sigma \in \mathfrak{S}_{r+s}$ vérifiant $\sigma(1) < \cdots < \sigma(r)$ et $\sigma(r+1) < \cdots < \sigma(r+s)$.

Supposons que $\theta_i\theta_j = \theta_j\theta_i$ pour tout $1 \le i \le r < j \le r+s$. Alors, on a [1] la formule $\partial(\gamma' * \gamma'') = \partial(\gamma') * \gamma'' + \gamma' * \partial(\gamma'')$. D'où il suit que si deux cycles de la bar-construction commutent, leur shuffle-produit est un cycle.

5.3 Démonstration du Théorème 1.4(i)

Décomposables Singer [49] a montré que $h_i \in \mathrm{Im}\, Tr_1$ et $c_0 \in \mathrm{Im}\, Tr_3$. Boardman [5] a montré que $c_i \in \mathrm{Im}\, Tr_3$ pour tout $i > 0$. Comme $\bigoplus_{n\geq 1} Tr_n$ est un morphisme d'algèbres [49], il suit que $\mathrm{Im}\, Tr_4$ contient tous les décomposables de $H^4(\mathcal{A})$.

Reprenons les calculs par lesquels Singer est parvenu à montrer $c_0 \in \mathrm{Im}\, Tr_3$. Les ingrédients en sont :

- une description explicite de l'objet dual de l'algèbre différentielle graduée Lambda [7] (dont l'homologie est isomorphe à $H^*(\mathcal{A})$) en termes des invariants de Dickson [18, 49],
- un cycle représentant explicite de c_0 en "langage" Lambda.

Cette méthode peut s'appliquer à d'autres éléments de $H^*(\mathcal{A})$. Elle risque pourtant d'échouer si les cycles représentants concernés sont compliqués, ou si leur expressions en termes des invariants de Dickson ne sont pas explicites. En fait, cette méthode ne marche plus dès que $k = 4$ et pour tous les indécomposables de $H^4(\mathcal{A})$. Face à cette difficulté, nous offrons la solution suivante :

- identifier les éléments non nuls de $(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$,
- choisir (intuitivement) des cycles représentants de la bar-construction de l'algèbre de Steenrod, puis vérifier qu'ils correspondent par le transfert aux éléments $(\mathcal{P}_{\mathcal{A}})^{\mathcal{GL}}$ identifiés plus haut.

Nous espérons que notre méthode exprime bien ce que voulait dire Singer lorsque'il a construit son morphisme : *le transfert sert (i) à vérifier si un élément donné de l'homologie de l'algèbre de Steenrod est non nul, (ii) à prédire l'existence de certains éléments non nuls de l'homologie de l'algèbre de Steenrod.*

À titre d'exemple, voici notre preuve de ce que $c_0 \in \mathrm{Im}\, Tr_3$. Comme $\pi(x_1x_2)$ est un $\mathcal{GL}_2$-invariant de $\mathbb{F}_2[x_1, x_2]_{\mathcal{A}}$ et Tr_2^* est un isomorphisme [49], il existe un cycle $\gamma_2 \in \bar{\mathcal{A}}^{\otimes 2}$ tel que $Tr_2^*(\gamma_2) = \pi(x_1x_2)$. Explicitement

$$\gamma_2 := [Sq^2|Sq^2] + [Sq^1|P_2^1].$$

Posons $c_0^* := \gamma_2 * [P_3^0]$. Comme P_3^0 est un élément primitif de $\mathcal{A}$, la formule évaluant $e_3(c_0^*)$ est simple. En effet $e_3(c_0^*) = x_1^6x_2x_3 + x_1x_2^6x_3 + x_1x_2x_3^6 \not\equiv 0$. Ceci implique que $Tr_3^*(c_0^*) \neq 0$. Comme $Tr_3^* : Tor_{3,11}^{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) = \mathbb{F}_2 \longrightarrow (\mathcal{P}_{\mathcal{A}}^8)^{\mathcal{GL}} = \mathbb{F}_2$ est non nul, il suit que Tr_3 est bijectif en degré 8. D'où $c_0 \in \mathrm{Im}\, Tr_3$.

Indécomposables d_i, e_i Parmi les preuves du fait $d_0, e_0 \in \mathrm{Im}\, Tr_4$, celle donnée par Hà [15] mérite bien notre attention. Son idée est de considérer le diagramme commutatif

$$\begin{array}{ccc} (\Gamma^{\mathcal{A}})_{\mathcal{GL}} & \xrightarrow{Tr_4} & H^4(\mathcal{A}) \\ \downarrow & & \downarrow \\ (\Gamma^{\mathcal{B}})_{\mathcal{GL}} & \xrightarrow{Tr_4^{\mathcal{B}}} & H^4(\mathcal{B}) \end{array}$$

où $\mathcal{B} \subset \mathcal{A}$ désigne la sous-algèbre de Hopf engendrée par Sq^1 et Sq^2, les flèches verticales sont des morphismes naturels, et $Tr_4^{\mathcal{B}}$ désigne l'analogue du transfert algébrique. Les images de d_0, e_0 par la projection canonique $H^*(\mathcal{A}) \longrightarrow H^*(\mathcal{B})$ ont été explicitées par Zachariou [59, 60]. Elles sont décomposables et suffisamment simples pour que Hà puisse montrer l'existence des élements de $(\Gamma^{\mathcal{B}})_{\mathcal{GL}}$

qui leur correspondent par le morphisme $Tr_4^{\mathcal{B}}$. Il reste à vérifier que ces éléments de $(\Gamma^{\mathcal{B}})_{\mathcal{GL}}$ proviennent de $(\Gamma^{\mathcal{A}})_{\mathcal{GL}}$, ce qu'a pu faire Hà en dualisant la situation.

La méthode de Hà peut s'appliquer aux wedge-algèbres [28, 31, 42]. Appliquée à un élément concret $\gamma \in H^*(\mathcal{A})$, le succès de sa méthode dépend

- de la connaissance de l'image de γ par la projection canonique $H^*(\mathcal{A}) \longrightarrow H^*(\mathcal{B}')$, où $\mathcal{B}' \subset \mathcal{A}$ est une certaine sous-algèbre de Hopf,
- de ce que cette image soit suffisamment simple pour qu'on puisse trouver son correspondant dans $(\Gamma^{\mathcal{B}'})_{\mathcal{GL}}$.

Ainsi, ce succès n'est plus assuré dans le cas de l'élément $f_0 \in H^{4,22}$, dont on ne connaît pas l'image par les projections canoniques $H^*(\mathcal{A}) \longrightarrow H^*(\mathcal{B}')$.

Voici notre preuve de ce que $d_0, e_0 \in \operatorname{Im} Tr_4$. Comme $\pi(x_1x_2x_3)$ est un $\mathcal{GL}_3$-invariant de $\mathbb{F}_2[x_1,x_2,x_3]_{\mathcal{A}}$ et Tr_3^* est un isomorphisme [5], il existe un cycle $\gamma_3 \in \bar{\mathcal{A}}^{\otimes 3}$ tel que $Tr_3^*(\gamma_3) = \pi(x_1x_2x_3)$. Explicitement

$$\begin{aligned}\gamma_3 \quad := \quad & [Sq^2|Sq^2|Sq^2] + [Sq^1|Sq^1] * [Sq^4] + [Sq^1|Sq^2|Sq^3] \\ & + [Sq^2|Sq^3|Sq^1] + [Sq^3|Sq^1|Sq^2].\end{aligned}$$

(Notons que l'existence d'un cycle contenant le terme $[Sq^2|Sq^2|Sq^2]$ équivaut à ce que $h_1^3 \neq 0$.)

Rappelons le cycle $\gamma_2 = [Sq^2|Sq^2] + [Sq^1|P_2^1]$. Posons $d_0^* := \gamma_2 * [P_3^0|P_3^0]$ et $e_0^* := \gamma_3 * [P_4^0]$. Pour évaluer $e_4(d_0^*)$ et $e_4(e_0^*)$, observons

- que si $P \in \mathcal{P}^{14}$ est divisible par $\theta P_3^0(u^{-1})$, avec $\theta \in \bar{\mathcal{A}}$ et $\deg u = 1$, alors $P \equiv 0$,
- que si $P \in \mathcal{P}^{17}$ est divisible par $\theta P_4^0(u^{-1})$, avec $\theta \in \bar{\mathcal{A}}$ et $\deg u = 1$, alors $P \equiv 0$.

En posant $(\sigma P)(x_1,x_2,x_3,x_4) := P(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)}, x_{\sigma^{-1}(4)})$ pour tout $P \in \mathcal{P}$ et $\sigma \in \mathfrak{S}_4$, il suit que

$$\begin{aligned} e_4(d_0^*) \quad &\equiv \quad \sigma \sum_{\sigma \in \mathfrak{S}_4/\mathfrak{S}_2\times\mathfrak{S}_2} P_3^0(x_4)P_3^0(x_3)e_2(\gamma_2) \\ &\equiv \quad x_1x_2(x_3x_4)^6 + (x_1x_2)^3(x_3x_4)^4 \not\equiv 0 \text{ d'après la Proposition 6.13,} \\ e_4(e_0^*) \quad &\equiv \quad \sigma \sum_{\sigma \in \mathfrak{S}_4/\mathfrak{S}_3\times\mathfrak{S}_1} P_4^0(x_4)e_3(\gamma_3) \\ &\equiv \quad x_1^{14}x_2x_3x_4 + x_1x_2^{14}x_3x_4 + x_1x_2x_3^{14}x_4 + x_1x_2x_3x_4^{14} \not\equiv 0, \end{aligned}$$

ceci d'après la Proposition 6.16. D'où $Tr_4^*(d_0^*) \neq 0$ et $Tr_4^*(e_0^*) \neq 0$. Comme les morphismes

$$\begin{aligned} Tr_4^* : Tor_{4,18}^{\mathcal{A}}(\mathbb{F}_2,\mathbb{F}_2) = \mathbb{F}_2 \longrightarrow (\mathcal{P}_{\mathcal{A}}^{14})^{\mathcal{GL}} = \mathbb{F}_2, \\ Tr_4^* : Tor_{4,21}^{\mathcal{A}}(\mathbb{F}_2,\mathbb{F}_2) = \mathbb{F}_2 \longrightarrow (\mathcal{P}_{\mathcal{A}}^{17})^{\mathcal{GL}} = \mathbb{F}_2, \end{aligned}$$

sont non nuls, il suit que Tr_4 est bijectif dans les degrés 14 et 17. D'où $d_0, e_0 \in \operatorname{Im} Tr_4$.

Pour les lecteurs qui aiment la diversité, les cycles suivants ont également des images non nulles par Tr_4^* :

$$d_0^* := [P_2^0|P_2^0] * [P_2^1|P_2^1],\ e_0^* := [P_2^1|P_2^1|P_2^1] * [P_2^0].$$

Comme $Sq^0Tr_4 = Tr_4Sq^0$, ce qui précède implique que $d_i = (Sq^0)^i(d_0) \in \operatorname{Im} Tr_4$ et que $e_i = (Sq^0)^i(e_0) \in \operatorname{Im} Tr_4$.

Indécomposables f_i Soit $f_0^* := ([Sq^4|Sq^4] + [Sq^2|P_2^1]) * [P_3^0|P_3^0]$. Des calculs explicites montrent que

$$Tr_4^*(f_0^*) = \pi(x_1^3x_2^3x_3^4x_4^8 + x_1^4x_2^8x_3^3x_4^3 + x_1^3x_2^3x_3^6x_4^6 + x_1^6x_2^6x_3^3x_4^3),$$

l'expression qui n'est pas nulle d'après la Proposition 6.17.

Observons que $h_4h_2h_0^2 \neq 0$ d'après Lin [24]. Ceci équivaut à l'existence d'un cycle $\gamma_4 \in \bar{\mathcal{A}}^{\otimes 4}$ contenant $[Sq^{16}|Sq^4|Sq^1|Sq^1]$. Il est facile de vérifier que le monôme $x_1^{15}x_2^3$ apparaît dans l'expression de $e_4(\gamma_4)$. D'où $Tr_4^*(\gamma_4) \neq 0$ et $Tr_4^*(\gamma_4) \neq Tr_4^*(f_0^*)$. Comme l'image du morphisme

$$Tr_4^* : Tor_{4,22}^{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) = \mathbb{F}_2 \oplus \mathbb{F}_2 \longrightarrow (\mathcal{P}_{\mathcal{A}}^{18})^{\mathcal{GL}} = \mathbb{F}_2 \oplus \mathbb{F}_2$$

est de dimension au moins 2, il suit que Tr_4 est bijectif en degré 18. D'où $f_0 \in \mathrm{Im}\, Tr_4$. Comme $Sq^0Tr_4 = Tr_4Sq^0$, ceci implique que $f_i = (Sq^0)^i(f_0) \in \mathrm{Im}\, Tr_4$.

Indécomposables g_{i+1}, p_i, $D_3(i)$, p_i' Soient $i \geq 0$ et d un entier tel que $H^{4,d+4}$ contient l'un des éléments g_{i+1}, p_i, $D_3(i)$, p_i'. Si $i = 0$, alors $(\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} = (\mathrm{Im}\, Tr_4)_d = 0$ d'après [8] et d'après les Propositions 6.21, 6.22, 6.23. Si $i > 0$, alors d'après le Théorème 1.3, on a soit $(\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} = Sq^0(\Gamma_{d/2-2}^{\mathcal{A}})_{\mathcal{GL}}$, soit

$$(\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} = \mathcal{GL}\langle a_1^{(2^p-1)}a_2^{(2^q-1)}\rangle + Sq^0(\Gamma_{d/2-2}^{\mathcal{A}})_{\mathcal{GL}}$$

pour certains $p, q \geq 0$. Comme $Tr_4(\iota^*(a_1^{(2^p-1)}a_2^{(2^q-1)})) = h_ph_qh_0^2$ d'après [5], il suit que l'espace vectoriel $(\mathrm{Im}\, Tr_4)^d$ est engendré par $h_ph_qh_0^2$ et $(\mathrm{Im}\, Tr_4)^{d/2-2}$. D'où, par récurrence sur i, on déduit que $(\mathrm{Im}\, Tr_4)^d$ est engendré par les produits $h_{i_1}h_{i_2}h_{i_3}h_{i_4}$. Par conséquent, les indécomposables g_{i+1}, p_i, $D_3(i)$, p_i' ne sont pas dans l'image de Tr_4.

5.4 Démonstration du Théorème 1.4(ii)

Cas 1 $\alpha(d+4) > 4$.

Dans ce cas $\mathcal{P}_{\mathcal{A}}^d = 0$ d'après le Théorème 4.1.1(ii), et $H^{4,d+4} = 0$ d'après Lin [24]. D'où $Tr_4 : (\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow H^{4,d+4}$ est bijectif.

Cas 2 $d \leq 22$.

La bijectivité de $Tr_4 : (\Gamma_d^{\mathcal{A}})_{\mathcal{GL}} \longrightarrow H^{4,d+4}$ est justifiée par le Théorème 1.4(i) grâce aux tableaux suivants (cf. la Section 6) :

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$(\mathcal{P}_{\mathcal{A}}^d)^{\mathcal{GL}}$	0	0	0	0	0	0	$\mathbb{F}_2$	0	$\mathbb{F}_2$	0	0	0	0	$\mathbb{F}_2$
$H^{4,d+4}$	0	0	0	0	0	0	$\mathbb{F}_2$	0	$\mathbb{F}_2$	0	0	0	0	$\mathbb{F}_2$

d	15	16	17	18	19	20	21	22
$(\mathcal{P}_{\mathcal{A}}^d)^{\mathcal{GL}}$	$\mathbb{F}_2$	0	$\mathbb{F}_2$	$\mathbb{F}_2 \oplus \mathbb{F}_2$	0	0	0	$\mathbb{F}_2$
$H^{4,d+4}$	$\mathbb{F}_2$	0	$\mathbb{F}_2$	$\mathbb{F}_2 \oplus \mathbb{F}_2$	0	0	0	$\mathbb{F}_2$

d	7	9	14	15	17	18	22
$H^{4,d+4}$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2 \oplus \mathbb{F}_2$	$\mathbb{F}_2$
Générateurs	$h_3h_0^3$	c_0h_1	d_0	$h_4h_0^3$	e_0	$f_0, h_4h_2h_0^2$	c_1h_2

Cas 3 *$H^{4,d+4}$ contient $h_0\gamma$ avec* $\gamma = \begin{cases} c_j & j \geq 4, \\ h_{i_2}h_{i_3}h_{i_4}, & i_4 > i_3 \geq i_2 \geq 4. \end{cases}$

Il est clair que $\gamma \in (Sq^0)^4(H^{4,\widetilde{d}+4})$ avec $\widetilde{d} := (d-60)/16$. Il est facile de vérifier que $\alpha(\widetilde{d}+2) \geq 2$. Posons $\widetilde{\Gamma} := \Gamma(a_2, a_3, a_4)$ et $\widetilde{\mathcal{GL}} := \mathcal{GL}_3$. D'après le Théorème 1.2(ii) on a le diagramme commutatif

$$\begin{array}{ccccc} (\widetilde{\Gamma}^{\mathcal{A}}_{\widetilde{d}})_{\widetilde{\mathcal{GL}}} & \xrightarrow{(Sq^0)^4} & (\widetilde{\Gamma}^{\mathcal{A}}_{d})_{\widetilde{\mathcal{GL}}} & \xrightarrow{\varphi} & (\Gamma^{\mathcal{A}}_{d})_{\mathcal{GL}} \\ \downarrow{\scriptstyle Tr_3} & & & & \downarrow{\scriptstyle Tr_4} \\ H^{3,\widetilde{d}+3} & \xrightarrow{(Sq^0)^4} & H^{3,d+3} & \xrightarrow{h_0} & H^{4,d+4} \end{array}$$

où $(Sq^0)^4$ de la première ligne est bijectif, et φ est une certaine surjection. Le morphisme Tr_3 est bijectif d'après Boardman [5]. Les morphismes de la seconde ligne sont injectifs d'après Lin [24]. Il suit que Tr_4 est injectif.

Cas 4 *$s = 0$, $d > 22$ et $H^{4,d+4}$ contient un certain indécomposable.*

Dans ce cas, les seuls indécomposables que puissent contenir $H^{4,d+4}$ sont p_0, $D_3 = D_3(0)$, p_0'. L'injectivité de $Tr_4 : (\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} \longrightarrow H^{4,d+4}$ est justifiée par le tableau suivant :

d	33	61	69
$(\mathcal{P}^d_{\mathcal{A}})^{\mathcal{GL}}$	0	0	0
$H^{4,d+4}$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2$
Générateurs de $H^{4,d+4}$	p_0	$D_3 = D_3(0)$	p_0'

Cas 5 *$s > 0$ et $d > 22$.*

Soit $n = d/2 - 2$. On a le diagramme commutatif [5]

$$\begin{array}{ccc} (\Gamma^{\mathcal{A}}_n)_{\mathcal{GL}} & \xrightarrow{Sq^0} & (\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} \\ \downarrow{\scriptstyle Tr_4} & & \downarrow{\scriptstyle Tr_4} \\ H^{4,n+4} & \xrightarrow{Sq^0} & H^{4,d+4} \end{array}$$

Le morphisme Sq^0 de la première ligne est toujours injectif. D'après Lin [24], le morphisme Sq^0 de la seconde ligne est injectif. Si $\alpha(d+2) > 2$, alors $(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = Sq^0(\Gamma^{\mathcal{A}}_n)_{\mathcal{GL}}$ d'après le Théorème 1.3(i). Ceci implique que Tr_4 est injectif en degré d si et seulement s'il l'est en degré n.

Supposons $\alpha(d+2) \leq 2$. Soient $p \geq 1$, $q \geq 0$ des entiers tels que $d = 2^{p+q} + 2^p - 2 > 22$. Si $q = 1$ ou $p \leq 2$, alors $(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = Sq^0(\Gamma^{\mathcal{A}}_n)_{\mathcal{GL}}$ d'après le Théorème 1.3(ii). D'où Tr_4 est injectif en degré d si et seulement s'il l'est en degré n. Si $q \neq 1$ et $p \geq 3$, d'après le Théorème 1.3(ii) on a

$$(\Gamma^{\mathcal{A}}_d)_{\mathcal{GL}} = \mathbb{F}_2\langle \iota^*(a_1^{(2^{p+q}-1)}a_2^{(2^p-1)})\rangle \oplus Sq^0(\Gamma^{\mathcal{A}}_n)_{\mathcal{GL}}.$$

Observons que $Tr_4(\iota^*(a_1^{(2^{p+q}-1)}a_2^{(2^p-1)}) = h_{p+q}h_ph_0^2$ d'après Boardman [5], et que $h_{p+q}h_ph_0^2 \notin Sq^0(H^{4,n+4})$ d'après Lin [24]. Il suit que Tr_4 est injectif en degré d si et seulement s'il l'est en degré n.

Ce qui a été fait jusqu'ici permet de montrer, par récurrence sur d, que Tr_4 est injectif en degré d si et seulement s'il l'est en degré n, et que Tr_4 est injectif en degré d si $H^{4,d+4}$ contient

- au moins un indécomposable,
- $h_i c_j$ avec $j \geq i+4 \geq 4$,
- $h_{i_1} h_{i_2} h_{i_3} h_{i_4}$ avec $i_4 > i_3 \geq i_2 \geq i_1 \geq 4$.

Ceci termine la démonstration du Théorème 1.4(ii).

6 Indécomposables de degré petit

Cette section a pour objectif la détermination de $\mathcal{P}_{\mathcal{A}}$ en degré petit pour $k=4$. Écrivons x,y,z,t respectivement à la place de x_1,x_2,x_3,x_4 et renvoyons à la Section 4.1 pour les notations. Rappelons les formules

$$\begin{array}{lcl}
\mathcal{P}^d_{\mathcal{A}} & \cong & \mathcal{P}^{d/2-2}_{\mathcal{A}} \oplus (\operatorname{Ker}\psi)^d \text{ si } d \text{ est pair,}\\
\Gamma^{\mathcal{A}}_d & = & Sq^0(\Gamma^{\mathcal{A}}_{d/2-2}) \oplus (\operatorname{Coker} Sq^0)_d \text{ si } d \text{ est pair,}\\
\mathcal{P}^d_{\mathcal{A}} & = & (\operatorname{Ker}\psi)^d \text{ si } d \text{ est impair,}\\
\Gamma^{\mathcal{A}}_d & = & (\operatorname{Coker} Sq^0)_d \text{ si } d \text{ est impair,}\\
(\operatorname{Ker}\psi)^d & \cong & \pi(\mathcal{W}^d \cap \mathcal{P}_{xyzt}) \oplus \mathbb{F}_2\langle \pi(\mathcal{B}^d_x \cup \mathcal{B}^d_y \cup \mathcal{B}^d_z \cup \mathcal{B}^d_t \cup \mathcal{B}^d_{xy} \cup \mathcal{B}^d_{xz} \cup \mathcal{B}^d_{xt}\\
 & & \quad \cup \mathcal{B}^d_{yz} \cup \mathcal{B}^d_{yt} \cup \mathcal{B}^d_{zt} \cup \mathcal{B}^d_{xyz} \cup \mathcal{B}^d_{xyt} \cup \mathcal{B}^d_{xzt} \cup \mathcal{B}^d_{yzt})\rangle \text{ si } d>0.
\end{array}$$

Rappelons également que $(\operatorname{Ker}\psi)^d = (\operatorname{Coker} Sq^0)_d = 0$ si $\alpha(d+2) > 2$, en particulier si $d = 12, 20$.

Démontrables à la main (c'est de cette manière que nous les avons trouvées), les 23 propositions suivantes se vérifient aisément à l'aide de l'ordinateur grâce au logiciel de Bruner transcrit dans l'Appendice 8.1.

Proposition 6.1 *Soit $d=1$. Alors $\pi(\mathcal{W}^1 \cap \mathcal{P}_{xyzt}) = 0$, et l'image par π de x,y,z,t forme une base de $\mathcal{P}^1_{\mathcal{A}} = (\operatorname{Ker}\psi)^1$. De plus $(\mathcal{P}^1_{\mathcal{A}})^{\mathcal{GL}} = 0$.*

Proposition 6.2 *Soit $d=2$. Alors $\pi(\mathcal{W}^2 \cap \mathcal{P}_{xyzt}) = 0$, et l'image par π de xy, xz, xt, yz, yt, zt forme une base de $\mathcal{P}^2_{\mathcal{A}} = (\operatorname{Ker}\psi)^2$. De plus $(\mathcal{P}^2_{\mathcal{A}})^{\mathcal{GL}} = 0$.*

Proposition 6.3 *Soit $d=3$. Alors $\pi(\mathcal{W}^3 \cap \mathcal{P}_{xyzt}) = 0$ et l'image par π de 14 monômes $x^3, y^3, z^3, t^3, xy^2, xz^2, xt^2, yz^2, yt^2, zt^2, xyz, xyt, xzt, yzt$ forme une base de $\mathcal{P}^3_{\mathcal{A}} = (\operatorname{Ker}\psi)^3$. De plus $(\mathcal{P}^3_{\mathcal{A}})^{\mathcal{GL}} = 0$.*

Proposition 6.4 *Soit $d=4$. Alors*

$$\pi(\mathcal{W}^4 \cap \mathcal{P}_{xyzt}) = 0,\ \dim \mathcal{P}^4_{\mathcal{A}} = 21,\ \dim(\operatorname{Ker}\psi)^4 = 20,\ (\mathcal{P}^4_{\mathcal{A}})^{\mathcal{GL}} = 0.$$

(Rappelons que $\mathcal{B}^4_x = \varnothing$, $\mathcal{B}^4_{xy} = \{xyx^2, xyy^2\}$ et $\mathcal{B}^4_{xyz} = \{xyz^2, xzy^2\}$.)

Proposition 6.5 *Soit $d=5$. Alors l'image par π de $xyzt^2$, $xytz^2$, $xzty^2$ forme une base de $\pi(\mathcal{W}^5 \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^5_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^5 = 15$, $(\mathcal{P}^5_{\mathcal{A}})^{\mathcal{GL}} = 0$.*

(Rappelons que $\mathcal{B}^5_x = \mathcal{B}^5_{xy} = \varnothing$ et $\mathcal{B}^5_{xyz} = \{xyzx^2, xyzy^2, xyzz^2\}$.)

Proposition 6.6 *Soit $d=6$. Alors l'image par π de $xy(zt)^2$, $xz(yt)^2$ forme une base de $\pi(\mathcal{W}^6 \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^6_{\mathcal{A}} = 24$, $\dim(\operatorname{Ker}\psi)^6 = 20$, $(\mathcal{P}^6_{\mathcal{A}})^{\mathcal{GL}} = 0$.*

(Rappelons que $\mathcal{B}^6_x = \varnothing$, $\mathcal{B}^6_{xy} = \{(xy)^3\}$ et $\mathcal{B}^6_{xyz}$ est composé de $xy(xz)^2$, $xy(yz)^2$, $xz(yz)^2$.)

Proposition 6.7 *Soit $d = 7$. Alors l'image par π de 9 monômes*

$$\begin{array}{lll} xyz(xt)^2, & xyz(yt)^2, & xyz(zt)^2, \\ xyt(xz)^2, & xyt(yz)^2, & xyt(zt)^2, \\ xzt(yz)^2, & xzt(yt)^2, & x(yzt)^2, \end{array}$$

forme une base de $\pi(\mathcal{W}^7 \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^7_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^7 = 35$, $(\Gamma^{\mathcal{A}}_7)_{\mathcal{GL}} = \mathbb{F}_2\langle \iota^*(a_1^{(7)})\rangle$.

(Rappelons que $\mathcal{B}^7_x = \{x^7\}$, $\mathcal{B}^7_{xy} = \{xy^6\}$ et $\mathcal{B}^7_{xyz}$ est composé de $xyz(xy)^2$, $xyz(xz)^2$, $xyz(yz)^2$, xy^2z^4.)

Proposition 6.8 (cf. aussi [8]) *Soit $d = 8$. Alors l'image par π de*

$$\begin{array}{llll} xyz^2t^4, & xzy^2t^4, & xty^2z^4, & \\ xt(yzt)^2, & xy(xzt)^2, & xy(yzt)^2, & xz(yzt)^2, \end{array}$$

forme une base de $\pi(\mathcal{W}^8 \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^8_{\mathcal{A}} = 55$, $\dim(\operatorname{Ker}\psi)^8 = 49$, $(\mathcal{P}^8_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^8_x = \varnothing$, $\mathcal{B}^8_{xy}$ est composé de xyx^6, xyy^6, xyx^2y^4, et $\mathcal{B}^8_{xyz}$ est composé de xyx^2z^4, xyy^2z^4, xzy^6, xzy^2z^4, xyz^6, $xy(xyz)^2$.)

Proposition 6.9 *Soit $d = 9$. Alors l'image par π de 18 monômes*

$$\left\{ \begin{array}{ll} xyzP^2, & P \in \{xt^2, yt^2, zt^2, t^3, xyt, xzt, yzt\}, \\ xytP^2, & P \in \{xz^2, yz^2, zt^2, z^3, xzt, yzt\}, \\ xztP^2, & P \in \{xy^2, yz^2, yt^2, y^3, yzt\}, \end{array} \right.$$

forme une base de $\pi(\mathcal{W}^9 \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^9_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^9 = 46$ et $(\Gamma^{\mathcal{A}}_9)_{\mathcal{GL}} = \mathbb{F}_2\langle \iota^*(c_0 a_4)\rangle$, où [3, 5]

$$c_0 := a_1a_2a_3^{(6)} + a_1a_2^{(2)}a_3^{(5)} + a_1a_2^{(4)}a_3^{(3)} + a_1^{(2)}a_2^{(3)}a_3^{(3)}.$$

(Rappelons que $\mathcal{B}^9_x = \mathcal{B}^9_{xy} = \varnothing$ et $\mathcal{B}^9_{xyz}$ est composé de 7 monômes

$$xyzP^2, P \in \{x^3, y^3, z^3, xy^2, xz^2, yz^2, xyz\}.)$$

Proposition 6.10 *Soit $d = 10$. Alors l'image par π de 12 monômes*

$$\begin{array}{llll} xy(xz)^2t^4, & xy(xt)^2z^4, & xy(zt)^2z^4, & xy(zt)^2t^4, \\ xy(yz)^2t^4, & xy(yt)^2z^4, & xz(yz)^2t^4, & xz(yt)^2y^4, \\ xz(yt)^2z^4, & xz(yt)^2t^4, & xt(yt)^2z^4, & xy(xyzt)^2, \end{array}$$

forme une base de $\pi(\mathcal{W}^{10} \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^{10}_{\mathcal{A}} = 70$, $\dim(\operatorname{Ker}\psi)^{10} = 56$, $(\mathcal{P}^{10}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{10}_x = \varnothing$, $\mathcal{B}^{10}_{xy} = \{(xy)^3x^4, (xy)^3y^4\}$ et $\mathcal{B}^{10}_{xyz}$ est composé de 8 monômes

$$\begin{array}{llll} xy(xz)^2x^4, & xy(xz)^2z^4, & xy(yz)^2y^4, & xy(yz)^2z^4, \\ xz(yz)^2y^4, & xz(yz)^2z^4, & xy(xz)^2y^4, & (xy)^3z^4.) \end{array}$$

Proposition 6.11 *Soit $d = 11$. Alors forme une base de $\pi(\mathcal{W}^{11} \cap \mathcal{P}_{xyzt})$ l'image par π de 32 monômes*

$$\begin{cases} xyzP^2, & P \in \{xyzt, xyt^2, xy^2t, xzt^2, xz^2t, yzt^2, yz^2t\} \\ & \quad \cup \{x^3t, xt^3, y^3t, yt^3, z^3t, zt^3\}, \\ xytP^2, & P \in \{xyzt, xyz^2, xy^2z, xzt^2, xz^2t, yzt^2, yz^2t\} \\ & \quad \cup \{x^3z, xz^3, y^3z, yz^3, z^3t, zt^3\}, \\ xztP^2, & P \in \{yzt^2, yz^2t, y^3z, yz^3, y^3t, yt^3\}. \end{cases}$$

De plus $\dim \mathcal{P}^{11}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{11} = 64$, $(\mathcal{P}^{11}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{11}_{x} = \varnothing$, $\mathcal{B}^{11}_{xy}$ est composé de $xyz(xy)^2x^4$, $xyz(xy)^2y^4$ et $\mathcal{B}^{11}_{xyz}$ est composé de 8 monômes

$$xyzP^2, P \in \{xyz^2, xy^2z, x^3y, xy^3, x^3z, xz^3, y^3z, yz^3\}.)$$

Proposition 6.12 *Soit $d = 13$. Alors forme une base de $\pi(\mathcal{W}^{13} \cap \mathcal{P}_{xyzt})$ l'image par π de 23 monômes*

$$\begin{cases} xyz(xyt)^2P^4, & P \in \{x, y, z, t\}, \\ xyz(xzt)^2P^4, & P \in \{x, y, z, t\}, \\ xyz(yzt)^2P^4, & P \in \{y, z, t\}, \\ xyt(xzt)^2P^4, & P \in \{x, y, z, t\}, \\ xyt(yzt)^2P^4, & P \in \{y, z, t\}, \\ xzt(yzt)^2P^4, & P \in \{y, z, t\}, \\ (xyz)^3t^4, (xyt)^3z^4. \end{cases}$$

De plus $\dim \mathcal{P}^{13}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{13} = 35$, $(\mathcal{P}^{13}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{13}_{x} = \mathcal{B}^{13}_{xy} = \varnothing$ et $\mathcal{B}^{13}_{xyz}$ est composé de $(xyz)^3x^4$, $(xyz)^3y^4$, $(xyz)^3z^4$.)

Proposition 6.13 *Soit $d = 14$. Alors l'image par π de 13 monômes*

$$\begin{array}{llll} xy(xz)^2(xt)^4, & xy(xz)^2(zt)^4, & xy(xt)^2(zt)^4, & \\ xy(yz)^2(yt)^4, & xy(yz)^2(zt)^4, & xy(yt)^2(zt)^4, & \\ xz(yz)^2(zt)^4, & xz(yt)^2(zt)^4, & xt(yt)^2(zt)^4, & \\ xy(xz)^2(yt)^4, & (xy)^3(zt)^4, & xy(zt)^6, & xz(yt)^6, \end{array}$$

forme une base de $\pi(\mathcal{W}^{14} \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^{14}_{\mathcal{A}} = 50$, $\dim(\operatorname{Ker}\psi)^{14} = 35$, $(\mathcal{P}^{14}_{\mathcal{A}})^{\mathcal{GL}} = \mathbb{F}_2\langle \pi(d_0^*)\rangle$, *où* $d_0^* := (xy)^3(zt)^4 + xy(zt)^6$.

(Rappelons que $\mathcal{B}^{14}_{x} = \varnothing$, $\mathcal{B}^{14}_{xy} = \{(xy)^7\}$ et $\mathcal{B}^{14}_{xyz}$ est composé de $xy(xz)^6$, $xy(yz)^6$, $xz(yz)^6$, $xy(xz)^2(yz)^4$.)

Proposition 6.14 *Soit $d = 15$. Alors forme une base $\pi(\mathcal{W}^{15} \cap \mathcal{P}_{xyzt})$ l'image par π de 37 monômes*

$$\begin{cases} xyzP^2, & P \in \mathcal{B}^6_{xyt} \cup \mathcal{B}^6_{xzt} \cup \mathcal{B}^6_{yzt} \cup \{(xt)^3, (yt)^3, (zt)^3, xy(zt)^2, xz(yt)^2\}, \\ xytP^2, & P \in \mathcal{B}^6_{xzt} \cup \mathcal{B}^6_{yzt} \cup \{(xz)^3, (yz)^3, (zt)^3, xy(zt)^2, xz(yt)^2\}, \\ xztP^2, & P \in \mathcal{B}^6_{yzt} \cup \{(yz)^3, (yt)^3, xz(yz)^2, xt(yt)^2, xz(yt)^2\}, \\ xy^2z^4t^8, \end{cases}$$

où $\mathcal{B}^6_{xyz} = \{xy(xz)^2, xy(yz)^2, xz(yz)^2\}$. *De plus* $\dim \mathcal{P}^{15}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{15} = 75$, $(\Gamma^{\mathcal{A}}_{15})_{\mathcal{GL}} = \mathbb{F}_2\langle \iota^*(a_1^{(15)})\rangle$.

(Rappelons que $\mathcal{B}^{15}_{x} = \{x^{15}\}$, $\mathcal{B}^{15}_{xy} = \{xy^{14}\}$ et $\mathcal{B}^{15}_{xyz}$ est composé de xy^2z^{12} et les monômes

$$xyzP^2,\ P \in \{xy(xz)^2, xy(yz)^2, xz(yz)^2, (xy)^3, (xz)^3, (yz)^3\}.)$$

Proposition 6.15 *Soit $d = 16$. Alors l'image par π de 11 monômes*

$$\begin{array}{llll} xyx^2z^4t^8, & xyy^2z^4t^8, & xyz^2t^{12}, & \\ xzy^2z^4t^8, & xzy^2t^{12}, & xty^2z^4t^8, & xty^2z^{12}, \\ xy(xzt)^2(yz)^4, & xy(xzt)^2(yt)^4, & xy(xzt)^2(zt)^4, & xy(yzt)^2(zt)^4, \end{array}$$

forme une base de $\pi(\mathcal{W}^{16} \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^{16}_{\mathcal{A}} = 73$, $\dim(\operatorname{Ker}\psi)^{16} = 49$, $(\mathcal{P}^{16}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{16}_{x} = \varnothing$, $\mathcal{B}^{16}_{xy}$ est composé de xyx^{14}, xyy^{14}, xyx^2y^{12}, et $\mathcal{B}^{16}_{xyz}$ est composé de xyx^2z^{12}, xyy^2z^{12}, xzy^{14}, xzy^2z^{12}, xyz^{14}.)

Proposition 6.16 *Soit $d = 17$. Alors forme une base de $\pi(\mathcal{W}^{17} \cap \mathcal{P}_{xyzt})$ l'image par π de 47 monômes*

$$\left\{\begin{array}{ll} xyzP^2, & P \in \{xy^2t^4, xz^2t^4, yz^2t^4, xt^6, yt^6, zt^6, t^7\}, \\ xytP^2, & P \in \{xy^2z^4, xz^2t^4, yz^2t^4, xz^6, yz^6, zt^6, z^7\}, \\ xztP^2, & P \in \{yz^2t^4, yz^6, yt^6, y^7\}, \\ xyz(xyt)^2P^4, & P \in \{xy, xz, xt, yz, yt, zt\}, \\ xyz(xzt)^2P^4, & P \in \{xz, xt, yz, yt, zt\}, \\ xyz(yzt)^2P^4, & P \in \{yz, yt, zt\}, \\ xyt(xzt)^2P^4, & P \in \{xz, xt, yz, yt, zt\}, \\ xyt(yzt)^2P^4, & P \in \{yz, yt, zt\}, \\ xzt(yzt)^2P^4, & P \in \{yz, yt, zt\}, \\ (xyz)^3P^4, & P \in \{xt, yt, zt\}, \\ (xyt)^3(zt)^4. & \end{array}\right.$$

De plus $\dim \mathcal{P}^{17}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{17} = 87$, $(\mathcal{P}^{17}_{\mathcal{A}})^{\mathcal{GL}} = \mathbb{F}_2\langle\pi(e^*_0)\rangle$, où

$$e^*_0 := x^{14}yzt + xy^{14}zt + xyz^{14}t + xyzt^{14}.$$

(Rappelons que $\mathcal{B}^{17}_{x} = \mathcal{B}^{17}_{xy} = \varnothing$ et $\mathcal{B}^{17}_{xyz}$ est composé de 10 monômes

$$\left\{\begin{array}{ll} xyzP^2, & P \in \{xy^2z^4, xy^6, xz^6, yz^6, x^7, y^7, z^7\}, \\ (xyz)^3P^4, & P \in \{xy, xz, yz\}.) \end{array}\right.$$

Proposition 6.17 *Soit $d = 18$. Alors forme une base de $\pi(\mathcal{W}^{18} \cap \mathcal{P}_{xyzt})$ l'image par π de 25 monômes*

$$\left\{\begin{array}{ll} xyP^2, & P \in \mathcal{B}^8_{xzt} \cup \mathcal{B}^8_{yzt} \cup \mathcal{B}^8_{zt} \backslash \{xz(xzt)^2, yz(yzt)^2\}, \\ xzP^2, & P \in \mathcal{B}^8_{yzt} \cup \mathcal{B}^8_{yt} \backslash \{yzy^2t^4, yz(yzt)^2\}, \\ xtP^2, & P \in \{ytz^2t^4, ytz^6\}, \\ xyP^2, & P \in \{xyz^2t^4, xzy^2t^4, xz(yzt)^2\}, \end{array}\right.$$

où $\mathcal{B}^8_{xy} = \{xyx^6, xyx^2y^4, xyy^6\}$ et $\mathcal{B}^8_{xyz}$ est composé de xyx^2z^4, xyy^2z^4, xyz^6, xzy^2z^4, xzy^6, $xy(xyz)^2$. De plus $\dim \mathcal{P}^{18}_{\mathcal{A}} = 126$, $\dim(\operatorname{Ker}\psi)^{18} = 91$, $(\mathcal{P}^{18}_{\mathcal{A}})^{\mathcal{GL}} = \mathbb{F}_2 \oplus \mathbb{F}_2\langle\pi(f^*_0)\rangle$, où $f^*_0 := x^3y^3z^4t^8 + x^4y^8z^3t^3 + x^3y^3z^6t^6 + x^6y^6z^3t^3$.

(Rappelons que $\mathcal{B}^{18}_{x} = \varnothing$, $\mathcal{B}^{18}_{xy}$ est composé de $(xy)^3x^{12}$, $(xy)^3y^{12}$, $(xy)^3x^4y^8$, et $\mathcal{B}^{18}_{xyz}$ est composé de 12 monômes

$$\begin{array}{llll} xy(xz)^2x^{12}, & xy(xz)^2z^{12}, & xy(xz)^2x^4z^8, & xy(yz)^2y^{12}, \\ xy(yz)^2z^{12}, & xy(yz)^2y^4z^8, & xz(yz)^2y^{12}, & xz(yz)^2z^{12}, \\ xz(yz)^2y^4z^8, & xy(xz)^2y^{12}, & (xy)^3z^{12}, & xy(xz)^2y^4z^8.) \end{array}$$

Proposition 6.18 *Soit $d = 19$. Alors forme une base de $\pi(\mathcal{W}^{19} \cap \mathcal{P}_{xyzt})$ l'image par π de 80 monômes*

$$\left\{ \begin{array}{ll} xyzP^2, & P \in \mathcal{B}^8_{xyt} \cup \mathcal{B}^8_{xzt} \cup \mathcal{B}^8_{yzt} \cup \mathcal{B}^8_{xt} \cup \mathcal{B}^8_{yt} \cup \mathcal{B}^8_{zt} \cup E^8, \\ xytP^2, & P \in \mathcal{B}^8_{xyz} \cup \mathcal{B}^8_{xzt} \cup \mathcal{B}^8_{yzt} \cup \mathcal{B}^8_{xz} \cup \mathcal{B}^8_{yz} \cup \mathcal{B}^8_{zt} \cup E^8, \\ xztP^2, & P \in \mathcal{B}^8_{yzt} \cup \mathcal{B}^8_{yz} \cup \mathcal{B}^8_{yt} \cup E^8, \end{array} \right.$$

où $\mathcal{B}^8_{xy} = \{xyx^6, xyx^2y^4, xyy^6\}$, $\mathcal{B}^8_{xyz}$ est composé de xyx^2z^4, xyy^2z^4, xyz^6, xzy^2z^4, xzy^6, $xy(xyz)^2$, et E^8 est l'ensemble des 7 monômes mentionnés dans la Proposition 6.8. De plus $\dim \mathcal{P}^{19}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{19} = 140$, $(\mathcal{P}^{19}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{19}_{x} = \mathcal{B}^{19}_{xy} = \varnothing$ et $\mathcal{B}^{19}_{xyz}$ est composé de 15 monômes

$$xyzP^2, P \in \mathcal{B}^8_{xyz} \cup \mathcal{B}^8_{xy} \cup \mathcal{B}^8_{xz} \cup \mathcal{B}^8_{yz}.)$$

Proposition 6.19 *Soit $d = 21$. Alors l'image par π de 66 monômes*

$$\left\{ \begin{array}{ll} xyz(xyt)^2P^4, & P \in \{x^3, y^3, z^3, t^3, xy^2, xz^2, xt^2, yz^2, yt^2, zt^2, xyt, xzt, yzt\}, \\ xyz(xzt)^2P^4, & P \in \{x^3, y^3, z^3, t^3, xy^2, xz^2, xt^2, yz^2, yt^2, zt^2, xzt, yzt\}, \\ xyz(yzt)^2P^4, & P \in \{y^3, z^3, t^3, yz^2, yt^2, zt^2, yzt\}, \\ xyt(xzt)^2P^4, & P \in \{x^3, y^3, z^3, t^3, xy^2, xz^2, xt^2, yz^2, yt^2, zt^2, xzt, yzt\}, \\ xyt(yzt)^2P^4, & P \in \{y^3, z^3, t^3, yz^2, yt^2, zt^2, yzt\}, \\ xzt(yzt)^2P^4, & P \in \{y^3, z^3, t^3, yz^2, yt^2, zt^2, yzt\}, \\ (xyz)^3P^4, & P \in \{xt^2, yt^2, zt^2, t^3\}, \\ (xyt)^3P^4, & P \in \{xz^2, yz^2, zt^2, z^3\}, \end{array} \right.$$

forme une base de $\pi(\mathcal{W}^{21} \cap \mathcal{P}_{xyzt})$. De plus $\dim \mathcal{P}^{21}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{21} = 94$, $(\mathcal{P}^{21}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{21}_{x} = \mathcal{B}^{21}_{xy} = \varnothing$ et $\mathcal{B}^{21}_{xyz}$ est composé de 7 monômes

$$(xyz)^3P^4, P \in \{x^3, y^3, z^3, xy^2, xz^2, yz^2, xyz\}.)$$

Proposition 6.20 *Soit $d = 22$. Alors $\pi(\mathcal{W}^{22} \cap \mathcal{P}_{xyzt})$ a une base formée de l'image par π de 26 monômes*

$$\left\{ \begin{array}{ll} xyP^2, & P \in \mathcal{B}^{10}_{xzt} \cup \mathcal{B}^{10}_{yzt} \cup \mathcal{B}^{10}_{zt} \backslash \{xz(xt)^2z^4, yz(yt)^2z^4, (xz)^3t^4, (yz)^3t^4\}, \\ xzP^2, & P \in \mathcal{B}^{10}_{yzt} \cup \mathcal{B}^{10}_{yt} \backslash \{yz(yt)^2y^4, yz(yt)^2z^4, yz(yt)^2t^4, (yz)^3t^4\}, \\ xtP^2, & P \in \{yt(zt)^2z^4, yt(zt)^2t^4\}, \\ xyP^2, & P \in \{xz(yz)^2t^4, xz(yt)^2z^4, xz(yt)^2y^4, xz(yt)^2t^4\}, \end{array} \right.$$

où $\mathcal{B}^{10}_{xy} = \{(xy)^3x^4, (xy)^3y^4\}$ et $\mathcal{B}^{10}_{xyz}$ est composé de 8 monômes

$$\begin{array}{llll} xy(xz)^2x^4, & xy(xz)^2z^4, & xy(yz)^2y^4, & xy(yz)^2z^4, \\ xz(yz)^2y^4, & xz(yz)^2z^4, & xy(xz)^2y^4, & (xy)^3z^4. \end{array}$$

De plus $\dim \mathcal{P}^{22}_{\mathcal{A}} = 116$, $\dim(\operatorname{Ker}\psi)^{22} = 70$, $(\Gamma^{\mathcal{A}}_{22})_{\mathcal{GL}} = \mathbb{F}_2\langle \iota^*(c_1 a^{(3)}_4)\rangle$, *où* [3, 5]

$$c_1 := a^{(3)}_1 a^{(3)}_2 a^{(13)}_3 + a^{(3)}_1 a^{(5)}_2 a^{(11)}_3 + a^{(3)}_1 a^{(9)}_2 a^{(7)}_3 + a^{(5)}_1 a^{(7)}_2 a^{(7)}_3.$$

(Rappelons que $\mathcal{B}_x^{22} = \varnothing$, $\mathcal{B}_{xy}^{22}$ est composé de $(xy)^7x^8$, $(xy)^7y^8$, et $\mathcal{B}_{xyz}^{22}$ est composé de 8 monômes

$$\begin{array}{llll} xy(xz)^6x^8, & xy(xz)^6z^8, & xy(yz)^6y^8, & xy(yz)^6z^8, \\ xz(yz)^6y^8, & xz(yz)^6z^8, & xy(xz)^2(yz)^4y^8, & xy(xz)^2(yz)^4z^8.) \end{array}$$

Proposition 6.21 *Soit $d = 33$. Alors $\pi(\mathcal{W}^{33} \cap \mathcal{P}_{xyzt})$ a une base formée de l'image par π de 84 monômes*

$$\left\{ \begin{array}{ll} xyzP^2, & P \in \{xy^2t^{12}, xz^2t^{12}, yz^2t^{12}, xt^{14}, yt^{14}, zt^{14}, t^{15}\}, \\ xytP^2, & P \in \{xz^2t^{12}, yz^2t^{12}, xz^{14}, yz^{14}, zt^{14}, z^{15}\}, \\ xztP^2, & P \in \{yz^2t^{12}, yz^{14}, yt^{14}, y^{15}\}, \\ xyz(xyt)^2P^4, & P \in \mathcal{B}_{xyt}^6 \cup \mathcal{B}_{xzt}^6 \cup \mathcal{B}_{yzt}^6 \cup \{xz(yz)^2, xy(zt)^2, xz(yt)^2\} \\ & \quad \cup \{(xy)^3, (xz)^3, (xt)^3, (yz)^3, (yt)^3, (zt)^3\}, \\ xyz(xzt)^2P^4, & P \in \mathcal{B}_{xzt}^6 \cup \mathcal{B}_{yzt}^6 \cup \{(xz)^3, (xt)^3, (yz)^3, (yt)^3, (zt)^3\}, \\ xyz(yzt)^2P^4, & P \in \mathcal{B}_{yzt}^6 \cup \{(yz)^3, (yt)^3, (zt)^3\}, \\ xyt(xzt)^2P^4, & P \in \mathcal{B}_{xzt}^6 \cup \mathcal{B}_{yzt}^6 \cup \{(xz)^3, (xt)^3, (yz)^3, (yt)^3, (zt)^3\}, \\ xyt(yzt)^2P^4, & P \in \mathcal{B}_{yzt}^6 \cup \{(yz)^3, (yt)^3, (zt)^3\}, \\ xzt(yzt)^2P^4, & P \in \mathcal{B}_{yzt}^6 \cup \{(yz)^3, (yt)^3, (zt)^3\}, \\ (xyz)^3P^4, & P \in \{xy(zt)^2, (xt)^3, (yt)^3, (zt)^3, xt(yt)^2, xt(zt)^2, yt(zt)^2\}, \\ (xyt)^3P^4, & P \in \{xy(zt)^2, (zt)^3\}, \end{array} \right.$$

où $\mathcal{B}_{xyz}^6 = \{xy(xz)^2, xy(yz)^2, xz(yz)^2\}$. De plus $\dim \mathcal{P}_{\mathcal{A}}^{33} = \dim(\operatorname{Ker}\psi)^{33} = 136$, $(\mathcal{P}_{\mathcal{A}}^{33})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}_x^{33} = \mathcal{B}_{xy}^{33} = \varnothing$ et $\mathcal{B}_{xyz}^{33}$ est composé de 13 monômes

$$\begin{array}{ll} xyzP^2, & P \in \{xy^2z^{12}, xy^{14}, xz^{14}, yz^{14}, x^{15}, y^{15}, z^{15}\}, \\ (xyz)^3P^4, & P \in \{(xy)^3, (xz)^3, (yz)^3, xy(xz)^2, xy(yz)^2, xz(yz)^2\}.) \end{array}$$

Proposition 6.22 (Nam [40]) *Soit $d = 61$. Alors $\pi(\mathcal{W}^{61} \cap \mathcal{P}_{xyzt})$ a une base formée de l'image par π de 33 monômes*

$$\left\{ \begin{array}{ll} xyz(xyt)^{14}P^{16}, & P \in \{x, y, t\}, \\ xyz(xzt)^{14}P^{16}, & P \in \{x, z, t\}, \\ xyz(yzt)^{14}P^{16}, & P \in \{y, z, t\}, \\ xyt(xzt)^{14}P^{16}, & P \in \{x, z, t\}, \\ xyt(yzt)^{14}P^{16}, & P \in \{y, z, t\}, \\ xzt(yzt)^{14}P^{16}, & P \in \{y, z, t\}, \\ xyz(xyt)^2(xzt)^{12}P^{16}, & P \in \{x, z, t\}, \\ xyz(xyt)^2(yzt)^{12}P^{16}, & P \in \{y, z, t\}, \\ xyz(xzt)^2(yzt)^{12}P^{16}, & P \in \{y, z, t\}, \\ xyt(xzt)^2(yzt)^{12}P^{16}, & P \in \{y, z, t\}, \\ xyz(xyt)^2(xzt)^4(yzt)^8P^{16}, & P \in \{y, z, t\}, \end{array} \right.$$

De plus $\dim \mathcal{P}_{\mathcal{A}}^{61} = \dim(\operatorname{Ker}\psi)^{61} = 45$, $(\mathcal{P}_{\mathcal{A}}^{61})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}_x^{61} = \mathcal{B}_{xy}^{61} = \varnothing$ et $\mathcal{B}_{xyz}^{61}$ est composé de $(xyz)^{15}x^{16}$, $(xyz)^{15}y^{16}$, $(xyz)^{15}z^{16}$.)

Proposition 6.23 *Soit $d = 69$. Alors $\pi(\mathcal{W}^{69} \cap \mathcal{P}_{xyzt})$ a une base formée de l'image par π de 128 monômes*

$$\begin{cases} (xyz)^3P^4, & P \in \{xy^2t^{12}, xt^{14}, yt^{14}, zt^{14}, t^{15}\}, \\ (xyt)^3P^4, & P \in \{z^{15}, zt^{14}\}, \\ xyz(xyt)^2P^4, & P \in \mathcal{B}^{15}_{xyt} \cup \mathcal{B}^{15}_{xzt} \cup \mathcal{B}^{15}_{yzt} \cup \{x^{15}, y^{15}, z^{15}, t^{15}\} \\ & \quad \cup \{xy^{14}, xz^{14}, xt^{14}, yz^{14}, yt^{14}, zt^{14}\}, \\ xyz(xzt)^2P^4, & P \in \mathcal{B}^{15}_{xzt} \cup \mathcal{B}^{15}_{yzt} \cup \{x^{15}, y^{15}, z^{15}, t^{15}\} \\ & \quad \cup \{xz^{14}, xt^{14}, yz^{14}, yt^{14}, zt^{14}\}, \\ xyz(yzt)^2P^4, & P \in \mathcal{B}^{15}_{yzt} \cup \{y^{15}, z^{15}, t^{15}, yz^{14}, yt^{14}, zt^{14}\}, \\ xyt(xzt)^2P^4, & P \in \mathcal{B}^{15}_{xzt} \cup \mathcal{B}^{15}_{yzt} \cup \{x^{15}, y^{15}, z^{15}, t^{15}\} \\ & \quad \cup \{xz^{14}, xt^{14}, yz^{14}, yt^{14}, zt^{14}\}, \\ xyt(yzt)^2P^4, & P \in \mathcal{B}^{15}_{yzt} \cup \{y^{15}, z^{15}, t^{15}, yz^{14}, yt^{14}, zt^{14}\}, \\ xzt(yzt)^2P^4, & P \in \mathcal{B}^{15}_{yzt} \cup \{y^{15}, z^{15}, t^{15}, yz^{14}, yt^{14}, zt^{14}\}, \\ xyz(xyt)^2(xzt)^4P^8, & P \in \{(yz)^3, (yt)^3, yz(yt)^2, yz(zt)^2, yt(zt)^2\}, \end{cases}$$

où $\mathcal{B}^{15}_{xyz}$ est composé de xy^2z^{12} et des monômes

$$xyzP^2,\ P \in \{xy(xz)^2, xy(yz)^2, xz(yz)^2, (xy)^3, (xz)^3, (yz)^3\}.$$

De plus $\dim \mathcal{P}^{69}_{\mathcal{A}} = \dim(\operatorname{Ker}\psi)^{69} = 180$, $(\mathcal{P}^{69}_{\mathcal{A}})^{\mathcal{GL}} = 0$.

(Rappelons que $\mathcal{B}^{69}_{x} = \mathcal{B}^{69}_{xy} = \varnothing$ et $\mathcal{B}^{69}_{xyz}$ est composé de 13 monômes

$$\begin{cases} (xyz)^3P^4, & P \in \{xy^2z^{12}, xy^{14}, xz^{14}, yz^{14}, x^{15}, y^{15}, z^{15}\}, \\ (xyz)^7P^8, & P \in \{(xy)^3, (xz)^3, (yz)^3, xy(xz)^2, xy(yz)^2, xz(yz)^2\}.) \end{cases}$$

7 Conjectures

Dimension des indécomposables La première conjecture que nous proposons concerne $\dim \mathcal{P}_{\mathcal{A}}$. Elle a son origine dans le Théorème 1.1(ii) et dans un théorème de [40].

Supposons que $\omega = (r, k_0, \dots, k_{r+1}, m_1, \dots, m_{r+1}) \in \Omega$ vérifie

$$\begin{cases} r = k \text{ et } k_i = i \text{ pour } 1 \leq i \leq k, \\ m_i - m_{i+1} > 1 \text{ pour } 1 \leq i < k. \end{cases}$$

Alors $G_\omega \subset \mathcal{GL}$ coïncide avec le sous-groupe de Borel des matrices triangulaires supérieures inversibles, et $\deg a_\omega = (2^{m_1} - 1) + \cdots + (2^{m_k} - 1)$. D'après le Théorème 1.1(ii), le $\mathcal{GL}$-module $\mathcal{GL}\langle a_\omega\rangle$ est isomorphe à $\mathbb{F}_2\langle \mathcal{GL}/G_\omega\rangle$.

Conjecture 7.1 (i) *$\mathcal{GL}\langle a_\omega\rangle = \Gamma^{\mathcal{A}}_{\deg a_\omega}$ et $\dim \mathcal{P}^{\deg a_\omega}_{\mathcal{A}} = \prod_{1\leq i\leq k}(2^i - 1)$.*

(ii) *Si $d \neq \deg a_\omega$ pour tout $\omega \in \Omega$ vérifiant les conditions énumérées plus haut, alors $\dim \mathcal{P}^d_{\mathcal{A}} < \prod_{1\leq i\leq k}(2^i - 1)$.*

Cohomologie de l'algèbre de Steenrod La seconde conjecture que nous avons à proposer concerne $H^*(\mathcal{A})$. Son origine réside dans le Théorème 1.2(iii) et dans un problème que nous a suggéré Nick Kuhn. Comme à l'ordinaire, on note $\alpha(t)$ le nombre d'occurences du chiffre 1 dans l'écriture binaire de t.

Conjecture 7.2 *Soient $t \geq s \geq 1$ des entiers.*

(i) *Si $\alpha(t) > s$, alors $Ext^{s,t}_{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) = 0$.*

(ii) *Si $t = 2^{m_1} + \cdots + 2^{m_s}$ et $m_i - m_{i+1} > 1$ pour $1 \leq i < s$, alors*

$$Ext^{s,t}_{\mathcal{A}}(\mathbb{F}_2, \mathbb{F}_2) = \mathbb{F}_2 = \mathbb{F}_2\langle h_{m_1} \cdots h_{m_s}\rangle.$$

8 Appendice

8.1 Logiciel de Bruner

Soit $\mathcal{P}$ l'algèbre polynomiale à $k = 4$ variables. Écrit en langage Magma [6], le logiciel suivant de Bob Bruner calcule la dimension de $\mathcal{P}_{\mathcal{A}}$ en degré inférieur à 35 et, étant donné un polynôme homogène $P \in \mathcal{P}$, vérifie si $P \in \bar{\mathcal{A}}\mathcal{P}$.

```
%% ------ The main program ----------------
%% P is the polynomial ring in 4 variables.
%% RP is used to compute the total Steenrod operation
%% PSq(i,x) computes Sq^i(x)
%% Mon[i] contains the monomials of degree i
%% V[i] is the vector space spanned by monomials of degree i
%% MV[i] is the set of polynomials of degree i the form
%%      Sq^j(x), where j is 1,2,4,8,... and x is a monomial
%%      of degree i-j
%% AV[i] is the subspace of V[i] spanned by MV[i], that is
%%      the degree i part of the decomposables

MWD := MonomialsOfWeightedDegree;
CV := CharacteristicVector;
N := 35;
s := [2^j : j in [0..N] | 2^j lt N];
P<x1,x2,x3, x4> := PolynomialRing(GaloisField(2),[1,1,1,1]);
RP<t> := PolynomialRing(P);
j1 := x1 + t*x1^2; j2 := x2 + t*x2^2;
j3 := x3 + t*x3^2; j4 := x4 + t*x4^2;
hP := hom<P->RP | j1, j2, j3, j4>;

PSq := function(i,x)
   v := Coefficients(hP(x));
   if i ge #v then return P!0;
               else return v[i+1];
   end if;
end function;

Mon := [ [x : x in MWD(P,i)] : i in [1..N]]; print "Mon";
V := [VectorSpace(GF(2),#x) : x in Mon]; print "V";
MV := [&join{{ PSq(j,x) : x in Mon[i-j]} : j in s | j lt i}
           : i in[1..21]]; print "MV";
AV := [sub<V[i]| {CV(V[i],{Index(Mon[i],y) : y in Terms(x)})
           : x in MV[i]} >  : i in [1..21]]; print "AV";
MV[33] := &join{{ PSq(j,x) : x in Mon[33-j]}
           : j in s | j lt 33} ; print "MV";
AV[33] := sub<V[33]|{CV(V[33],{Index(Mon[33],y) : y in Terms(x)})
           : x in MV[33]} > ; print "AV";
MV[34] := &join{{ PSq(j,x) : x in Mon[34-j]}
           : j in s | j lt 34} ; print "MV";
AV[34] := sub<V[34]|{CV(V[34],{Index(Mon[34],y) : y in Terms(x)})
           : x in MV[34]} > ; print "AV";
```

```
%% ---- The program to test the 7 elements -------------
%%  D,x,y,z,t and F are convenient abbreviations
%%  For the element in degree 16, we also test xy times its
%%    square to verify that it is decomposable

D := Dimension; x := x1; y := x2; z := x3; t := x4;
F := func <a,b,c,d | a * b^2 * c^4 * d^8 >;

n1 := 16;
a1 := F(x*y, z*t*x, z*t, 1); b1 := F(x*y, x, z, t);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;

n12 := 2 + 2*n1;
dd := CV(V[n12],{Index(Mon[n12],i) : i in Terms(x*y*(a1-b1)^2)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n12, D(AV[n12]), D(V[n12]), dd in AV[n12];
printf "Element: %o\n\n",x*y*(a1-b1)^2;

n1 := 18;
a1 := F(x*y,z*t,z,z)+F(x*y,z*t,z,t)+F(x*y,z*t,t,t);
b1 := F(x*y,z*t,x,x)+F(x*y,z*t,x,y)+F(x*y,z*t,y,y);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;

n1 := 17;
a1 :=  F(z*x*y,x,y,t)+F(z*x*y,x,t,t)
     + F(z*x*y,y,t,t)+F(z*x*y,t,t,t);
b1 :=  F(t*x*y,x,y,z)+F(t*x*y,x,z,z)
     + F(t*x*y,y,z,z)+F(t*x*y,z,z,z);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;

n1 := 21;
a1 :=  F(z*x*y,z*t*x,x,t)+F(z*x*y,z*t*x,t,t)
     + F(t*x*y,z*t*x,x,z)+F(t*x*y,z*t*x,z,z);
b1 :=  F(z*x*y,z*x*y,x,t)+F(z*x*y,z*x*y,t,t)
     + F(t*x*y,t*x*y,x,z)+F(t*x*y,t*x*y,z,z);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;
```

```
n1 := 33;
a1 :=  F(z*x*y,z*t*x,t*x,z*t)+F(z*x*y,z*t*x,t*y,z*t)
       F(z*x*y,z*t*y,t*y,z*t)+F(z*x*y,z*x*y,x*y,z*t)
     + F(z*x*y,t*x*y,x*y,z*t);
b1 :=  F(t*x*y,z*t*x,z*x,z*t)+F(t*x*y,z*t*y,z*y,z*t)
     + F(t*x*y,z*t*x,z*y,z*t)+F(t*x*y,t*x*y,x*y,z*t);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;

n1 := 19;
a1 :=  F(z*x*y,x*y,y,t)+F(z*x*y,t*y,y,t)
     + F(z*x*y,t*y,t,t)+F(z*x*y,x*y,t,t);
b1 :=  F(t*x*y,x*y,z*t*y,1)+F(t*x*y,t*y,z*t*y,1)
     + F(t*x*y,x*y,z,t)+F(t*x*y,z*y,z,t);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;

n1 := 14;
a1 := F(x*y,x*y,z*t,1); b1 := F(x*y,z*t,z*t,1);
d := CV(V[n1],{Index(Mon[n1],i) : i in Terms(a1-b1)});
printf "\degree %o: decomposables (%o dim) in %o dim: %o\n",
  n1, D(AV[n1]), D(V[n1]), d in AV[n1];
printf "Element: %o\n\n",a1-b1;

%% ------------ The results -------------------------

Loading "tests"
degree 16: decomposables (896 dim) in 969 dim: false
Element: x^3*y*z^6*t^6 + x^3*y*z^4*t^8

degree 34: decomposables (7605 dim) in 7770 dim: true
Element: x^7*y^3*z^12*t^12 + x^7*y^3*z^8*t^16

degree 18: decomposables (1204 dim) in 1330 dim: false
Element: x^13*y*z^2*t^2 + x^5*y^9*z^2*t^2 + x*y^13*z^2*t^2 +
x*y*z^14*t^2 + x*y*z^6*t^10 + x*y*z^2*t^14

degree 17: decomposables (1053 dim) in 1140 dim: false
Element: x^3*y^5*z^8*t + x^3*y^5*z*t^8 + x^3*y*z^12*t +
x^3*y*z*t^12 + x*y^3*z^12*t + x*y^3*z*t^12 + x*y*z^14*t +
x*y*z*t^14

degree 21: decomposables (1930 dim) in 2024 dim: false
Element: x^7*y^3*z^8*t^3 + x^7*y^3*z^3*t^8 + x^7*y*z^10*t^3 +
x^7*y*z^3*t^10 + x^3*y^3*z^12*t^3 + x^3*y^3*z^3*t^12 +
x^3*y*z^14*t^3 + x^3*y*z^3*t^14
```

```
degree 33: decomposables (7004 dim) in 7140 dim: false
Element: x^7*y^7*z^11*t^8 + x^7*y^7*z^9*t^10 + x^7*y^7*z^8*t^11 +
x^7*y*z^14*t^11 + x^7*y*z^11*t^14 + x^3*y^5*z^14*t^11 +
x^3*y^5*z^11*t^14 + x*y^7*z^14*t^11 + x*y^7*z^11*t^14

degree 19: decomposables (1400 dim) in 1540 dim: false
Element: x^3*y^7*z^4*t^5 + x^3*y^7*z*t^8 + x^3*y^3*z^4*t^9 +
x^3*y^3*z*t^12 + x*y^7*z^4*t^7 + x*y^7*z*t^10 + x*y^3*z^6*t^9 +
x*y^3*z*t^14

degree 14: decomposables (630 dim) in 680 dim: false
Element: x^3*y^3*z^4*t^4 + x*y*z^6*t^6

%% ------------ The End ---------------------------
```

8.2 Travaux de Kameko

Soient $\mathcal{P}$ l'algèbre polynomiale à $k = 4$ variables et $d = (2^{t+s+u} - 1) + (2^{s+u} - 1) + (2^u - 1)$ avec $t, s, u \geq 0$. Les tableaux suivants donnent toutes les valeurs possibles de $\dim \mathcal{P}^d_{\mathcal{A}}$. Le nombre entre parenthèses, si présent, indique le degré d.

$u = 0$

	$s=0$	$s=1$	$s=2$	$s=3$	$s=4$	$s=5$	$s\geq 6$
$t=0$	$1^{(0)}$	$4^{(1)}$	$14^{(3)}$	$35^{(7)}$	$75^{(15)}$	$89^{(31)}$	$85^{(63)}$
$t=1$	$6^{(2)}$	$21^{(4)}$	$55^{(8)}$	$73^{(16)}$	$95^{(32)}$	$115^{(64)}$	125
$t=2$	$24^{(6)}$	$70^{(10)}$	$126^{(18)}$	$165^{(34)}$	$179^{(66)}$	175	175
$t=3$	$50^{(14)}$	$116^{(22)}$	$192^{(38)}$	$241^{(70)}$	255	255	255
$t=4$	$70^{(30)}$	$164^{(46)}$	$240^{(78)}$	285	300	300	300
$t\geq 5$	$80^{(62)}$	$175^{(94)}$	255	300	315	315	315

$u = 1$

	$s=0$	$s=1$	$s=2$	$s=3$	$s=4$	$s\geq 5$
$t=0$	$14^{(3)}$	$15^{(5)}$	$46^{(9)}$	$87^{(17)}$	$136^{(33)}$	$150^{(65)}$
$t=1$	$35^{(7)}$	$64^{(11)}$	$140^{(19)}$	$120^{(35)}$	$120^{(67)}$	120
$t=2$	$75^{(15)}$	$155^{(23)}$	$225^{(39)}$	$225^{(71)}$	225	225
$t=3$	$89^{(31)}$	$140^{(47)}$	$210^{(79)}$	210	210	210
$t\geq 4$	$85^{(63)}$	$140^{(95)}$	210	210	210	210

$u = 2$

	$s=0$	$s=1$	$s=2$	$s=3$	$s=4$	$s\geq 5$
$t=0$	$46^{(9)}$	$35^{(13)}$	$94^{(21)}$	$135^{(37)}$	$180^{(69)}$	195
$t=1$	$87^{(17)}$	$120^{(25)}$	$225^{(41)}$	$210^{(73)}$	210	210
$t=2$	$136^{(33)}$	$210^{(49)}$	$315^{(81)}$	315	315	315
$t\geq 3$	$150^{(65)}$	$210^{(97)}$	315	315	315	315

$u = 3$

	$s=0$	$s=1$	$s=2$	$s=3$	$s=4$	$s\geq 5$
$t=0$	$94^{(21)}$	$45^{(29)}$	$105^{(45)}$	$150^{(77)}$	195	210
$t=1$	$135^{(37)}$	$120^{(53)}$	$225^{(85)}$	210	210	210
$t=2$	$180^{(69)}$	210	315	315	315	315
$t\geq 3$	195	210	315	315	315	315

$u \geq 4$

	$s=0$	$s=1$	$s=2$	$s=3$	$s=4$	$s\geq 5$
$t=0$	$105^{(45)}$	$45^{(61)}$	$105^{(93)}$	150	195	210
$t=1$	$150^{(77)}$	120	225	210	210	210
$t=2$	195	210	315	315	315	315
$t\geq 3$	210	210	315	315	315	315

Les tableaux suivants donnent $\dim \mathcal{P}^d_{\mathcal{A}}$ pour $d \leq 99$.

d	1	2	3	4	5	6	7	8	9	10	11	12	13
$\dim \mathcal{P}^d_{\mathcal{A}}$	4	6	14	21	15	24	35	55	46	70	64	21	35

d	14	15	16	17	18	19	20	21	22	23	24	25
$\dim \mathcal{P}^d_{\mathcal{A}}$	50	75	73	87	126	140	55	94	116	155	70	120

d	26	27	28	29	30	31	32	33	34	35	36	37
$\dim \mathcal{P}^d_{\mathcal{A}}$	64	0	21	45	70	89	95	136	165	120	73	135

d	38	39	40	41	42	43	44	45	46	47	48
$\dim \mathcal{P}^d_{\mathcal{A}}$	192	225	126	225	140	0	55	105	164	140	116

d	49	50	51	52	53	54	55	56	57	58	59	60
$\dim \mathcal{P}^d_{\mathcal{A}}$	210	155	0	70	120	120	0	64	0	0	0	21

d	61	62	63	64	65	66	67	68	69	70	71
$\dim \mathcal{P}^d_{\mathcal{A}}$	45	80	85	115	150	179	120	95	180	241	225

d	72	73	74	75	76	77	78	79	80	81	82
$\dim \mathcal{P}^d_{\mathcal{A}}$	165	210	120	0	73	150	240	210	192	315	225

d	83	84	85	86	87	88	89	90	91	92	93
$\dim \mathcal{P}^d_{\mathcal{A}}$	0	126	225	225	0	140	0	0	0	55	105

d	94	95	96	97	98	99
$\dim \mathcal{P}^d_{\mathcal{A}}$	175	140	164	210	140	0

Références

[1] J. F. Adams, On the non-existence of elements of Hopf invariant one, *Ann. of Math.* **72** (1960), 20–104.

[2] J. F. Adams, On the structure and applications of the Steenrod algebra, *Comment. Math. Helv.* **32** (1958), 180–214.

[3] M. A. Alghamdi, M. C. Crabb and J. R. Hubbuck, Representations of the homology of BV and the Steenrod algebra I, *London Math. Soc. Lecture Note Ser.* **176** (1992), 217–234.

[4] M. G. Barratt and S. Priddy, On the homology of non-connected monoids and their associated groups, *Comment. Math. Helv.* **47** (1972), 1–14.

[5] J. M. Boardman, Modular representations on the homology of powers of real projective spaces, *Contemp. Math.* **146** (1993), 49–70.

[6] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I : The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[7] A. K. Bousfield, E. B. Curtis, D. M. Kan, D. G. Quillen, D. L. Rector and J. W. Schlesinger, The mod p lower central series and the Adams spectral sequence, *Topology* **5** (1966), 331–342.

[8] R. Bruner, L. M. Hà and N. H. V. Hung, On behavior of the algebraic transfer, preprint.

[9] M. C. Crabb and J. R. Hubbuck, Representations of the homology of BV and the Steenrod algebra II, *Progr. Math.* **136** (1996), 143–154.

[10] M. D. Crossley, $\mathcal{A}(p)$ generators for H^*V and Singer's homological transfer, *Math. Z.* **230** (1999), 401–411.

[11] E. B. Curtis, The Dyer–Lashof algebra and the Λ-algebra, *Illinois J. Math.* **19** (1975), 231–246.

[12] E. Dyer and R. K. Lashof, Homology of iterated loopspaces, *Amer. J. Math.* **84** (1962), 35–88.

[13] S. Eilenberg and S. MacLane, On the groups $H(\pi, n)$, I, *Ann. of Math.* **58** (1953), 55–106.

[14] P. Goerss, Unstable projectives and stable Ext : with applications, *Proc. London Math. Soc.* **53** (1986), 539–561.

[15] L. M. Hà, Sub-Hopf algebras of the Steenrod algebra and the Singer transfer, in preparation.

[16] N. H. V. Hung, Spherical classes and the algebraic transfer, *Trans. Amer. Math. Soc.* **349** (1997), 3893–3910. Erratum **355** (2003), 3841–3842.

[17] N. H. V. Hung, The cohomology of the Steenrod algebra and representations of the general linear groups, preprint.

[18] N. H. V. Hung and T. N. Nam, The hit problem for the Dickson algebra, *Trans. Amer. Math. Soc.* **353** (2001), 5029–5040.

[19] M. Kameko, *Products of projective spaces as Steenrod modules*, Ph.D. Thesis, Johns Hopkins University, May 1990.

[20] M. Kameko, Generators of the cohomology of BV_4, in preparation.

[21] J. Lannes et S. Zarati, Foncteurs dérivés de la déstabilisation, *C. R. Acad. Sci. Paris Sér. I Math.* **296** (1983), 573–576.

[22] J. Lannes et S. Zarati, Invariants de Hopf d'ordre supérieur et suite spectrale d'Adams, *C. R. Acad. Sci. Paris Sér. I Math.* **296** (1983), 695–698.

[23] J. Lannes et S. Zarati, Sur les foncteurs dérivés de la déstabilisation, *Math. Z.* **194** (1987), 25–59.

[24] W. H. Lin, Some differentials in the Adams spectral sequence for spheres, preprint.

[25] A. Liulivicius, *The factorization of cyclic reduced powers by secondary operations*, Mem. Amer. Math. Soc., No. **42**, 1962.

[26] S. Mac Lane, *Homology*, Classics in Mathematics, Springer–Verlag, Berlin, 1995.

[27] I. Madsen, On the action of the Dyer–Lashof algebra in $H_*(G)$, *Pacific J. Math.* **60** (1975), 235–275.

[28] M. Mahowald and M. Tangora, An infinite subalgebra of $Ext_{\mathcal{A}}(\mathbb{Z}_2, \mathbb{Z}_2)$, *Trans. Amer. Math. Soc.* **132** (1968), 263–274.

[29] B. M. Mann, E. Y. Miller and H. R. Miller, S^1-equivariant function spaces and characteristic classes, *Trans. Amer. Math. Soc.* **295** (1986), 233–256.

[30] H. R. Margolis, *Spectra and the Steenrod algebra*, North–Holland Mathematical Library, Vol. **29**, 1983.

[31] H. Margolis, S. Priddy and M. Tangora, Another systematic phenomenon in the cohomology of the Steenrod algebra, *Topology* **10** (1970), 43–46.

[32] J. P. May, *The cohomology of restricted Lie algebras and Hopf algebras, applications to the Steenrod algebra*, Ph.D. Thesis, Princeton University, 1964.

[33] J. Milnor, The Steenrod algebra and its dual, *Ann. of Math.* **67** (1958), 150–171.

[34] N. Minami, The Adams spectral sequence and the triple transfer, *Amer. J. Math.* **117** (1995), 965–985.

[35] N. Minami, On the Kervaire invariant problem, *Contemp. Math.*, **220** (1998), 229–253.

[36] N. Minami, The iterated transfer analogue of the new doomsday conjecture, *Trans. Amer. Math. Soc.* **351** (1999), 2325–2351.

[37] S. Mitchell, Splitting $B(\mathbb{Z}/p)^n$ and BT^n via modular representation theory, *Math. Z.* **189** (1985), 1–9.

[38] H. Mùi, Modular invariant theory and cohomology algebras of symmetric groups, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **22** (1975), 319–369.

[39] T. N. Nam, *Système générateur minimal de* $\mathbb{F}_2[x, y, z]$ *comme module sur l'algèbre de Steenrod* (en langue vietnamienne), Mémoire de fin d'études universitaires, Université des Sciences à Hanoï, Juin 1999.

[40] T. N. Nam, $\mathcal{A}$-générateurs génériques pour l'algèbre polynomiale, à paraître dans *Advances in Mathematics.*

[41] S. P. Novikov, On the cohomology of the Steenrod algebra (Russian), *Dokl. Akad. Nauk SSSR* **128** (1959), 893–895.

[42] J. H. Palmieri, Quillen stratification for the Steenrod algebra, *Ann. of Math.* **149** (1999), 421–449.

[43] F. P. Peterson, Generators of $H^*(\mathbb{R}P^\infty \wedge \mathbb{R}P^\infty)$ as a module over the Steenrod algebra, *Abstracts Amer. Math. Soc.* 833–55–89, April 1987.

[44] F. P. Peterson, $\mathcal{A}$-generators for certain polynomial algebras, *Math. Proc. Cambridge Philos. Soc.* **105** (1989), 311–312.

[45] D. Quillen, On the completion of a simplicial monoid, preprint.

[46] L. Schwartz, *Unstable modules over the Steenrod algebra and Sullivan's fixed point set conjecture*, Chicago Lectures in Math., 1994.

[47] W. M. Singer, On finite linear groups and the homology of the Steenrod algebra, preprint (1980).

[48] W. M. Singer, Invariant theory and the lambda algebra, *Trans. Amer. Math. Soc.* **280** (1983), 673–693.

[49] W. M. Singer, The transfer in homological algebra, *Math. Z.* **202** (1989), 493–523.

[50] N. E. Steenrod and D. B. A. Epstein, *Cohomology operations*, Ann. of Math. Stud., No. **50**, Princeton University Press, 1962.

[51] M. C. Tangora, On the cohomology of the Steenrod algebra, *Math. Z.* **116** (1970), 18–64.

[52] T. T. Trí, The irreducible modular representations of parabolic subgroups of general linear groups, *Comm. Algebra* **26** (1998), 41–47.

[53] J. S. P. Wang, On the cohomology of the mod 2 Steenrod algebra and the nonexistence of elements of Hopf invariant one, *Illinois J. Math.* **11** (1967), 480–490.

[54] C. Wilkerson, Classifying spaces, Steenrod operations and algebraic closure, *Topology* **16** (1977), 227–237.

[55] R. M. W. Wood, Steenrod squares of polynomials and the Peterson conjecture, *Math. Proc. Cambridge Philos. Soc.* **105** (1989), 307–309.

[56] R. M. W. Wood, Steenrod squares of polynomials, *London Math. Soc. Lecture Note Ser.* **139** (1989), 173–177.

[57] R. M. W. Wood, Problems in the Steenrod algebra, *Bull. London Math. Soc.* **146** (1998), 449–517.

[58] N. Yoneda, Notes on products in *Ext*, *Proc. Amer. Math. Soc.* **9** (1958), 873–875.

[59] A. Zachariou, A subalgebra of $Ext^{**}_{\mathcal{A}}(\mathbb{Z}_2, \mathbb{Z}_2)$, *Bull. Amer. Math. Soc.* **73** (1967), 647–648.

[60] A. Zachariou, A polynomial subalgebra of the cohomology of the Steenrod algebra, *Publ. Res. Inst. Math. Sci.* **9** (1973/74), 157–164.

LAGA, Université de Paris XIII, 93430 Villetaneuse, France
Electronic address : trngnam@hotmail.com, tran@math.univ-paris13.fr