Canad. J. Math. Vol. **55** (3), 2003 pp. 533–560

Automorphismes modérés de l'espace affine

Eric Edo

Résumé. Le problème de Jung-Nagata (*cf.* [J], [N]) consiste à savoir s'il existe des automorphismes de $k[x, y, z]$ qui ne sont pas modérés. Nous proposons une approche nouvelle de cette question, fondée sur l'utilisation de la théorie des automates et du polygone de Newton. Cette approche permet notamment de généraliser de façon significative les résultats de [A].

Abstract. The Jung-Nagata's problem (*cf.* [J], [N]) asks if there exists non-tame (or wild) automorphisms of $k[x, y, z]$. We give a new way to attack this question, based on the automata theory and the Newton polygon. This new approch allows us to generalize significantly the results of [A].

1 Introduction

Notation 1.1 Tout au long de cet article, k est un corps commutatif. On note $\mathrm{car}(k)$ la caractéristique de k. On pose $k^* = k \setminus \{0\}$. On considère :

- G, le groupe des automorphismes notés, $\sigma = (f, g, h)$, de la k-algèbre $k[x, y, z]$ tels que $f(0, 0, 0) = g(0, 0, 0) = h(0, 0, 0) = 0$ (pour $\sigma \in G$, la notation $\sigma = (f, g, h)$ signifie que $\sigma(x) = f$, $\sigma(y) = g$ et $\sigma(z) = h$ et la composition des automorphismes se fait de droite à gauche, *i.e.*, si $\sigma = (f, g, h)$ et $\sigma' = (f', g', h')$ alors $\sigma\sigma' = \big(f'(f, g, h), g'(f, g, h), h'(f, g, h)\big)$),
- $B = \{\sigma \in G\,;\, \sigma(x) \in k^*x + k[y, z], \sigma(y) \in k^*y + k[z], \sigma(z) \in k^*z\}$, le sous-groupe des automorphismes *triangulaires (supérieurs)*,
- $A = \mathrm{Gl}_3(k) \subset G$, le sous-groupe des automorphismes *linéaires*, $N = A \cap B$, $\mathfrak{S} = \mathfrak{S}_3 \subset A$, le groupe symétrique, $\pi = (y, x, z) \in \mathfrak{S}$, $\lambda = (x, z, y) \in \mathfrak{S}$,
- $T = \langle A \cup B\rangle_G$, le sous-groupe des automorphismes *modérés* (pour tout sous-ensemble $G_1 \subset G$, on note $\langle G_1\rangle_G$ le sous-groupe de G engendré par G_1),
- $E = \{\sigma \in G\,;\, \sigma(x) \in k^*x, \sigma(y) \in k[y, z], \sigma(z) \in k[y, z]\}$, le produit semi-direct du groupe multiplicatif k^* et du groupe des automorphismes de la k-algèbre $k[y, z]$,
- $F = \langle\{\pi\} \cup B\rangle_G$, le sous-groupe des automorphismes *fortement modérés*,
- $D = \langle\{\lambda\} \cup B\rangle_G$, le produit semi-direct du groupe additif $k[y, z]$ et de E,
- $Z = \{\sigma \in G\,;\, \sigma(z) \in k^*z\}$, le sous-groupe des z-automorphismes, produit semi-direct du groupe multiplicatif k^* et du groupe des automorphismes de la $k[z]$-algèbre $k[z][x, y]$,
- $H = \{\sigma \in A \cap B\,;\, \sigma(x) \in k^*x, \sigma(y) \in k^*y, \sigma(z) \in k^*z\}$.

La question centrale est la suivante (*cf.* [J], [N], [A] et [E]) :

Reçu par la rédaction le 13 novembre, 2001; revu le 19 mars, 2002.
Classification (AMS) par sujet: 14R10.
Mots clés: tame automorphisms, automata, Newton polygon.

Question 1.2 **([J])** A-t-on $G = T$?

Cette question est motivée par l'égalité correspondante en dimension 2 (*cf.* [J] pour le cas $k = \mathbb{C}$ et [Ku] pour le cas général).

Théorème 1.3 **([J], [Ku])** *On a :* $E = E \cap A * E \cap B$ *où* $*$ *désigne le produit libre amalgamé le long de* $E \cap N$.

Il est naturel, dans un premier temps, de restreindre la question 1.2 au sous-groupe Z. Le premier élément de $Z \setminus F$ a été construit par Nagata (*cf.* [N]).

Exemple 1.4 **([N])** Soit $\sigma = (x - 2yW - zW^2, y + zW, z)$ avec $W = y^2 + xz$, alors $\sigma \in Z \setminus F$.

Nagata conjecture que $\sigma \notin T$, mais malgré certains progrès dans cette direction (*cf.* [A], [LB] et [DGY]), cette question reste ouverte.

Dans [A], Alev utilise la décomposition de Bruhat et la présentation du groupe $\mathfrak{S}$ par les générateurs λ et π et les relations $\lambda^2 = \pi^2 = \mathrm{Id}$ et $\pi\lambda\pi = \lambda\pi\lambda$ (*cf.* [A, théorème 3.1]) pour démontrer (*cf.* [A, Proposition 3.6]) que l'automorphisme de Nagata n'admet pas certaines décompositions (écritures comme produit d'automorphismes linéaires et triangulaires) :

Proposition 1.5 **([A])** *Soit* σ *(cf. exemple 1.4) l'automorphisme de Nagata, alors :*

(1) $\sigma \notin B\pi B \cdots \pi B = F$,

(2) $\sigma \notin B\lambda B \cdots \lambda B = D$,

(3) (a) $\sigma \notin B\pi B\lambda B\pi B\lambda B\pi B$,

(b) $\sigma \notin B\pi B\lambda B\pi B\lambda B$.

Dans cet article, nous améliorons les résultats d'Alev dans deux directions, en considérant des décompositions plus générales et en démontrant que tout élément de $Z \setminus F$ (et pas seulement pour l'automorphisme de Nagata) n'admet pas de telles décompositions, (*cf.* les corollaires 12.3, 12.5 et 12.8) :

Proposition 1.6 *On a :*

(1) $(Z \setminus F) \cap FDF = \varnothing$,

(2) $(Z \setminus F) \cap FD\pi DF = \varnothing$,

(3) $(Z \setminus F) \cap FD\pi D\pi B\lambda F = \varnothing$.

Remarquons que (3) de la proposition 1.6 est un cas particulier de $(Z \setminus F) \cap FD\pi D\pi DF = \varnothing$. La proposition 1.6 est le début d'une étude systématique des décompositions où apparaissent des "boucles λ" (éléments de D).

On peut construire des éléments de Z de plusieurs façons. Par exemple, en considérant l'exponentielle d'une dérivation localement nilpotente (*cf.* [E, ch. 2, p. 43]) ou des critères explicites pour les automorphismes de petite (1 ou 2) longueur rationnelle (*cf.* [R] et [EV, théorèmes 3 et 4]).

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Étant donné un z-automorphisme $\sigma \in Z$, le théorème de Jung et van der Kulk permet de déterminer si σ est fortement modéré ou pas (*cf.* [Fu, proposition 1], [EV, corollaire 1] ou [E, ch. 5, p. 85]).

On dispose ainsi de nombreux automorphismes de $Z \setminus F$ parmi lesquels l'automorphisme de Nagata apparaît comme le plus simple (*i.e.*, celui de degré minimal) mais non comme le meilleur candidat à être non-modéré.

En résumé, on a : $F \subset T \cap Z \subset Z$ et $F \subsetneq Z$ et la question suivante se pose alors :

Question 1.7 Laquelle des trois assertions suivantes est vraie ?

(1) $F = Z \cap T \subsetneq Z$,
(2) $F \subsetneq Z \cap T \subsetneq Z$,
(3) $F \subsetneq Z \cap T = Z$.

Dans les cas (1) et (2), on aurait $T \subsetneq G$, mais dans le cas (3) répondre à la question 1.7 ne permettrait pas de répondre à la question 1.2 (cette situation serait vraiment inattendue).

Pour répondre à la question 1.7, il est indispensable d'étudier la "structure" du groupe T. Celle-ci n'est pas aussi rigide que celle de E comme le montre l'exemple suivant (*cf.* [A, exemple 2.2]).

Exemple 1.8 **([A])** Soient, dans B, $b_1 = (x + y^2, y, z)$ et $b_2 = (x + z^2, y, z)$, on a : $b_2 = \lambda b_1 \lambda$.

Le groupe T n'est donc pas le produit libre amalgamé de A et de B le long de N. Les automorphismes de T admettent plusieurs décompositions.

Dans la section 2, nous montrons (*cf.* théorème 2.13) que l'existence pour tout automorphisme modéré d'une CD-décomposition (décomposition dans laquelle le degré d'une composante croît) impliquerait que la réponse à la question 1.7 soit la première assertion.

Dans l'exemple d'Alev, l'écriture b_2 est plus courte que l'écriture $\lambda b_1 \lambda$. Dans la section 4, nous construisons un automate $\mathcal{A}$ dont la mémoire permet de réduire la longueur d'une décomposition qu'il ne reconnaît pas (*cf.* le théorème 6.7 dans la section 6) et, par exemple, de transformer la décomposition $\lambda b_1 \lambda$ en b_2.

Dans la section 3, nous donnons des exemples de décompositions et des principes permettant de les transformer en CD-décompositions.

Dans la section 7, nous formalisons ces principes pour aboutir à la notion de $\mathcal{A}$-décomposition minimale et nous montrons (*cf.* le théorème 7.7) que tout automorphisme modéré admet une $\mathcal{A}$-décomposition minimale. La question est donc de savoir si les $\mathcal{A}$-décompositions minimales sont des CD-décompositions.

L'automorphisme modéré suivant est une variante de l'automorphisme de Freudenburg (*cf.* [Fr, exemple 3] et [DGY, exemple 2.4]).

Exemple 1.9 **([Fr])** Si $\mathrm{car}(k) \neq 2$, posons $b_1 = (x + y^2, y, z)$, $b_2 = (x, y - z^3, z)$ et $b_3' = (x + \frac{3}{2}yz + z^3, y + z^2, z)$ et considérons l'automorphisme : $\sigma = \lambda b_3' \lambda b_2 \pi b_1 \pi \lambda = \left(x + \frac{3}{2}yz + y^3, z + y^2, y - z^3 - \frac{3}{4}y^2z^2 + xy(3z + 2y^2) + x^2\right)$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

La décomposition $\sigma = \lambda b_3' \lambda b_2 \pi b_1 \pi \lambda$ est une $\mathcal{A}$-décomposition minimale. La suite des degrés de la troisième composante est $1, 2, 3, 4$, ce qui montre que cette décomposition est une CD-décomposition. Cependant, le degré croît lentement et le calcul de σ fait apparaître d'importantes simplifications. Les décompositions de ce genre (appelées $\mathcal{L}_2$-décompositions minimales) ont un comportement plus complexe que celles considérées par Alev. Nous les étudions en détail et nous montrons que ce sont des CD-décompositions lorsque $\mathrm{car}(k) = 0$ (*cf.* sections 10 et 11).

2 Croissance du degré d'une composante

Dans cette section, nous introduisons la notion de CD-décomposition d'un automorphisme modéré et nous démontrons qu'un z-automorphisme est fortement modéré si, et seulement si, il admet une CD-décomposition.

Notation 2.1 On note $\mathbf{g} = \{\lambda, \pi\}$. Pour $s \in \mathbf{g}$, on définit $\bar{s}$ par $\bar{\lambda} = \pi$ et $\bar{\pi} = \lambda$.

Dans [A], apparaît l'idée de remplacer A par $\mathbf{g}$ pour engendrer T avec B. On utilise pour cela le résultat suivant (*cf.* par exemple [MT]) :

Proposition 2.2 **(Décomposition de Bruhat)**

$$A = \coprod_{s \in \mathfrak{S}} NsN.$$

Corollaire 2.3 *On a :* $T = \langle \mathfrak{S} \cup B \rangle_G = \langle \mathbf{g} \cup B \rangle_G$.

Définition 2.4 **(Décomposition)** On appelle *décomposition* (resp. **g**-*décomposition*) tout mot (*cf.* A.1) $\mathcal{D} = (h_n, \ldots, h_1)$ sur l'alphabet $\coprod_{s \in \mathfrak{S} \setminus \{\mathrm{Id}\}} sB$ (resp. $\coprod_{s \in \mathbf{g}} sB$).

Définition 2.5 **(Sous-décomposition)** Soit $\mathcal{D}$ une décomposition. Une *sous-décomposition* de $\mathcal{D}$ est un sous-mot (*cf.* A.3. (3)) de $\mathcal{D}$. Une *sous-décomposition initiale* de $\mathcal{D}$ est un suffixe (*cf.* A.3. (2)) de $\mathcal{D}$.

Définition 2.6 **(Décompositions équivalentes)** Soient $\mathcal{D} = (g_m, \ldots, g_1)$ et $\mathcal{D}' = (h_n, \ldots, h_1)$ deux décompositions. On dit que $\mathcal{D}$ et $\mathcal{D}'$ sont *quasi-équivalentes* s'il existe $b \in B$ tel que $g_m \cdots g_1 = b h_n \cdots h_1$. On dit qu'elles sont *équivalentes* si $g_m \cdots g_1 = h_n \cdots h_1$.

Définition 2.7 (CD-**décomposition**) Soit $\sigma \in T$ et soit $\mathcal{D} = (h_n, \ldots, h_1)$ une décomposition. On dit que $\mathcal{D}$ est une *décomposition de* σ, s'il existe $b \in B$ tel que $\sigma = b h_n \cdots h_1$. Pour $i \in \{1, \ldots, n\}$, on note $z_i(\mathcal{D}) = h_i \cdots h_1(z)$ et $z_*(\mathcal{D}) = z_n(\mathcal{D})$. On pose $z_{n+1}(\mathcal{D}) = \sigma(z)$. Lorsque la suite $\big(\deg z_i(\mathcal{D})\big)_{1 \le i \le n+1}$ est croissante, on dit que $\mathcal{D}$ est une CD-*décomposition de* σ. On note $\mathrm{CD}(\sigma)$ l'ensemble des CD-décompositions de σ.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Définition 2.8 **(Automate)** On appelle *automate* un automate déterministe (*cf.* définition A.6) sur l'alphabet $\coprod_{s\in\mathbf{g}} sB$ dont tous les états sont terminaux et contenant un unique état initial noté E_{Id}.

Définition 2.9 **($\mathcal{A}_0$-décomposition)** Soit $\mathcal{A}_0$ un automate. On appelle *$\mathcal{A}_0$-décomposition* toute **g**-décomposition $\mathcal{D}$ reconnue (*cf.* A.7) par l'automate $\mathcal{A}_0$.

Notation 2.10 Pour $s \in \mathfrak{S}$, on note $B^s = B \cap (s^{-1}Bs)$ et $B(s) = NB^s$.

Proposition 2.11

(1) *On a :* $B^\lambda = \{\sigma \in B \,;\, \sigma(y) \in k^*y\}$, $B^\pi = \{\sigma \in B \,;\, \sigma(x) \in k^*x + k[z]\}$, $B^{\lambda\pi} = \{\sigma \in B \,;\, \sigma(x) \in k^*x\}$, $B^{\pi\lambda} = \{\sigma \in B \,;\, \sigma(x) \in k^*x + k[y], \sigma(y) \in k^*y\}$ *et* $B^{\lambda\pi\lambda} = \{\sigma \in B \,;\, \sigma(x) \in k^*x, \sigma(y) \in k^*y\}$.
(2) *Pour tout* $s \in \mathbf{g}$, *on a* $B^sN = B(s)$.
(3) *On a :* $B(\lambda) = \{\sigma \in B \,;\, \deg\sigma(y) = 1\}$ *et* $B(\lambda\pi) = \{\sigma \in B \,;\, \deg\sigma(x) = 1\}$.

Preuve Vérifications immédiates.

Corollaire 2.12 *L'application $s \mapsto B^s$ est un anti-isomorphisme d'ensembles ordonnés entre $\mathfrak{S}$ muni de l'ordre suffixe (cf. A.3) induit (cf. A.4) par la représentation par les générateurs λ et π et les relations $\lambda^2 = \pi^2 = \mathrm{Id}$ et $\pi\lambda\pi = \lambda\pi\lambda$ et $\{B^s \,;\, s \in \mathfrak{S}\}$ muni de l'inclusion.*

Preuve Avec les notations de A.4, pour tout $s \in \mathbf{g}$, on a $\min(s) = \{(s)\}$ et $\min(s\bar{s}) = \{(s\bar{s})\}$ et $\min(\lambda\pi\lambda) = \{(\lambda,\pi,\lambda),(\pi,\lambda,\pi)\}$. L'ordre suffixe induit est donc engendré par les relations $s \le \bar{s}s \le \lambda\pi\lambda$ (où $s \in \mathbf{g}$). Par ailleurs, d'après la proposition 2.11, on a $B^{\lambda\pi\lambda} \subset B^{\bar{s}s} \subset B^s$ (où $s \in \mathbf{g}$), d'où l'anti-isomorphisme.

Théorème 2.13 *On a : $Z \cap \{\sigma \in T \,;\, \mathrm{CD}(\sigma) \neq \varnothing\} = F$. Autrement dit : un z-automorphisme est fortement modéré si et seulement s'il admet une* CD*-décomposition.*

Preuve Clairement, $F \subset Z \cap \{\sigma \in T \,;\, \mathrm{CD}(\sigma) \neq \varnothing\}$. Pour établir l'inclusion réciproque on utilise (3) de la proposition 2.11.

Soit $\sigma \in Z \cap \{\sigma \in T \,;\, \mathrm{CD}(\sigma) \neq \varnothing\}$. Pour $\mathcal{D} \in \mathrm{CD}(\sigma)$, on note :

$$\mathrm{lgz}(\mathcal{D}) = \max\big\{\, i \in \{1,\dots,n\} \,;\, \forall j \in \{1,\dots,i-1\} z_j(\mathcal{D}) \in k^*z\big\}\,.$$

Considérons $\mathcal{D} = (a_nb_n,\dots,a_1b_1) \in \mathrm{CD}(\sigma)$ où $a_i \in \mathfrak{S}$ et $b_i \in B$ tel que $n = \mathrm{lg}(\mathcal{D})$ soit minimale et $i = \mathrm{lgz}(\mathcal{D})$ maximale (n fixé). La suite $\big(\deg z_i(\mathcal{D})\big)_{1\le i\le n+1}$ est croissante et $\deg z_{n+1}(\mathcal{D}) = \deg\big(\sigma(z)\big) = 1$, donc cette suite est constante et égale à 1. Supposons, par l'absurde, que $i < n$ et distingons deux cas :

Cas 1 Si $a_i(z) = x$, alors d'une part $a_i = \pi\lambda\pi^\epsilon$ avec $\epsilon \in \{0,1\}$ et d'autre part $\deg\big(b_{i+1}(x)\big) = \deg\big(z_{i+1}(\mathcal{D})\big) = 1$ donc $b_{i+1} = ab$ avec $a \in N$ et $b \in B^{\lambda\pi}$. On a alors : $a_{i+1}b_{i+1}a_i = (a_{i+1}a\pi\lambda)(\lambda\pi b\pi\lambda)\pi^\epsilon$ avec $a_{i+1}a\pi\lambda \in A$ et $\lambda\pi b\pi\lambda \in B$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Cas 2 Si $a_i(z) = y$, alors d'une part $a_i = \lambda\pi^\epsilon$ avec $\epsilon \in \{0,1\}$ et d'autre part $\deg\big(b_{i+1}(y)\big) = \deg\big(z_{i+1}(\mathcal{D})\big) = 1$ donc $b_{i+1} = ab$ avec $a \in N$ et $b \in B^\lambda$. On a alors $a_{i+1}b_{i+1}a_i = (a_{i+1}a\lambda)(\lambda b\lambda)\pi^\epsilon$ avec $a_{i+1}a\lambda \in A$ et $\lambda b\lambda \in B$.

Dans les deux cas, après utilisation de la décomposition de Bruhat, on obtient un élément de $\mathrm{CD}(\sigma)$ qui contredit la minimalité de n si $\epsilon = 0$ ou la maximalité de i si $\epsilon = 1$. Finalement, on a $i = n$, donc $a_j = \pi$ pour tout $j \in \{1, \dots, n\}$, et $\sigma \in F$.

Corollaire 2.14 *Soient $f_1, f_2 \in F$ et $\sigma \in T$. Si $\mathrm{CD}(\sigma) \neq \varnothing$, alors $f_2\sigma f_1 \notin Z \smallsetminus F$.*

Preuve Si $f_2\sigma f_1 \in Z$, alors $\sigma \in Z$, donc $\sigma \in F$ car $\mathrm{CD}(\sigma) \neq \varnothing$. Donc $f_2\sigma f_1 \in F$.

Conjecture 2.15 **(Croissance du degré d'une composante)** *Pout tout $\sigma \in T$, on a :* $\mathrm{CD}(\sigma) \neq \varnothing$.

Remarque 2.16 D'après le théorème 2.13, la conjecture 2.15 implique que $Z \cap T \subset F$, or, clairement, $F \subset Z \cap T$, donc la conjecture 2.15 implique que $F = Z \cap T \subsetneq Z$ (ce qui répondrait à la question 1.7).

3 Principes et exemples

Dans cette section, nous donnons des exemples de décompositions qui ne sont pas des CD-décompositions et nous décrivons trois principes fondamentaux permettant de les transformer en CD-décompositions.

Question 3.1 Soit $\sigma \in T$. Étant donnée une décomposition $\mathcal{D}$ de σ, peut-on construire une CD-décomposition de σ quasi-équivalente à $\mathcal{D}$?

Il est naturel, pour tenter de répondre à cette question, d'utiliser la méthode des preuves et réfutations de Lakatos (*cf.* [Lak]). Nous appelons *principe* un algorithme permettant de transformer certaines décompositions en CD-décompositions (ce que Lakatos appelle "preuve"). Chaque exemple illustre l'utilisation d'un principe et "réfute" le principe précédent.

Principe 1 **(Minimalité)** *Étant donnée une décomposition, il existe une décomposition quasi-équivalente $\mathcal{D} = (h_n, \dots, h_1)$ avec $h_i = a_ib_i$ ($a_i \in \mathfrak{S}$ et $b_i \in B$), telle que $z_i(\mathcal{D})$ soit de degré minimal dans l'ensemble $B^{a_i^{-1}} z_i(\mathcal{D})$ pour $1 \leq i \leq n$.*

Preuve Pour i valant successivement $1, \dots, n$, on remplace b_i par $b_i' = a_i^{-1}c_ia_ib_i$ et b_{i+1} par $b_{i+1}'b_{i+1}c_i^{-1}$ où $c_i \in B^{a_i^{-1}}$ est tel que $c_iz_i(\mathcal{D})$ soit de degré minimal dans l'ensemble $B^{a_i^{-1}} z_i(\mathcal{D})$. On obtient ainsi une décomposition $\mathcal{D}'$ quasi-équivalente, car $b_{i+1}'a_ib_i' = (b_{i+1}c_i^{-1})a_i(a_i^{-1}c_ia_ib_i) = b_{i+1}a_ib_i$, et vérifiant la condition de minimalité, car $z_i(\mathcal{D}') = a_ib_i'z_{i-1}(\mathcal{D}) = c_iz_i(\mathcal{D})$.

Exemple 3.2 Posons $b = (x + z^2, y + z^3, z)$, $\mathcal{D}_1 = (\lambda b, \pi\lambda)$ (resp. $\mathcal{D}_2 = (\pi b, \pi\lambda)$) et $\sigma_1 = (z + y^3, y, x)$ (resp. $\sigma_2 = (x + z^3, z, y)$). La décomposition $\mathcal{D}_1$ (resp. $\mathcal{D}_2$) n'est pas une CD-décomposition de σ_1 (resp. σ_2). Grâce au principe de minimalité,

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

on construit $\mathcal{D}'_1 = (\lambda b', \pi\lambda)$ (resp. $\mathcal{D}'_2 = (\pi b', \pi\lambda)$) où $b' = (x, y + z^3, z)$, qui est une CD-décomposition de σ_1 (resp. σ_2).

Principe 2* (Générateurs)** *Étant donnée une décomposition $\mathcal{D}$, il existe une* **g-décomposition $\mathcal{D}'$ équivalente à $\mathcal{D}$.*

Preuve L'ensemble **g** engendre $\mathfrak{S}$.

Remarque 3.3 Dans la pratique, on fait apparaître des triangulaires égaux à l'identité. Pour $\lambda\pi$ et $\pi\lambda$ cela se fait de façon canonique ($\lambda\pi \mapsto (\lambda, \pi)$ et $\pi\lambda \mapsto (\pi, \lambda)$), mais pour $\lambda\pi\lambda = \pi\lambda\pi$ il faut faire un choix. Le principe 3 ci-dessous nous dicte de préférer (λ, π, λ). Cependant, dans la notion de décomposition minimale (*cf.* section 7) qui formalise ces trois principes, λ et π jouent des rôles symétriques.

Exemple 3.4 Posons $b = \big(x + z(z + y^2)^2, y, z\big)$, $\mathcal{D}_1 = (\pi\lambda b, \pi\lambda)$ et $\sigma_1 = \big(z, x - z^2, y + x^2(x - z^2)\big)$. La décomposition $\mathcal{D}_1$ vérifie le principe de minimalité, mais n'est pas une CD-décomposition de σ_1. Grâce aux principes des générateurs puis de minimalité, on construit $\mathcal{D}'_1 = (\pi b', \lambda, \pi, \lambda)$ où $b' = \big(x + y^2(y - z^2), y, z\big)$, qui est une CD-décomposition de σ_1.

Principe 3* (Relations)** *Étant donnée une* **g-décomposition $\mathcal{D}$, il existe une* **g***-décomposition $\mathcal{D}'$ équivalente à $\mathcal{D}$ et de même longueur telle qu'en notant $\mathcal{D}' = (h_n, \dots, h_1)$, pour tout $1 \leq m \leq n-2$ on ait $(h_{m+2}, h_{m+1}, h_m) \notin \{\pi\} \times \lambda B^\pi \times \pi B$.*

Preuve Si $h_{m+2} = \pi$, $h_{m+1} = \lambda b_2$ avec $b_2 \in B^\pi$ et $h_m = \pi b_1$ avec $b_1 \in B$, on peut remplacer (h_{m+2}, h_{m+1}, h_m) par $\big(\lambda, \pi, \lambda(\pi b_2 \pi) b_1\big)$ car $\pi\lambda b_2 \pi b_1 = \pi\lambda\pi(\pi b_2 \pi) b_1 = \lambda\pi\lambda(\pi b_2 \pi) b_1$.

Exemple 3.5 Posons $b = (x + z^2 - y^4, y + z^3, z)$, $\mathcal{D}_1 = (\pi, \lambda, \pi b, \lambda, \pi, \lambda)$ et $\sigma_1 = \big(x + y^2, y + (x + y^2)^3, z + x^2 + 2xy^2\big)$. La **g**-décomposition $\mathcal{D}_1$ vérifie le principe de minimalité, mais n'est pas une CD-décomposition de σ_1. Grâce aux principes des relations puis de minimalité, on construit $\mathcal{D}'_1 = (\lambda, \pi b'', \lambda b', \lambda, \pi, \lambda)$ où $b' = (x, y + z^3, z)$ et $b'' = (x + y^2 + 2yz^2, y + z^2, z)$ qui est une CD-décomposition de σ_1.

Remarque 3.6 Les principes 2 et 3 sont liés à la présentation de $\mathfrak{S}$ par générateurs et relations, ils rendent l'utilisation du principe 1 plus efficace.

4 L'automate de longueur

Définition 4.1 On dit qu'une **g**-décomposition *est de longueur* **g***-minimale* si elle est de longueur minimale dans l'ensemble des **g**-décompositions quasi-équivalentes.

Étant donnée une **g**-décomposition $\mathcal{D}$, nous ne disposons pas d'un algorithme permettant de déterminer une **g**-décomposition équivalente à $\mathcal{D}$ de longueur **g**-minimale (car nous ne disposons même pas d'un algorithme permettant de savoir si $\mathcal{D}$ est

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

de longueur **g**-minimale, *i.e.*, d'un test d'arrêt). L'automate de longueur $\mathcal{A}$ permet, cependant, de diminuer la longueur de certaines **g**-décompositions.

Soit $s \in \mathbf{g}$, par définition de B^s, on a : $BsB^s sB \subset B$. Donc si $\mathcal{D} = (h_n, \dots, h_1)$ est une **g**-décomposition de longueur **g**-minimale, pour $i \in \{1, \dots, n-1\}$, on doit avoir :

$$(*) \qquad h_i \in sB \Rightarrow h_{i+1} \notin sB^s.$$

De même l'inclusion $B\bar{s}B^{\bar{s}}sB^{s\bar{s}}\bar{s}B^s sB \subset Bs\bar{s}B$ (obtenue par un calcul utilisant la relation $s\bar{s}s = \bar{s}s\bar{s}$) se traduit par la condition suivante :

$$(**) \qquad h_{i-2} \in sB, \quad h_{i-1} \in \bar{s}B^s, \quad h_i \in sB^{s\bar{s}} \Rightarrow h_{i+1} \notin \bar{s}B^{\bar{s}}.$$

Pour connaître la condition à imposer à une lettre de $\mathcal{D}$, il est nécessaire de se souvenir des trois lettres précédentes. C'est ce que fait l'automate suivant dont les six états correspondent aux éléments du groupe symétrique.

Les états sont E_s (pour chaque $s \in \mathfrak{S}$).

Les transitions sont (pour chaque $r, s \in \mathbf{g}$) :

De	E_{Id}	vers	E_s	: sB.
De	E_r	vers	E_s	: $s(B \smallsetminus B^r)$.
De	$E_{r\bar{r}}$	vers	E_s	: $s(B \smallsetminus B^r)$.
De	$E_{\lambda\pi\lambda}$	vers	E_s	: $s\big(B \smallsetminus (B^\lambda \cup B^\pi)\big)$.
De	E_s	vers	$E_{\bar{s}\bar{s}}$	: $\bar{s}B^s$.
De	$E_{s\bar{s}}$	vers	$E_{\bar{s}\bar{s}}$	: $\bar{s}(B^s \smallsetminus B^{\bar{s}s})$.
De	$E_{\lambda\pi\lambda}$	vers	$E_{\bar{s}\bar{s}}$	: $\bar{s}\big(B^s \smallsetminus (B^{\bar{s}} \cup B^{\bar{s}s})\big)$.
De	$E_{\bar{s}\bar{s}}$	vers	$E_{\lambda\pi\lambda}$	: $sB^{s\bar{s}}$.
De	$E_{\lambda\pi\lambda}$	vers	$E_{\lambda\pi\lambda}$	: $s(B^{s\bar{s}} \smallsetminus B^s)$.

Cependant, cet automate n'est pas satisfaisant car il ne prend pas en compte les affines-triangulaires (éléments de N). Il est facile de voir (*cf.* lemme 6.4) que, pour $s \in \mathbf{g}$, on a $sNs \subset N \amalg NsN$. On en déduit que $BsB(s)sB \subset B \amalg BsB$, ce qui permet de remplacer $(*)$ par la condition suivante qui est plus restrictive :

$$(*)' \qquad h_i \in sB \Rightarrow h_{i+1} \notin sB(s).$$

On ne peut pas restreindre aussi facilement la condition $(**)$. En effet, pour réduire la longueur d'un élément de $B\bar{s}B(\bar{s})sB(s\bar{s})\bar{s}B(s)sB$, nous sommes confrontés au problème de non-commutativité suivant : $B^{s\bar{s}}\bar{s}N \neq NB^{s\bar{s}}\bar{s}$. L'état $E_{\bar{s}\bar{s}}$ doit être capable de conserver l'information de la valeur de l'affine-triangulaire situé entre le $\bar{s}$ et le s. On est ainsi amené à éclater les états $E_{\bar{s}\bar{s}}$ (resp. l'état $\lambda\pi\lambda$) en une droite (resp. en la réunion de deux plans) *cf.* remarque 4.3. (2). Ceci permet d'utiliser une propriété de commutation (*cf.* lemme 5.2) et conduit naturellement à la définition de l'automate de longueur.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Notation 4.2

(1) On pose $B//H = \{\sigma \in B\ ;\ \sigma(x) - x \in k[y,z], \sigma(y) - y \in k[z], \sigma(z) = z\}$ et pour $C \subset B$, on pose $C//H = C \cap (B//H)$.
(2) Pour $s \in \mathfrak{S}$, on note $N^s = N \cap B^s$.
(3) Pour $s \in \mathbf{g}$ et $t \in N^{s\bar{s}}//H$, on pose $N_t^{s\bar{s}} = tH$ et $B_t(s) = N_t^{s\bar{s}}(B^s//H)$.
(4) Pour $s \in \mathbf{g}$, $t \in N^{\bar{s}s}//H$ et $\alpha \in N^s//H$, on pose $N_{t,\alpha}^s = s\alpha Hs\bar{s}t^{-1}\bar{s}$ et $B_{t,\alpha}(s\bar{s}) = N_{t,\alpha}^s(B^{s\bar{s}}//H)$.

Remarque 4.3 (1) Pour tout $s \in \mathfrak{S}$, on a $Hs = sH$.

(2) Pour tout $s \in \mathbf{g}$, on a les isomorphismes canoniques de groupe suivants $N^{s\bar{s}}//H \simeq k$ (droite), $N^s//H \simeq k^2$ (plan) et $N//H \simeq k^3$, k étant considéré comme groupe additif.

Proposition 4.4

(1) *Pour tout $s \in \mathbf{g}$, $N^{s\bar{s}}$ est réunion disjointe des $N_t^{s\bar{s}}$ ($t \in N^{s\bar{s}}//H$).*
(2) *Pour tout $s \in \mathbf{g}$ et $t \in N^{\bar{s}s}//H$, N^s est réunion disjointe des $N_{t,\alpha}^s$ ($\alpha \in N^s//H$).*

Preuve Pour $s \in \mathbf{g}$, (1) résulte de $\coprod_{t \in N^{s\bar{s}}//H} tH = N^{s\bar{s}}$.

Pour $s \in \mathbf{g}$ et $t \in N^{\bar{s}s}//H$, on a $\bar{s}t^{-1}\bar{s} \in N^s$. Les applications $\beta \mapsto s\beta s$ et $\beta \mapsto \beta\bar{s}t^{-1}\bar{s}$ sont des bijections de N^s dans lui-même. Donc (2) découle de $\coprod_{\alpha \in N^s//H} \alpha H = N^s$.

Définition 4.5 **(L'automate de longueur)** On définit un automate $\mathcal{A}$:

Les états sont : E_{Id} l'état initial.

– Pour chaque $s \in \mathbf{g}$, un état E_s.
– Pour chaque $s \in \mathbf{g}$ et $t \in N^{s\bar{s}}//H$, un état $E_{\bar{s}s}(t)$.
– Pour chaque $\alpha \in (N^\lambda \cup N^\pi)//H$, un état $E_{\lambda\pi\lambda}(\alpha)$.

Les transitions sont (pour $r, s \in \mathbf{g}$, $t \in N^{s\bar{s}}//H$, $u \in N^{\bar{s}s}//H$, $v \in N^{\bar{r}r}//H$, $\alpha \in N^s//H$ et $\beta \in (N^\lambda \cup N^\pi)//H$) :

De	E_{Id}	vers	E_s	: sB.
De	E_r	vers	E_s	: $s\big(B \smallsetminus B(r)\big)$.
De	$E_{r\bar{r}}(v)$	vers	E_s	: $s\big(B \smallsetminus B(r)\big)$.
De	$E_{\lambda\pi\lambda}(\beta)$	vers	E_s	: $s\Big(B \smallsetminus \big(B(\lambda) \cup B(\pi)\big)\Big)\beta^{-1}$.
De	E_s	vers	$E_{\bar{s}s}(t)$	: $\bar{s}B_t(s)$.
De	$E_{s\bar{s}}(u)$	vers	$E_{\bar{s}s}(t)$	: $\bar{s}\big(B_t(s) \smallsetminus B(\bar{s}s)\big)$.
De	$E_{\lambda\pi\lambda}(\beta)$	vers	$E_{\bar{s}s}(t)$	: $\bar{s}\Big(B_t(s) \smallsetminus \big(B(\bar{s}) \cup B(\bar{s}s)\big)\Big)\beta^{-1}$.
De	$E_{\bar{s}s}(t)$	vers	$E_{\lambda\pi\lambda}(\alpha)$	: $sB_{t,\alpha}(s\bar{s})$.
De	$E_{\lambda\pi\lambda}(\beta)$	vers	$E_{\lambda\pi\lambda}(\alpha)$	: $s\big(B_{\mathrm{Id},\alpha}(s\bar{s}) \smallsetminus B(s)\big)\beta^{-1}$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Remarque 4.6 Les transitions sont classées ci-dessus (resp. ci-dessous) en fonction de l'état d'arrivée (de départ), ceci pour faciliter la démonstration de la proposition 5.4 (resp. du lemme 6.2).

De	E_{Id}	vers	E_s	$: sB.$
De	E_s	vers	E_r	$: r\big(B \smallsetminus B(s)\big).$
De	E_s	vers	$E_{\bar{s}s}(t)$	$: \bar{s}B_t(s).$
De	$E_{s\bar{s}}(u)$	vers	E_r	$: r\big(B \smallsetminus B(s)\big).$
De	$E_{s\bar{s}}(u)$	vers	$E_{\bar{s}s}(t)$	$: \bar{s}\big(B_t(s) \smallsetminus B(\bar{s}s)\big).$
De	$E_{s\bar{s}}(u)$	vers	$E_{\lambda\pi\lambda}(\alpha)$	$: \bar{s}B_{u,\alpha}(\bar{s}s).$
De	$E_{\lambda\pi\lambda}(\beta)$	vers	E_s	$: s\Big(B \smallsetminus \big(B(s) \cup B(\bar{s})\big)\Big)\beta^{-1}.$
De	$E_{\lambda\pi\lambda}(\beta)$	vers	$E_{\bar{s}s}(t)$	$: \bar{s}\Big(B_t(s) \smallsetminus \big(B(s) \cup B(s\bar{s})\big)\Big)\beta^{-1}.$
De	$E_{\lambda\pi\lambda}(\beta)$	vers	$E_{\lambda\pi\lambda}(\alpha)$	$: s\big(B_{\mathrm{Id},\alpha}(s\bar{s}) \smallsetminus B(s)\big)\beta^{-1}.$

5 Le lemme de l'état final

Remarque 5.1 Le lemme de l'état final (*cf.* proposition 5.4) est un résultat technique qui sert à démontrer le théorème d'automatisation (*cf.* théorème 6.7). L'idée est que si $\mathcal{D}$ est une $\mathcal{A}$-décomposition, l'information donnée par $\mathrm{fin}(\mathcal{D})$ (*cf.* A.8) se traduit par des conditions sur les dernières lettres d'une décomposition équivalente.

Lemme 5.2 *Pour $s \in \mathbf{g}$ et $f \in N^{\bar{s}s}$ on a : $s(B^{\bar{s}s}//H)sf = fs(B^{\bar{s}s}//H)s$.*

Preuve Il suffit de démontrer que $s(B^{\bar{s}s}//H)sf \subset fs(B^{\bar{s}s}//H)s$ car $N^{\bar{s}s}$ est un sous-groupe de B.

Cas 1 $s = \lambda$.
Soient $f = (ax + by, cy, dz) \in N^{\pi\lambda}$ et $g = \big(x + P(y), y\big) \in B^{\pi\lambda}//H$.
Alors $\lambda f^{-1}\lambda g\lambda f\lambda = \big(x + aP(d^{-1}y), y\big) \in B^{\pi\lambda}//H$.

Cas 2 $s = \pi$.
Soient $f = (ax, by + cz, dz) \in N^{\lambda\pi}$ et $g = \big(x, y + P(z)\big) \in B^{\lambda\pi}//H$.
Alors $\pi f^{-1}\pi g\pi f\pi = \big(x, y + aP(d^{-1}z)\big) \in B^{\lambda\pi}//H$.

Lemme 5.3 *Pour $s \in \mathbf{g}$, $t \in N^{s\bar{s}}//H$ et $\alpha \in N^s//H$, on a : $sN^s_{t,\alpha}\bar{s}N^{s\bar{s}}_t s = \alpha s\bar{s}sH$.*

Preuve On a : $sN^s_{t,\alpha}\bar{s}N^{s\bar{s}}_t s = ss\alpha Hs\bar{s}t^{-1}\bar{s}\bar{s}tHs = \alpha Hs\bar{s}Hs = \alpha s\bar{s}sH$.

Proposition 5.4 **(Lemme de l'état final)** *Étant donnée une $\mathcal{A}$-décomposition $\mathcal{D}$, il existe une $\mathbf{g}$-décomposition $\mathcal{D}' = (a_n b_n, \ldots, a_1 b_1)$ ($a_i \in \mathbf{g}$ et $b_i \in B$) équivalente, de même longueur n et telle que :*

(a) *si $\mathrm{fin}(\mathcal{D}) = E_s$ avec $s \in \mathbf{g}$ alors $a_n = s$,*

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

(b) *si* $\mathrm{fin}(\mathcal{D}) = E_{\bar{s}s}(t)$ *avec* $s \in \mathbf{g}$ *et* $t \in N^{s\bar{s}}//H$ *alors* $a_n = \bar{s}$, $b_n \in N_t^{s\bar{s}}$ *et* $a_{n-1} = s$,
(c) *si* $\mathrm{fin}(\mathcal{D}) = E_{\lambda\pi\lambda}(\alpha)$ *avec* $\alpha \in (N^\lambda \cup N^\pi)//H$ *alors* $a_n b_n a_{n-1} b_{n-1} a_{n-2} \in \alpha\lambda\pi\lambda H$.

Preuve Démontrons la proposition 5.4 par récurrence sur $\mathrm{lg}(\mathcal{D})$.

Si $\mathrm{lg}(\mathcal{D}) = 0$, alors $\mathrm{fin}(\mathcal{D}) = E_{\mathrm{Id}}$, donc on peut prendre $\mathcal{D}' = \mathcal{D}$. Soit $n \in \mathbb{N}$ un entier, supposons le résultat acquis pour les $\mathcal{A}$-décompositions de longueur inférieure ou égale à n. Soit $\mathcal{E} = (c_{n+1}d_{n+1}, \ldots, c_1 d_1)$ ($c_i \in \mathbf{g}$ et $d_i \in B$) une $\mathcal{A}$-décomposition de longueur $n+1$. En appliquant l'hypothèse de récurrence à $\mathcal{D} = (c_n d_n, \ldots, c_1 d_1)$, on obtient une décomposition équivalente $\mathcal{D}' = (a_n b_n, \ldots, a_1 b_1)$ ($a_i \in \mathbf{g}$ et $b_i \in B$) vérifiant (a)–(c). Il y a trois cas :

Cas 0 $\mathrm{fin}(\mathcal{E}) = E_s$ avec $s \in \mathbf{g}$ alors $c_{n+1} = s$ et (a) est vérifié.

Cas 1 $\mathrm{fin}(\mathcal{E}) = E_{\bar{s}s}(t)$ avec $s \in \mathbf{g}$ et $t \in N^{s\bar{s}}//H$. Il y a deux sous-cas :

Cas 1.1 $\mathrm{fin}(\mathcal{D}) = E_s$ ou $\mathrm{fin}(\mathcal{D}) = E_{s\bar{s}}(u)$ avec $u \in N^{s\bar{s}}$.
On a : $c_{n+1} = \bar{s}$, $d_{n+1} = ab$ avec $a \in N_t^{s\bar{s}}$ et $b \in B^s//H$ et $a_n = s$.
D'où : $c_{n+1}d_{n+1}a_n b_n = \bar{s}absb_n = \bar{s}as(sbsb_n)$ et $sbsb_n \in B$.
Posons $\mathcal{E}' = \left(\bar{s}a, s(sbsb_n), a_{n-1}b_{n-1}, \ldots, a_1 b_1\right)$.
La $\mathcal{A}$-décomposition $\mathcal{E}'$ est équivalente à $\mathcal{E}$ et vérifie (b).

Cas 1.2 $\mathrm{fin}(\mathcal{D}) = E_{\lambda\pi\lambda}(\beta)$ avec $\beta \in (N^\lambda \cup N^\pi)//H$.
On a : $c_{n+1} = \bar{s}$ et $d_{n+1} = ab\beta^{-1}$ avec $a \in N_t^{s\bar{s}}$ et $b \in B^s//H$ et $a_n b_n a_{n-1} b_{n-1} a_{n-2} = \beta s\bar{s}sh$ avec $h \in H$.
D'où : $c_{n+1}d_{n+1}a_n b_n a_{n-1} b_{n-1} a_{n-2} b_{n-2} = \bar{s}abs\bar{s}shb_{n-2} = \bar{s}as(sbs)\bar{s}shb_{n-2}$ et $sbs \in B$.
Posons $\mathcal{E}' = \left(\bar{s}a, s(sbs), \bar{s}, shb_{n-2}, a_{n-3}b_{n-3} \ldots, a_1 b_1\right)$.
La $\mathcal{A}$-décomposition $\mathcal{E}'$ est équivalente à $\mathcal{E}$ et vérifie (b).

Cas 2 $\mathrm{fin}(\mathcal{E}) = E_{\lambda\pi\lambda}(\alpha)$ avec $\alpha \in (N^\lambda \cup N^\pi)//H$. Il y a deux sous-cas :

Cas 2.1 $\mathrm{fin}(\mathcal{D}) = E_{\bar{s}s}(t)$ avec $s \in \mathbf{g}$ tel que $\alpha \in N^s//H$ et $t \in N^{s\bar{s}}//H$.
On a : $c_{n+1} = s$ et $d_{n+1} = ab$ avec $a \in N_{t,\alpha}^s$ et $b \in B^{s\bar{s}}//H$, $a_n = \bar{s}$, $b_n \in N_t^{s\bar{s}}$ et $a_{n-1} = s$.
D'après le lemme 5.2, on a : $\bar{s}b\bar{s}b_n = b_n\bar{s}b'\bar{s}$ avec $b' \in B^{s\bar{s}}//H$.
D'après le lemme 5.3, on a : $sa\bar{s}b_n s \in \alpha s\bar{s}sH$.
D'où : $c_{n+1}d_{n+1}a_n b_n a_{n-1} b_{n-1} = sab\bar{s}b_n s b_{n-1} = sa\bar{s}b_n s(s\bar{s}b'\bar{s}sb_{n-1})$ et $s\bar{s}b'\bar{s}sb_{n-1} \in B$.
Posons $\mathcal{E}' = \left(sa, \bar{s}b_n, s(s\bar{s}b'\bar{s}sb_{n-1}), a_{n-2}b_{n-2}, \ldots, a_1 b_1\right)$.
La $\mathcal{A}$-décomposition $\mathcal{E}'$ est équivalente à $\mathcal{E}$ et vérifie (c).

Cas 2.2 $\mathrm{fin}(\mathcal{D}) = E_{\lambda\pi\lambda}(\beta)$ avec $\beta \in (N^\lambda \cup N^\pi)//H$.
On a : $c_{n+1} = s$ avec $s \in \mathbf{g}$ tel que $\alpha \in N^s//H$ et $d_{n+1} = ab\beta^{-1}$ avec $a \in N_{\mathrm{Id},\alpha}^s$ et $b \in B^{s\bar{s}}$ et $a_n b_n a_{n-1} b_{n-1} a_{n-2} = \beta s\bar{s}sh$ avec $h \in H$.
D'où $c_{n+1}d_{n+1}a_n b_n a_{n-1} b_{n-1} a_{n-2} b_{n-2} = sab\bar{s}s\bar{s}hb_{n-2} = sa\bar{s}s(s\bar{s}b\bar{s}s)\bar{s}hb_{n-2}$ et $s\bar{s}b\bar{s}s \in B$. D'après le lemme 5.3 (avec $t = \mathrm{Id}$), on a : $sa\bar{s}s \in \alpha s\bar{s}sH$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Posons $\mathcal{E}' = \big(sa, \bar{s}, s(s\bar{s}b\bar{s}s), \bar{s}hb_{n-2}, a_{n-3}b_{n-3}\ldots, a_1b_1\big)$.
La $\mathcal{A}$-décomposition $\mathcal{E}'$ est équivalente à $\mathcal{E}$ et vérifie (c).

6 Le théorème d'automatisation

Dans cette section, nous démontrons le théorème d'automatisation (*cf.* théorème 6.7) qui permet à partir d'une décomposition quelconque $\mathcal{D}$ de construire une décomposition $\mathcal{D}'$ équivalente à $\mathcal{D}$, reconnue par l'automate $\mathcal{A}$ et de longueur inférieure ou égale à celle de $\mathcal{D}$.

Notation 6.1 Soit E un état de l'automate $\mathcal{A}$. On note $\mathrm{out}(E)$ l'ensemble des transitions de E vers F, où F parcourt l'ensemble des états de $\mathcal{A}$.

Lemme 6.2 *On a :*

(a) *Pour* $s \in \mathbf{g}$ *et* $u \in N^{\bar{s}s}//H$, $\mathrm{out}(E_s) = \mathrm{out}\big(E_{s\bar{s}}(u)\big) = \bar{s}B \amalg s\big(B \smallsetminus B(s)\big)$.
(b) *Pour* $\beta \in (N^\lambda \cup N^\pi)//H$, $\mathrm{out}\big(E_{\lambda\pi\lambda}(\beta)\big) = \coprod_{s\in\mathbf{g}} s\big(B \smallsetminus B(s)\big)\,\beta^{-1}$.

Preuve Pour $s \in \mathbf{g}$, on a : $\coprod_{t\in N^{\bar{s}s}//H} N_t^{s\bar{s}} = N^{s\bar{s}}$ et $N^{s\bar{s}}(B^s//H) = B(s)$. Donc $\coprod_{t\in N^{\bar{s}s}//H} B_t(s) = B(s)$.

Pour $s \in \mathbf{g}$ et $t \in N^{s\bar{s}}//H$, on a : $\coprod_{\alpha\in N^s//H} N_{t,\alpha}^s = N^s$ et $N^s(B^{s\bar{s}}//H) = B(s\bar{s})$, donc $\coprod_{\alpha\in N^s//H} B_{t,\alpha}(s\bar{s}) = B(s\bar{s})$.

D'où, pour $s \in \mathbf{g}$ et $t \in N^{s\bar{s}}//H$:

$$\mathrm{out}(E_s) = \coprod_{r\in\mathbf{g}} r\big(B \smallsetminus B(s)\big) \amalg \coprod_{t\in N^{\bar{s}s}//H} \bar{s}B_t(s) = \bar{s}B \amalg s\big(B \smallsetminus B(s)\big),$$

$$\begin{aligned}\mathrm{out}\big(E_{s\bar{s}}(u)\big) &= \coprod_{r\in\mathbf{g}} r\big(B \smallsetminus B(s)\big) \amalg \coprod_{t\in N^{s\bar{s}}//H} \bar{s}\big(B_t(s) \smallsetminus B(\bar{s}s)\big) \amalg \coprod_{\alpha\in N^s//H} \bar{s}B_{u,\alpha}(\bar{s}s)\\ &= \bar{s}B \amalg s\big(B \smallsetminus B(s)\big),\end{aligned}$$

et pour $\beta \in (N^\lambda \cup N^\pi)//H$:

$$\begin{aligned}&\mathrm{out}\big(E_{\lambda\pi\lambda}(\beta)\big)\,\beta\\ &= \coprod_{s\in\mathbf{g}} s\Bigg(\Big(\big(B \smallsetminus B(\bar{s})\big) \amalg \coprod_{t\in N^{\bar{s}s}//H} \big(B_t(\bar{s}) \smallsetminus B(s\bar{s})\big) \amalg \coprod_{\beta\in N^s//H} B_{\mathrm{Id},\beta}(s\bar{s})\Big) \smallsetminus B(s)\Bigg)\\ &= \coprod_{s\in\mathbf{g}} s\big(B \smallsetminus B(s)\big).\end{aligned}$$

Corollaire 6.3 *Une sous-décomposition d'une $\mathcal{A}$-décomposition est encore une $\mathcal{A}$-décomposition.*

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Preuve Pour $s \in \mathbf{g}$, $t \in N^{s\bar{s}}//H$ et $\beta \in (N^\lambda \cup N^\pi)//H$, on a : $\mathrm{out}\big(E_{\lambda\pi\lambda}(\beta)\big) \subset \mathrm{out}(E_s) = \mathrm{out}\big(E_{s\bar{s}}(t)\big) \subset \mathrm{out}(E_{\mathrm{Id}})$. Ceci implique que $\mathcal{A}$ reconnaît les mêmes mots que si tous ses états étaient initiaux. Par ailleurs, tous les états de $\mathcal{A}$ sont terminaux.

Lemme 6.4 *Pour $s \in \mathbf{g}$, on a : $sNs \subset N \amalg NsN$.*

Preuve Pour $s = \pi$, on a $\pi N\pi \subset Z \cap \coprod_{s\in\mathfrak{S}} NsN = N \amalg N\pi N$.

Pour $s = \lambda$, soit $\nu = (ax + by + cz, dy + ez, fz) \in N$. Si $e = 0$ alors $\lambda\nu\lambda \in N$ et si $e \neq 0$ alors en posant $\rho = \big(x, e^{-1}(y - dz)\big) \in N$ on a : $\lambda\rho\lambda\nu\lambda \in N$. Donc $\lambda\nu\lambda \in N\lambda N$.

Notation 6.5 Soit $\mathcal{D} = (a_n b_n, \ldots, a_1 b_1)$ ($a_i \in \mathbf{g}$ et $b_i \in B$) une $\mathbf{g}$-décomposition. Pour $s \in \mathbf{g}$, on note $\lg_s(\mathcal{D}) = \mathrm{card}\big\{\, i \in \{1, \ldots, n\} \,;\, a_i = s\big\}$.

Remarque 6.6 Soit $\mathcal{D}$ une $\mathbf{g}$-décomposition ; on a $\lg(\mathcal{D}) = \lg_\lambda(\mathcal{D}) + \lg_\pi(\mathcal{D})$.

Théorème 6.7 **(Automatisation)** *Soit $\mathcal{E}$ une $\mathbf{g}$-décomposition. Si $\mathcal{E}$ n'est pas une $\mathcal{A}$-décomposition, alors il existe une $\mathbf{g}$-décomposition $\mathcal{E}'$ équivalente à $\mathcal{E}$, telle que $\lg(\mathcal{E}') < \lg(\mathcal{E})$ et $\lg_s(\mathcal{E}') \leq \lg_s(\mathcal{E})$, pour tout $s \in \mathbf{g}$.*

Preuve Soit $\mathcal{E} = (c_m d_m, \ldots, c_1 d_1)$ ($c_i \in \mathbf{g}$ et $d_i \in B$) une $\mathbf{g}$-décomposition, qui n'est pas une $\mathcal{A}$-décomposition. L'automate $\mathcal{A}$ reconnait tous les mots de longueur 1. Donc il existe $n \in \{1, \ldots, m-1\}$ tel que $\mathcal{D} = (c_n d_n, \ldots, c_1 d_1)$ est reconnu, mais pas $(c_{n+1} d_{n+1}, \ldots, c_1 d_1)$. On peut supposer que $n = m-1$. Appliquons la proposition 5.4 à la $\mathcal{A}$-décomposition $\mathcal{D}$. On obtient une décomposition $\mathcal{D}' = (a_n b_n, \ldots, a_1 b_1)$ ($a_i \in \mathbf{g}$ et $b_i \in B$) équivalente à $\mathcal{D}$ et vérifiant (a)–(c).

Cas 1 $\mathrm{fin}(\mathcal{D}) = E_s$ ou $\mathrm{fin}(\mathcal{D}) = E_{s\bar{s}}(t)$ avec $s \in \mathbf{g}$ et $t \in N^{s\bar{s}}//H$.

D'après le lemme 6.2, on a $c_{n+1} = s$, $d_{n+1} = ab$ avec $a \in N$ et $b \in B^s$. D'après la proposition 5.4, on a $a_n = s$. D'où : $c_{n+1} d_{n+1} a_n b_n = sabsb_n = (sas)(sbsb_n)$ avec $sbsb_n \in B$. D'après le lemme 6.4, $sas \in N \cup NsN$. Si $sas \in N$, on pose $\mathcal{E}' = (a_{n-1} b_{n-1}, \ldots, a_1 b_1)$, si $sas = a_2 s a_1$ avec $a_1, a_2 \in N$, on pose $\mathcal{E}' = \big(s(a_1 sbsb_n), a_{n-1} b_{n-1}, \ldots, a_1 b_1\big)$.

Cas 2 $\mathrm{fin}(\mathcal{D}) = E_{\lambda\pi\lambda}(\alpha)$ avec $\alpha \in (N^\lambda \cup N^\pi)//H$.

D'après le lemme 6.2, il existe $s \in \mathbf{g}$ tel que $c_{n+1} = s$ et $d_{n+1} = ab\alpha^{-1}$ avec $a \in N$ et $b \in B^s$. D'après la proposition 5.4, on a : $a_n b_n a_{n-1} b_{n-1} a_{n-2} = \alpha s\bar{s}\bar{s}h$ avec $h \in H$. D'où $c_{n+1} d_{n+1} a_n b_n a_{n-1} b_{n-1} a_{n-2} = (sas)(sbs)\bar{s}\bar{s}h$ avec $sbs \in B$ et, d'après le lemme 6.4, $sas \in N \cup NsN$. Si $sas \in N$, on pose $\mathcal{E}' = (\bar{s}, shb_{n-2}, a_{n-3} b_{n-3}, \ldots, a_1 b_1)$, si $sas = a_2 s a_1$ avec $a_1, a_2 \in N$, on pose $\mathcal{E}' = \big(s(a_1 sbs), \bar{s}, shb_{n-2}, a_{n-3} b_{n-3}, \ldots, a_1 b_1\big)$.

Dans les deux cas, on a obtenu une $\mathbf{g}$-décomposition $\mathcal{E}'$ équivalente à $\mathcal{E}$, et telle que $\lg(\mathcal{E}') < \lg(\mathcal{E})$ et $\lg_s(\mathcal{E}') \leq \lg_s(\mathcal{E})$, pour tout $s \in \mathbf{g}$.

Corollaire 6.8 *Soit $\mathcal{D}$ une $\mathbf{g}$-décomposition de longueur $\mathbf{g}$-minimale, alors $\mathcal{D}$ est une $\mathcal{A}$-décomposition.*

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Se pose le problème de la réciproque.

Question 6.9 Toute $\mathcal{A}$-décomposition est-elle de longueur **g**-minimale ?

Si la réponse à cette question s'avérait négative, il faudrait *affiner* l'automate $\mathcal{A}$. Ceci est toujours réalisable, car, étant donné un automate déterministe, il existe un automate qui reconnaît les mêmes mots sauf un mot donné.

7 Décompositions minimales

Une décomposition automatique est une décomposition dans laquelle on cherche à minimiser la longueur. Pour cela, on impose des conditions sur la fin de la décomposition. Une fois ceci fait, on cherche maintenant à minimiser la suite des degrés d'une composante. On procède par induction, en commençant par le début de la décomposition (que l'on parcourt donc dans l'autre sens). On aboutit à la formalisation des principes de la section 3, c'est à dire à la notion de décomposition minimale.

Notation 7.1 Soit $\mathcal{D} = (h_3, h_2, h_1)$ une $\mathcal{A}$-décomposition de longueur 3 telle que $\mathrm{fin}(\mathcal{D}) = E_{\lambda\pi\lambda}(\alpha)$ avec $\alpha \in (N^\lambda \cup N^\pi)//H$. Alors, d'après la proposition 5.4, il existe $b \in B$ tel que $\alpha\lambda\pi\lambda b = h_3h_2h_1$. Cette relation détermine b que l'on note $\mathfrak{b}(\mathcal{D})$.

Définition 7.2 (***B*-ordre**) On appelle *B-ordre* l'ordre sur $k[x, y, z]$ obtenu en comparant lexicographiquement le degré (total), le degré en y et z, puis le degré en z. Un polynôme est dit B-minimal s'il est minimal pour cet ordre.

Définition 7.3 (**Décomposition minimale**) Soit $\mathcal{D} = (h_n, \ldots, h_1)$ (avec $h_i = a_ib_i$, $a_i \in \mathbf{g}$ et $b_i \in B$) une $\mathcal{A}$-décomposition, on dit que $\mathcal{D}$ est *minimale* si pour tout $i \in \{1 \ldots n\}$,

(1) si $1 \leq i \leq n-2$ et si en posant $\mathcal{D}_i = (h_{i+2}, h_{i+1}, h_i)$ on a $\mathrm{fin}(\mathcal{D}_i) = E_{\lambda\pi\lambda}(\alpha)$ avec $\alpha \in (N^\lambda \cup N^\pi)//H$ alors $w_i(\mathcal{D}) = \mathfrak{b}(\mathcal{D}_i)z_{i-1}(\mathcal{D})$ est B-minimal dans l'ensemble $(B^\lambda \cup B^\pi)w_i(\mathcal{D})$,
(2) sinon $z_i(\mathcal{D})$ est B-minimal dans l'ensemble $B^{a_i}z_i(\mathcal{D})$.

Remarque 7.4 La conclusion dans (1) est plus forte que (2), *i.e.*, si $\mathcal{D}$ est une $\mathcal{A}$-décomposition minimale alors $z_i(\mathcal{D})$ est B-minimal dans l'ensemble $B^{a_i}z_i(\mathcal{D})$ pour tout $i \in \{1 \ldots n\}$. Cette condition est celle du principe 1 et la condition (1) formalise le principe 3.

Remarque 7.5 Une sous-décomposition d'une $\mathcal{A}$-décomposition minimale est encore une $\mathcal{A}$-décomposition minimale.

Définition 7.6 Soit $\mathcal{A}_0$ un automate. On appelle $\mathcal{A}_0$-décomposition minimale une $\mathcal{A}_0$-décomposition qui est aussi une $\mathcal{A}$-décomposition minimale.

Théorème 7.7 (**Minimisation**) *Soit $\sigma \in T$, alors il existe une $\mathcal{A}$-décomposition de σ, minimale.*

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Preuve D'après le corollaire 2.3, il existe une **g**-décomposition $\mathcal{D} = (h_n, \dots, h_1)$ (avec $h_i = a_i b_i$, $a_i \in \mathbf{g}$ et $b_i \in B$) de σ que l'on peut supposer de longueur **g**-minimale, ce qui implique, d'après le corollaire 6.8, que $\mathcal{D}$ est une $\mathcal{A}$-décomposition de σ.

Pour i valant successivement $1, \dots, n$:

Cas 1 $1 \leq i \leq n-2$ et, en posant $\mathcal{D}_i = (h_{i+2}, h_{i+1}, h_i)$, on a $\operatorname{fin}(\mathcal{D}_i) = E_{\lambda\pi\lambda}(\alpha)$ avec $\alpha \in (N^\lambda \cup N^\pi)//H$.

Posons $b = \mathfrak{b}(\mathcal{D}_i)$, on a : $\alpha\lambda\pi\lambda b = h_{i+2}h_{i+1}h_i$. Considérons $c_i \in B^\lambda \cup B^\pi$ tel que $c_i b z_{i-1}(\mathcal{D})$ soit B-minimal dans l'ensemble $(B^\lambda \cup B^\pi) b z_{i-1}(\mathcal{D})$. Soit $s \in \mathbf{g}$ tel que $c_i \in B^s$.

On remplace $\mathcal{D}$ par $\mathcal{D}' = \left(h_n, \dots, h_{i+4}, h_{i+3}\alpha, s, \bar{s}(sc_i^{-1}s), sc_i b, h_{i-1}, \dots, h_1\right)$.

La décomposition $\mathcal{D}'$ est équivalente à $\mathcal{D}$ si $i < n-2$, et quasi-équivalente à $\mathcal{D}$ si $i = n-2$.

Cas 2 Cas autres que le cas 1.

Considérons $c_i \in B^{a_i}$ tel que $c_i z_i(\mathcal{D})$ soit B-minimal dans l'ensemble $B^{a_i} z_i(\mathcal{D})$.

On remplace $\mathcal{D}$ par $\mathcal{D}' = \left(h_n, \dots, h_{i+2}, h_{i+1}c_i^{-1}, a_i(a_i c_i a_i)b_i, h_{i-1}, \dots, h_1\right)$.

La décomposition $\mathcal{D}'$ est équivalente à $\mathcal{D}$ si $i < n$, et quasi-équivalente à $\mathcal{D}$ si $i = n$.

Après ces n modifications, on obtient une décomposition minimale.

Conjecture 7.8 *Soit $\sigma \in T$ et soit $\mathcal{D}$ une $\mathcal{A}$-décomposition minimale de σ, alors $\mathcal{D}$ est une* CD*-décomposition de σ.*

8 Polynômes faibles

La notion de polynôme faible permet de reformuler la conjecture 7.8 en une conjecture portant uniquement sur un polynôme (*cf.* conjecture 8.6). Nous donnons, dans cette section, des exemples et des propriétés élémentaires des polynômes faibles.

Définition 8.1 **(Polynôme faible)** Soit $f \in k[x, y, z]$. On dit que f est *faible* si pour tout $b \in B$ on a : $\deg b(f) \geq \deg f$.

Remarque 8.2 Dans la définition précédente, on peut remplacer B par $B//H$.

Exemple 8.3 Les polynômes de degré 1 sont faibles.

Exemple 8.4 Soit $f(x, y, z) = y + z(xz + y^2) \in k[x, y, z]$. Il s'agit de la seconde composante de l'automorphisme de l'exemple 1.4. Elle est faible. En effet, pour tout $b = \left(x + P_0(y, z), y + Q_0(z), z\right) \in B//H$ on a :

$$b(f)(x, y, z) = y + Q_0(z) + z\Big(P_0(y, z)z + \big(y + Q_0(z)\big)^2\Big) + z^2 x.$$

Le terme $z^2 x$ est de degré 3 donc $\deg b(f)(x, y, z) \geq 3 = \deg f(x, y, z)$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Exemple 8.5 Soit $f(x,y,z) = y + x^2 + 2xy^3 - z^3 + 3xyz - \frac{3}{4}y^2z^2 \in k[x,y,z]$ avec $\mathrm{car}(k) \neq 2$. Il s'agit de la troisième composante de l'automorphisme de l'exemple 1.9. Elle est faible. En effet, soit $R \in k[y]$:

$$\begin{aligned} f\big(x+R(y),y,0\big) &= y + \big(x+R(y)\big)^2 + 2\big(x+R(y)\big)\,y^3 \\ &= R(y)\big(R(y)+2y^3\big) + y + 2x\big(R(y)+y^3\big) + x^2. \end{aligned}$$

Si le terme dominant de $R(y)$ est $-y^3$, le terme $R(y)\big(R(y)+2y^3\big)$ est de degré 6. Sinon le terme $2x\big(R(y)+y^3\big)$ est de degré ≥ 4. Donc pour tout $R \in k[y]$, $\deg f\big(x+R(y),y,0\big) \geq 4 = \deg f(x,y,z)$.

Pour tout $b = \big(x+P_0(y,z), y+Q_0(z), z\big) \in B//H$ on a donc :

$$\deg b(f)(x,y,z) \geq \deg f\big(x+P_0(y,0),y,0\big) \geq \deg f(x,y,z).$$

Rappelons que $z_*(\mathcal{D}) = z_n(\mathcal{D})$ où $n = \lg(\mathcal{D})$ (*cf.* 2.7). La conjecture centrale est la suivante :

Conjecture 8.6 *Soit $\mathcal{D}$ une $\mathcal{A}$-décomposition minimale, alors le polynôme $z_*(\mathcal{D})$ est faible.*

Corollaire 8.7 *La conjecture 8.6 implique la conjecture 2.15.*

Preuve Soit $\sigma \in T$. D'après le théorème 7.7, il existe une $\mathcal{A}$-décomposition $\mathcal{D}$ de σ minimale. En appliquant la conjecture 8.6 aux sous-décompositions initiales (*cf.* 2.5) de $\mathcal{D}$, on montre que $\mathcal{D} \in \mathrm{CD}(\sigma)$.

Proposition 8.8 *Soit $f \in k[x,y,z]$ un polynôme faible et $R \in k[T]$, alors $R\big(f(x,y,z)\big)$ est faible.*

Preuve Soit $b \in B$, on a $b\big(R(f)\big) = R\big(b(f)\big)$ donc :

$$\deg\Big(b\big(R(f)\big)\Big) = \deg(R)\deg\big(b(f)\big) \geq \deg(R)\deg(f) = \deg\big(R(f)\big).$$

Proposition 8.9 *Soit $R \in k[y,z] \subset k[x,y,z]$ un polynôme faible, alors $R(x,z)$ est faible.*

Preuve Soit $b = \big(x+P_0(y,z), y+Q_0(z), z\big) \in B//H$, on a $b\big(R(x,z)\big) = R\big(x+P(y,z),z\big)$. Donc

$$\deg\Big(b\big(R(x,z)\big)\Big) \geq \deg\Big(R\big(x+P_0(0,z),z\big)\Big).$$

Puisque $R \in k[y,z]$ est faible, $\deg\Big(R\big(y+P_0(0,z),z\big)\Big) \geq \deg\big(R(y,z)\big)$. On en déduit que $\deg\Big(b\big(R(x,z)\big)\Big) \geq \deg\big(R(x,z)\big)$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Proposition 8.10 *Soit $f(x,y,z)=\sum_{i+j+k\leq 2} a_{i,j,k}x^iy^jz^k$ un polynôme de degré 2. Les assertions suivantes sont équivalentes :*

(1) *le polynôme f est faible,*
(2) *$a_{2,0,0}\neq 0$ ou $a_{1,1,0}\neq 0$ ou $a_{1,0,1}\neq 0$ ou ($a_{1,0,0}=0$ et ($a_{0,2,0}\neq 0$ ou $a_{0,1,1}\neq 0$ ou ($a_{0,1,0}=0$ et $a_{0,0,2}\neq 0$)))).*

Preuve Un polynôme $f\in k[x,y,z]$ de degré 2 n'est pas faible si et seulement si il existe $l\in k[x,y,z]$ de degré 1 et $b\in B$ de degré 2 tel que $f=b(l)$.

Exemple 8.11 Les polynômes suivants sont faibles : $y+x^2$, $z+xy+y^2$, $y+xz$ et $z+y^2$.

Proposition 8.12 *Soient $a\in k^*$ et $R\in k[y]$, alors $f(x,y,z)=az+R(y)$ est faible.*

Preuve Pour tout $b=\big(x+P_0(y,z),y+Q_0(z)\big)\in B/\!/H$ on a : $b(f)(x,y,z)=az+R\big(y+Q_0(z)\big)$ donc $\deg b(f)=\max\{1,\deg(R)\deg(Q_0)\}\geq\deg(f)$.

Proposition 8.13 *Soient $a\in k^*$ et $P\in k[x,z]$, posons $f(x,y,z)=ay+P(x,z)$ et supposons que f soit B-minimal dans $B^\pi f$, alors f est faible.*

Preuve La B-minimalité de f dans $B^\pi f$ implique que $P(x,z)$ est de degré minimal dans l'ensemble $\big\{Q(z)+P\big(x+R(z),z\big)\ ;\ Q,R\in k[z]\big\}$. Pour tout $b=\big(x+P_0(y,z),y+Q_0(z)\big)\in B/\!/H$ on a : $b(f)(x,0,z)=aQ_0(z)+P\big(x+P_0(0,z),z\big)$, donc $\deg b(f)(x,0,z)\geq\deg P(x,z)$; d'où $\deg b(f)(x,y,z)\geq\deg f(x,y,z)$.

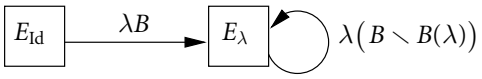
9 Boucles λ (l'automate $\mathcal{L}_0$)

Dans cette section, on étudie l'automate $\mathcal{L}_0$ qui décrit la situation en dimension 2. On démontre des résultats qui découlent du théorème de Jung-van der Kulk et qui seront utiles dans la section suivante.

Définition 9.1 **(L'automate $\mathcal{L}_0$)** On définit $\mathcal{L}_0$, l'automate dont les deux états sont E_{Id} (initial), et E_λ et dont les transitions sont :

$$\begin{array}{llll} \text{De} & E_{\mathrm{Id}} & \text{vers} & E_\lambda \quad : \lambda B. \\ \text{De} & E_\lambda & \text{vers} & E_\lambda \quad : \lambda\big(B\smallsetminus B(\lambda)\big). \end{array}$$

Remarque 9.2 On peut représenter $\mathcal{L}_0$ par la figure suivante :



Remarque 9.3 Ce sous-automate décrit les automorphismes de $D=B^\lambda E$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

***Définition 9.4* (c.H.g.)** On appelle *c.H.g.* un élément de H, ou tout automorphisme, ρ, qui s'écrit $\rho = h_n \cdots h_2$ où $(h_n, \dots, h_2, \lambda)$ est une $\mathcal{L}_0$-décomposition. Autrement dit, $(h_n, \dots, h_2)$ est reconnu par l'automate ayant un unique état (initial) E_λ et pour transition de E_λ vers E_λ : $\lambda\big(B \setminus B(\lambda)\big)$. On peut dire aussi que $(h_n, \dots, h_2)$ est une $\mathcal{L}_0$-décomposition telle que $h_2 \notin B(\lambda)$.

Remarque 9.5 Via la projection $(f, g, h) \mapsto (g, h)$ de D dans le groupe des automorphismes de la k-algèbre $k[y, z]$, les c.H.g. correspondent à ce que l'on appelle en dynamique, composée de transformations de Hénon généralisées (*cf.* [FM], [Lam]). Ce sont les automorphismes considérés comme dynamiquement intéressants.

Notation 9.6 Pour $P \in k[y, z]$, on note $\mathrm{lt}(P)$ la forme homogène de plus haut degré de P.

Proposition 9.7 *Soit $\mathcal{D} = (h_n, \dots, h_1)$ une $\mathcal{L}_0$-décomposition alors :*

(1) $\deg\big(z_n(\mathcal{D})\big) = \prod_{i=2}^{n} \deg\big(h_i(y)\big)$,
(2) $z_n(\mathcal{D}) \in k[y, z]$ *et si* $n \geq 1$ *alors* $\mathrm{lt}\big(z_n(\mathcal{D})\big) \in k[y]$.

Preuve La proposition 9.7 est une conséquence du théorème de Jung et van der Kulk (*cf.* [Fu, preuve de la proposition 1]).

Théorème 9.8 *Soit $\mathcal{D}$ une $\mathcal{L}_0$-décomposition alors le polynôme $z_*(\mathcal{D})$ est faible.*

Preuve Posons $f = z_*(\mathcal{D})$. Soit $b \in B//H$. Si $b \in B(\lambda)$ alors $\deg\big(b(f)\big) = \deg(f)$ car $f \in k[y, z]$. Si $b \in B \setminus B(\lambda)$ alors, d'après la proposition 9.7 appliquée à la $\mathcal{L}_0$-décomposition, $\mathcal{D}' = (\lambda b, \mathcal{D})$, on a : $\deg\big(b(f)\big) = \deg\big(z_*(\mathcal{D}')\big) = \deg\big(b(y)\big)\deg(f) \geq \deg(f)$.

Proposition 9.9 *Soit ρ une c.H.g. alors :*

(1) $\rho(y)$ *est faible,*
(2) $\deg\big(\rho(z)\big) \leq \deg\big(\rho(y)\big)$ *avec égalité si et seulement si* $\rho \in H$,
(3) *si* $R \in k[y]$ *et* $\epsilon \in \{0, 1\}$ *alors* $\epsilon\rho(z) + R\big(\rho(y)\big)$ *est faible.*

Preuve Si $\rho \in H$, il suffit d'appliquer la proposition 8.12. Sinon, on peut écrire $\rho = h_n \cdots h_2$ où $\mathcal{D} = (h_n, \dots, h_2, \lambda)$ est une $\mathcal{L}_0$-décomposition. Alors $\rho(y) = z_*(\mathcal{D})$, donc (1) résulte du théorème 9.8. En posant $\mathcal{D}_1 = (h_n, \dots, h_2)$, alors $\rho(z) = z_*(\mathcal{D}_1)$, donc (2) résulte de (1) de la proposition 9.7.

Montrons (3). Si $\deg(R) = 0$ c'est le théorème 9.8. On peut donc supposer $\deg(R) \geq 1$. Posons $f = \epsilon\rho(z) + R\big(\rho(y)\big)$ et soit $b \in B$. Si $b \in B(\lambda)$ alors $\deg\big(b(f)\big) = \deg(f)$. Si $b \in B \setminus B(\lambda)$ alors $\lambda b\rho$ est une c.H.g. En appliquant (2), on a donc $\deg(f) = \deg(R)\deg\big(\rho(y)\big)$ et $\deg\big(b(f)\big) = \deg(R)\deg\big(b\rho(y)\big)$ et d'après (1) on a $\deg\big(\rho(y)\big) \leq \deg\big(b\rho(y)\big)$, d'où $\deg(f) \leq \deg\big(b(f)\big)$ et f est faible.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

10 Polynômes faibles (suite)

Dans cette section, on suppose que la caractéristique de k est nulle. On montre que les polynômes d'une certaine forme sont faibles. Ceci répond en partie à la conjecture 8.6.

Théorème 10.1 ($\mathrm{car}(k) = 0$) *Soit* $f(x, y, z) = \epsilon\rho(z) + R\big(x + P_1(y, z), \rho(y)\big)$ *avec* $\epsilon \in \{0, 1\}$, $R \in k[x, y]$, ρ *une c.H.g. et* $P_1 \in k[y, z]$ *tel que* f *soit B-minimal dans* $B^\lambda f$. *Alors le polynôme* f *est faible.*

Preuve Dans cette démonstration, nous distinguons un certain nombre de cas ordonnés de façon lexicographique.

Cas 0 $R \in k^*x + k[y]$.
On a $f \in k^*x$, donc f est faible (*cf.* exemple 8.3).

Cas 1 $R \in k[y]$.
Alors f est faible d'après (3) de la proposition 9.9.

Cas 2 $R \in k[x, y] \setminus (kx + k[y])$.
On a, en particulier, $\deg(R) \geq 2$.
Soit $b = \big(x + P_0(y, z), Q_0(z), z\big) \in B//H$. On a :

$$b(f)(x, y, z) = \epsilon b\rho(z) + R\big(x + P(y, z), b\rho(y)\big)$$

où $P(y, z) = P_0(y, z) + P_1\big(Q_0(y, z), z\big)$.
Il s'agit de montrer que $\deg(f) \leq \deg\big(b(f)\big)$.

Cas 2.1 $b \in B(\lambda)$.
On peut supposer que $b \in B^\lambda//H$, *i.e.*, $Q_0(y, z) = y$. Alors $b(f)(x, y, z) = \epsilon\rho(z) + R\big(x + P(y, z), \rho(y)\big)$, donc $\deg(f) \leq \deg\big(b(f)\big)$ par minimalité de f.
Ceci termine la preuve du cas 2.1.

Cas 2.2 $b \in B \setminus B(\lambda)$.
On a $\deg(Q_0) \geq 2$.

Cas 2.2.1 $R \in k[x]$.

Cas 2.2.1.1 $\epsilon = 0$.
On a $\deg(f) \leq \deg\big(b(f)\big)$ d'après la proposition 8.8.

Cas 2.2.1.2 $\epsilon = 1$.
Posons $Q = b\rho(z)$ et $Q_1 = \rho(z)$. Posons $q = \deg Q$ et $q_1 = \deg Q_1$. D'après la proposition 9.7, $\deg\big(b\rho(z)\big) = \deg(Q_0)\deg\big(\rho(z)\big)$ donc $2q_1 \leq q$. Posons $\mathrm{lt}\, Q(y, z) = \beta z^q$, et $\mathrm{lt}\, Q_1(y, z) = \beta_1 y^{q_1}$ et $\mathrm{lt}\, R(x) = \gamma x^r$ ($r \geq 2$). On a $\deg(f) \leq \max\big\{\deg\big(\rho(z)\big), \deg(R)\big\} = \max\{q_1, r\}$ par minimalité de f.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Cas 2.2.1.2.1 lt $P(y,z) = \alpha z^p$ avec $\alpha \in k^*$ et $p \geq 2$ avec $pr = q$ et $\beta + \gamma\alpha^r = 0$.

Le coefficient de x dans $Q(y,z) + R\big(x + P(y,z)\big) \in k[y,z][x]$ est de degré $p(r-1)$ donc $\deg(f) \leq \max\{q_1, r\} \leq \frac{q}{2} \leq q(1-\frac{1}{r}) = p(r-1) \leq \deg\big(b(f)\big)$.

Cas 2.2.1.2.2 lt $P(y,z) \notin k[z]$ ou bien lt $P(y,z) = \alpha z^p$ avec $pr \neq q$ ou $\beta + \gamma\alpha^r \neq 0$.

On a $\deg(f) \leq \max\{q, r\} \leq \max\{q, pr, r\} = \deg\big(b(f)\big)$.

Ceci termine la preuve du cas 2.2.1.

Cas 2.2.2 (début) $R \in k[x,y] \setminus k[x]$.

Posons $Q = b\rho(y)$ et $Q_1 = \rho(y)$. Posons $q = \deg Q$ et $q_1 = \deg Q_1$. D'après la proposition 9.7, $\deg\big(b\rho(y)\big) = \deg(Q_0)\deg\big(\rho(y)\big)$ donc $2q_1 \leq q$.

Posons lt $Q(y,z) = \beta z^q$ et lt $Q_1(y,z) = \beta_1 y^{q_1}$.

On a $\deg(f) \leq \max\Big\{\deg\big(\epsilon\rho(z)\big), \deg\Big(R\big(x, Q_1(y,z)\big)\Big)\Big\} \leq \deg R\big(x, Q_1(y,z)\big)$, la première inégalité provenant de la minimalité de f et la seconde du fait que, en utilisant (2) de la proposition 9.9, et puisque $R \in k[x,y] \setminus k[x]$, on a $\deg\big(\epsilon\rho(z)\big) \leq \deg\big(\rho(y)\big) \leq \deg R\big(x, Q_1(y,z)\big)$.

Montrons que : $\deg R\big(x, Q_1(y,z)\big) \leq \deg R\big(x + P(y,z), Q(y,z)\big)$ (M).

Pour chaque polynôme-face[1] F de R on écrit :

$$(*) \qquad F(x,y) = cx^{\nu_0} y^{m_0} \prod_{i=1}^{l} \left[y^{a_i m} A_i\left(\frac{x^n}{y^m}\right)\right]^{\nu_i}$$

avec $c \in k^*$, $\nu_0, m_0 \in \mathbb{N}$, $l, m, n \in \mathbb{N}^*$, m et n étrangers et pour $i \in \{1,\dots,l\}$, $A_i \in k[x]$ unitaires, irréductibles, deux à deux étrangers et tels que $A_i(0) \neq 0$, $a_i = \deg A_i$ et $\nu_i \in \mathbb{N}^*$.

On pose $a_0 = \frac{1}{n}$, $a = \sum_{i=0}^{l} a_i\nu_i$, $F_0(x,y) = x$ et $F_i(x,y) = y^{a_i m} A_i(\frac{x^n}{y^m})$.

Quitte à remplacer $R(x,y)$ par $R\big(x + S(y), y\big)$ et $P(y,z)$ par $P(y,z) - S(y)$ pour $S \in k[y]$, on peut supposer que $an \geq 2\nu_i$ pour tout $i \in \{1,\dots,l\}$.

En effet, on procède par induction en considérant successivement chaque polynôme-face suivant l'ordre croissant de leur pente $(-m/n)$. Si pour un polynôme-face F on a: $an < 2\nu_{i_0}$ pour un certain $i_0 \in \{1,\dots,l\}$ alors, en particulier, $n = 1$, $a_{i_0} = 1$ et $\nu_{i_0} \geq \nu_i$ pour tout $i \in \{0,\dots,l\}$. En remplaçant $R(x,y)$ par $R\big(x - A_{i_0}(0)y^m, y\big)$, on ne modifie pas les polynômes-faces de pente plus petite et après cette transformation sur la face F on a: $\nu_0 \geq \nu_i$ pour tout $i \in \{1,\dots,l\}$ donc $an \geq \nu_0 + \nu_i \geq 2\nu_i$.

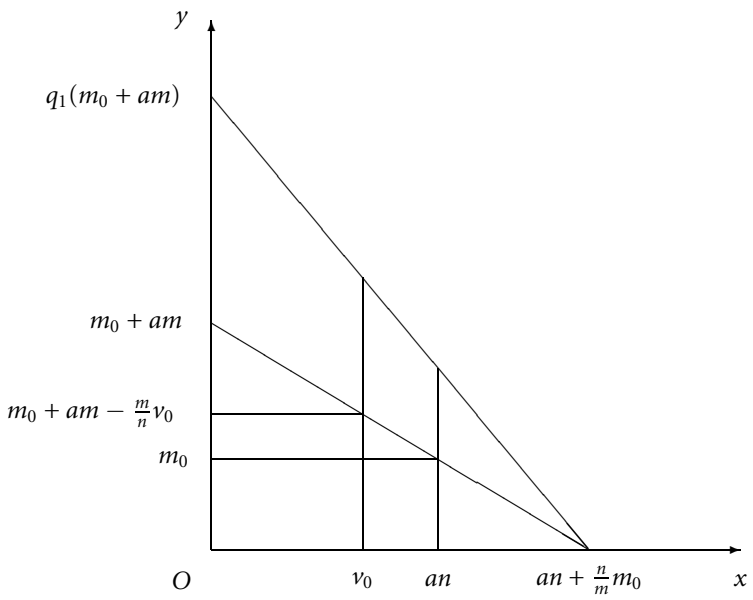
Cas 2.2.2.1 lt $P(y,z) = \alpha z^p$ avec $\alpha \in k^*$ et $p \in \mathbb{N}$ et il existe un polynôme-face F de R tel que, avec les notations de $(*)$, on ait $pn = qm$ et $A_{i_0}(\alpha^n) = 0$ pour un certain $i_0 \in \{1,\dots,l\}$ (c'est à dire que $A_{i_0}(T) = T - \frac{\alpha^n}{\beta^m}$).

Cas 2.2.2.1.1 $n \leq mq_1$ (c'est à dire $q_1(m_0 + am) \geq an + \frac{n}{m}m_0$).

Soit $i \in \{1,\dots,l\}$, posons $A_i(T) = \sum_{j=0}^{a_i} \alpha_{i,j} T^j$.

[1] Si $\nu \in \mathbb{N} \times \mathbb{N}$ est tel que la somme F_ν des monômes de R dont le degré pondéré par ν est maximal n'est pas un monôme, on dit que F_ν est un polynôme-face de R.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press



Soit $s \in \mathbb{N}$, le coefficient de x^s dans $F_i\big(x + P(y,z), Q(y,z)\big)$ est

$$\sum_{j=[s/n]}^{a_i} \alpha_{i,j} \binom{jn}{s} P(y,z)^{jn-s} Q(y,z)^{(a_i-j)m},$$

son degré est donc (si $s \leq a_i n$) inférieur ou égal à $qma_i - sp$ avec égalité si $s = 0$ et $i \neq i_0$ ou si $s = 1$ et $i = i_0$ et inégalité stricte si $s = 0$ et $i = i_0$.

Puisque $F(x,y) = cy^{m_0} \prod_{i=0}^{l} F_i(x,y)^{v_i}$, ceci implique que le coefficient de $x^{v_{i_0}}$ de $F\big(x + P(y,z), Q(y,z)\big) \in k[y,z][x]$ est de degré $q(m_0 + ma - v_{i_0}\frac{m}{n})$.

En effet, le coefficient de $x^{v_{i_0}}$ dans $\prod_{i=0}^{l} F_i\big(x + P(y,z), Q(y,z)\big)^{v_i}$ est la somme sur tous les $s_{i,j} \in \mathbb{N}$ tels que $\sum_{i=0}^{l} \sum_{j=1}^{v_i} s_{i,j} = v_{i_0}$ des produits des coefficients de $x^{s_{i,j}}$ dans $F_i\big(x + P(y,z), Q(y,z)\big)$. Son degré est donc majoré par $\sum_{i=0}^{l} \sum_{j=1}^{v_i} (qma_i - s_{i,j}p) = qma - v_{i_0}p$ avec égalité pour[2] $s_{i,j} = \delta_{i,i_0}$ et inégalité stricte sinon.

D'où : $\deg R\big(x + P(y,z), Q(y,z)\big) \geq q(m_0 + am - v_{i_0}\frac{m}{n}) \geq q_1(m_0 + am)$ car $q \geq 2q_1$ et $an \geq 2v_{i_0}$. Par ailleurs, $\deg R\big(x, Q_1(y,z)\big) \leq q_1(m_0 + am)$ car $n \leq mq_1$. D'où, finalement, $\deg R\big(x, Q_1(y,z)\big) \leq \deg R\big(x + P(y,z), Q(y,z)\big)$. On obtient la majoration (M).

Cas 2.2.2.1.2 $n > mq_1$ (c'est à dire $p < \frac{q}{q_1}$).

[2]On note δ le symbole de Kronecker, $\delta_{i,j} = 1$ si $i = j$ et 0 sinon.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Considérons un monôme $x^d y^e$ de $R(x,y)$ qui donne le degré de $R\big(x, Q_1(y,z)\big)$, c'est à dire tel que $d + q_1 e$ soit maximal. Le coefficient de x^d dans $(x+\alpha z^p)^d (\beta z^q)^e \in k[z][x]$ est nul ou de degré qe et si $x^{d'} y^{e'}$ est un autre monôme de $R(x,y)$, le coefficient de x^d dans $(x+\alpha z^p)^{d'} (\beta z^q)^{e'} \in k[z][x]$ est de degré $p(d'-d)+qe'$. On a : $p(d'-d)+qe' \leq \frac{q}{q_1}(d'+q_1e'-d) \leq qe$ et la première inégalité est stricte sauf si $d' = d$ et, dans ce cas, la seconde inégalité est stricte dès que $e' \neq e$. Donc le coefficient de x^d dans $R\big(x+P(y,z), Q(y,z)\big) \in k[y,z][x]$ est de degré qe. D'où : $\deg R\big(x, Q_1(y,z)\big) = d + q_1 e \leq d + qe \leq R\big(x+P(y,z), Q(y,z)\big)$. On obtient la majoration (M).

Cas 2.2.2.2 lt $P(y,z) \notin k[z]$ ou bien, en posant $p = \deg(P)$, il n'existe pas de polynôme-face F de R tel que, avec les notations de $(*)$, on ait $pn = qm$ et $A_{i_0}(\alpha^n) = 0$ pour un certain $i_0 \in \{1, \ldots, l\}$.

On a: $\deg R\big(x, Q_1(y,z)\big) \leq \deg R\big(x, Q(y,z)\big) \leq \deg R\big(x+P(y,z), Q(y,z)\big)$.

On obtient la majoration (M).

Cas 2.2.2 (fin) Grâce à la majoration (M), on obtient

$$\deg(f) \leq \deg R\big(x, Q_1(y,z)\big) \leq \deg R\big(x+P(y,z), Q(y,z)\big).$$

La majoration (M) provient, dans les cas 2.2.2.1.1 et 2.2.2.1.2, d'un monôme de $k[x,y,z] \setminus k[y,z]$ et, dans le cas 2.2.2.2, d'un terme de degré suppérieur ou égal à $\deg(Q)$ donc strictement supérieur à $\deg\big(\epsilon b \rho(z)\big)$. La majoration (M) implique donc que $\deg(f) \leq \deg\big(b(f)\big)$. Ceci termine la preuve du cas 2.2.2.

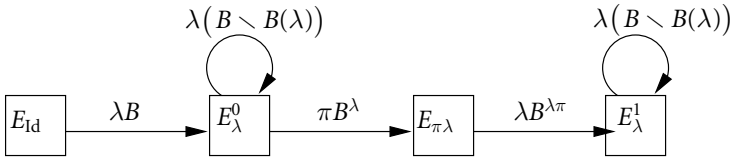
11 Boucles λ (les automates $\mathcal{L}_1$ et $\mathcal{L}_2$)

On introduit, dans cette section, l'automate $\mathcal{L}_1$ (resp. $\mathcal{L}_2$) qui décrit les décompositions minimales associées à des automorphismes de $D\pi D$ (resp. $D\pi D\pi B\lambda$). On montre la conjecture 8.6 pour les $\mathcal{L}_1$-décompositions (resp. $\mathcal{L}_2$-décompositions).

Définition 11.1 **(Le sous-automate $\mathcal{L}_1$)** On définit l'automate $\mathcal{L}_1$ dont les quatre états sont E_{Id} (initial), E^0_λ, $E_{\pi\lambda}$ et E^1_λ et dont les transitions sont :

De	E_{Id}	vers	E^0_λ	$: \lambda B$.
De	E^0_λ	vers	E^0_λ	$: \lambda\big(B \setminus B(\lambda)\big)$.
De	E^0_λ	vers	$E_{\pi\lambda}$	$: \pi B^\lambda$.
De	$E_{\pi\lambda}$	vers	E^1_λ	$: \lambda B^{\lambda\pi}$.
De	E^1_λ	vers	E^1_λ	$: \lambda\big(B \setminus B(\lambda)\big)$.

Remarque 11.2 On peut représenter $\mathcal{L}_1$ par la figure suivante :



https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Proposition 11.3 *Soit $\mathcal{D}$ une $\mathcal{L}_1$-décomposition minimale. Posons $f = z_*(\mathcal{D})$.*

Si $\mathrm{fin}(\mathcal{D}) = E^0_\lambda$, alors $\mathcal{D}$ est une $\mathcal{L}_0$-décomposition.

Si $\mathrm{fin}(\mathcal{D}) = E_{\pi\lambda}$, alors $f(x,y,z) = R(x,z)$ avec $R = z_*(\mathcal{D}_0)$ où $\mathcal{D}_0$ est un $\mathcal{L}_0$-décomposition.

Si $\mathrm{fin}(\mathcal{D}) = E^1_\lambda$, alors $f(x,y,z) = R\big(x+P_1(y,z),\rho(y)\big)$ avec $R = z_*(\mathcal{D}_0)$ où $\mathcal{D}_0$ est un $\mathcal{L}_0$-décomposition, ρ une c.H.g. et $P_1 \in k[y,z]$ tel que f soit B-minimal dans $B^\lambda f$.

Preuve Soit $R(y,z) \in k[y,z]$ et $h \in \pi B^\lambda$, alors $h\big(R(y,z)\big) = R(x,z)$.

Soit $R(x,z) \in k[x,z]$ et $h \in \lambda B^{\lambda\pi}$. Alors $h\big(R(x,z)\big) = R(x,y)$.

Soit $f(x,y,z) = R\big(x + P_1(y,z),\rho(y)\big)$ avec $R(x,y) \in k[x,y]$, ρ une c.H.g. et $P_1 \in k[y,z]$ et soit $h = \big(bx+P(y,z), cz+Q(y), dz\big) \in \lambda B \smallsetminus B(\lambda)$ alors $h(f)(x,y,z) = R\big(x + P_2(y,z), h\rho(y)\big)$ avec $R_1(x,y) = R(bx,y)$ et

$$P_2(y,z) = b^{-1}\Big(P_0(y,z) + P_1\big(cz + Q_0(y), dy\big)\Big).$$

Remarque 11.4 Dans la proposition 11.3, et ce sera également le cas dans la proposition 11.8, on n'utilise que la condition 2 de minimalité (*cf.* la remarque 7.4). Ceci est dû au fait que l'on considère des décompositions $\mathcal{D}$ telles que $\mathrm{lg}_\pi(\mathcal{D}) \leq 2$. Les problèmes qui justifient l'introduction du principe 3 (des relations) n'apparaissent qu'à partir de $\mathrm{lg}_\pi(\mathcal{D}) = 3$ (*cf.* l'exemple 3.5).

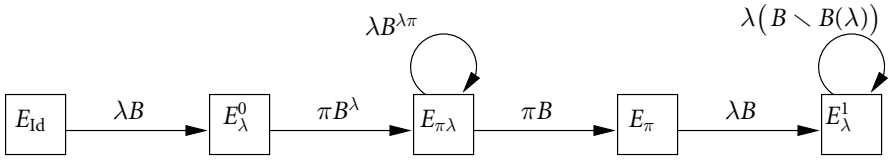
Théorème 11.5 ($\mathrm{car}(k) = 0$) *Soit $\mathcal{D}$ une $\mathcal{L}_1$-décomposition minimale, alors le polynôme $z_*(\mathcal{D})$ est faible.*

Preuve Si $\mathrm{fin}(\mathcal{D}) = E^0_\lambda$ (resp. $\mathrm{fin}(\mathcal{D}) = E_{\pi\lambda}$) cela résulte du théorème 9.8 (resp. et de la proposition 8.9). Si $\mathrm{fin}(\mathcal{D}) = E^1_\lambda$ cela résulte du théorème 10.1.

Définition 11.6 **(Le sous-automate $\mathcal{L}_2$)** On définit l'automate $\mathcal{L}_2$ dont les cinq états sont E_{Id} (initial), E^0_λ, E_π, $E_{\pi\lambda}$ et E^1_λ et dont les transitions sont :

De	E_{Id}	vers	E^0_λ	: λB.
De	E^0_λ	vers	$E_{\pi\lambda}$	: πB^λ.
De	$E_{\pi\lambda}$	vers	$E_{\pi\lambda}$	: $\lambda B^{\lambda\pi}$.
De	$E_{\pi\lambda}$	vers	E_π	: πB.
De	E_π	vers	E^1_λ	: λB.
De	E^1_λ	vers	E^1_λ	: $\lambda\big(B \smallsetminus B(\lambda)\big)$.

Remarque 11.7 On peut représenter $\mathcal{L}_2$ par la figure suivante :



https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Proposition 11.8 *Soit $\mathcal{D}$ une $\mathcal{L}_2$-décomposition minimale, posons $f = z_*(\mathcal{D})$.*
Si $\operatorname{fin}(\mathcal{D}) = E^0_\lambda$ *alors* $f(x,y,z) \in k^*y$.
Si $\operatorname{fin}(\mathcal{D}) = E_{\pi\lambda}$ *alors* $f(x,y,z) \in k^*x$.
Si $\operatorname{fin}(\mathcal{D}) = E_\pi$ *alors* $f(x,y,z) \in k^*y + k[x,z]$ *est B-minimal dans* $B^\pi f$.
Si $\operatorname{fin}(\mathcal{D}) = E^1_\lambda$ *alors* $f(x,y,z) = \rho(z) + R\big(x + P_1(y,z), \rho(y)\big)$ *avec* $R \in k[x,y]$, ρ *une c.H.g. et* $P_1 \in k[y,z]$ *tel que* f *soit B-minimal dans* $B^\lambda f$.

Preuve Soit $f \in k^*y$ et $h \in \pi B^\lambda$, alors $h(f) \in k^*x$.
Soit $f \in k^*x$ et $h \in \lambda B^{\lambda\pi}$, alors $h(f) \in k^*x$.
Soit $f \in k^*x$ et $h \in \pi B$, alors $h(f) \in k^*y + k[x,z]$.
Soit $f(x,y,z) = ay + R(x,z) \in k^*y + k[x,z]$ et $h = \big(bx + P(y,z), cz + Q(y), dy\big) \in \lambda B$. Alors $h(f)(x,y,z) = \rho(z) + R_1\big(x + P_1(y,z), \rho(y)\big)$, avec $R_1(x,y) = aQ(y) + R(bx,dy)$, $P_1(y,z) = b^{-1}P(y,z)$ et $\rho = (x,y,az)$.
Soit $f(x,y,z) = \rho(z) + R\big(x + P_1(y,z), \rho(y)\big)$ avec $R \in k[x,y]$, ρ une c.H.g. et $P_1 \in k[y,z]$. Si $h = \big(bx + P(y,z), cz + Q(y), dy\big) \in \lambda\big(B \smallsetminus B(\lambda)\big)$ alors $h\rho$ est une c.H.g. et $h(f)(x,y,z) = h\rho(z) + R_1\big(x + P_2(y,z), h\rho(y)\big)$ avec $R_1(x,y) = R(bx,y)$ et $P_2(y,z) = b^{-1}\Big(P(y,z) + P_1\big(cz + Q(y), dy\big)\Big)$.

Théorème 11.9 $(\operatorname{car}(k) = 0)$ *Soit $\mathcal{D}$ une $\mathcal{L}_2$-décomposition minimale, alors le polynôme $z_*(\mathcal{D})$ est faible.*

Preuve Si $\operatorname{fin}(\mathcal{D}) = E^0_\lambda$ (resp. $\operatorname{fin}(\mathcal{D}) = E_{\pi\lambda}$), cela résulte de l'exemple 8.3. Si $\operatorname{fin}(\mathcal{D}) = E_\pi$, cela résulte de la proposition 8.13. Si $\operatorname{fin}(\mathcal{D}) = E^1_\lambda$, cela résulte du théorème 10.1.

Exemple 11.10 Posons $b_1 = (x + y^2, y, z)$, $b_2 = (x, y - z^3, z)$ et $b_3 = (x, y + z^2, z)$. Considérons la décomposition suivante : $\mathcal{D} = (\lambda b_3, \lambda b_2, \pi b_1, \pi, \lambda)$.

C'est une $\mathcal{L}_2$-décomposition qui n'est pas minimale. La $\mathcal{L}_2$-décomposition minimale associée grâce au théorème 7.7 est celle donnée dans l'exemple 1.9, *i.e.*, $\mathcal{D}' = (\lambda b'_3, \lambda b_2, \pi b_1, \pi, \lambda)$ avec $b'_3 = (x + \frac{3}{2}yz + z^3, y + z^2, z)$. Elle est de longueur 5 et a la propriété suivante : $\deg\big(z_i(\mathcal{D}')\big) = i - 1$ pour $i \geq 2$. On peut se poser la question suivante :

Question 11.11 Existe-t-il une $\mathcal{A}$-décomposition minimale $\mathcal{D}$ de longueur 6 telle que $\deg\big(z_i(\mathcal{D})\big) = i - 1$ pour $i \geq 2$?

Exemple 11.12 Posons $b_1 = (x + y^2, y, z)$, $b_2 = (x, y - z^5, z)$ et $b_3 = (x, y + z^2, z)$. Considérons la décomposition suivante : $\mathcal{D} = (\lambda b_3, \lambda b_2, \pi b_1, \pi, \lambda)$.

C'est une $\mathcal{L}_2$-décomposition qui n'est pas minimale. La $\mathcal{L}_2$-décomposition minimale associée grâce au théorème 7.7, est : $\mathcal{D}' = (\lambda b'_3, \lambda b_2, \pi b_1, \pi, \lambda)$, avec $b'_3 = \big(x + P(z,y), y + z^2, z\big)$ où $P(y,z)$ minimise le degré de $z_*(\mathcal{D}') = f(x,y,z) = y + \big(x + P(y,z)\big)^2 - (z + y^2)^5$.

– Si $\operatorname{car}(k) = 2$, par exemple $P(y,z) = y^5 + yz^2$ et $f(x,y,z) = y + z^5 + y^8z + x^2$ est de degré 9 et est faible.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

En effet, soit $b = \big(x + P_0(y,z), Q_0(z), z\big) \in B//H$, on a :

$$b(f) = Q_0 + z^5 + Q_0^8 z + P_0^2 + x^2.$$

$\deg(Q_0 + z^5 + Q_0^8 z + P_0^2) \geq 9$, donc $\deg\big(b(f)\big) \geq 9 = \deg(f)$.

– Si $\mathrm{car}(k) = 5$, par exemple $P(y,z) = y^5$ et $f(x,y,z) = y - z^5 + 2xy^5 + x^2$ est de degré 6 et est faible.

En effet, soit $b = \big(x + P_0(y,z), Q_0(z), z\big) \in B//H$, on a :

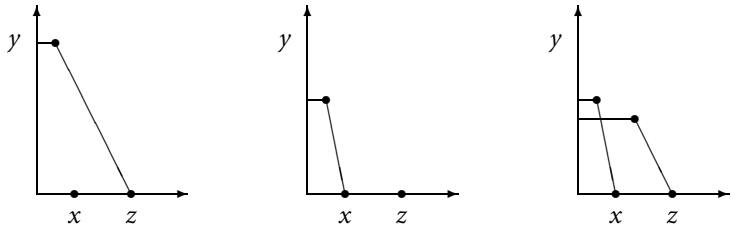
$$b(f) = Q_0 + P_0(P_0 + 2Q_0^5) - z^5 + 2x(P_0 + Q_0^5) + x^2.$$

Si $\mathrm{lt}\, P_0 + \mathrm{lt}\, Q_0^5 = 0$ alors $\deg\big(Q_0 + P_0(P_0 + 2Q_0^5)\big) \geq 25$, sinon $\deg(P_0 + Q_0^5) \geq 5$.

Donc $\deg\big(b(f)\big) \geq 6 = \deg(f)$.

Si $\mathrm{car}(k) \notin \{2,5\}$, par exemple $P(y,z) = y^5 + \frac{5}{2}y^3z + \frac{15}{8}yz^2$ et $f(x,y,z) = y + z^5 - \frac{95}{64}y^2z^4 - \frac{5}{8}y^4z^3 + (2y^5 + 5y^3z + \frac{15}{4}yz^2)x + x^2$ est de degré 7 et est faible (*cf.* la preuve du théorème 10.1).

Remarque 11.13 Dans l'exemple précédent, le polyèdre de Newton de f est l'enveloppe convexe de ses intersections avec les plans $x = 0$ et $z = 0$, ce qui permet de le représenter par ces deux polygones, sur un même plan.



$\mathrm{car}(k) = 2$ $\mathrm{car}(k) = 5$ $\mathrm{car}(k) = 0$

12 Résultats à l'Alev

Dans cette section, on applique de façon concrète les théorèmes de la section précédente pour obtenir des résultats d'impossibilité de décomposition des z-automorphismes qui ne sont pas fortement modérés.

Remarque 12.1 Chaque corollaire de cette section est obtenu en appliquant le corollaire 2.14 à la proposition qui le précède.

Proposition 12.2 *Soit $\sigma \in D$, alors* $\mathrm{CD}(\sigma) \neq \varnothing$.

Preuve Soit $\mathcal{D}$ une $\mathcal{A}$-décomposition de σ minimale. Clairement $\mathcal{D}$ est une $\mathcal{L}_0$-décomposition. En appliquant le théorème 9.8 aux sous-décompositions initiales de $\mathcal{D}$, on a $z_i(\mathcal{D})$ est faible pour tout $i \leq \lg(\mathcal{D})$, *i.e.*, $\mathrm{CD}(\sigma) \neq \varnothing$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

Corollaire 12.3 *Soit $s_1, s_2 \in F$ et $\sigma \in D$, alors $s_2\sigma s_1 \notin Z \setminus F$.*

Proposition 12.4 ($\mathrm{car}(k) = 0$) *Soit $\sigma_1, \sigma_2 \in D$, alors* $\mathrm{CD}(\sigma_1\pi\sigma_2) \neq \varnothing$.

Preuve Soit $\mathcal{E} = (h_m, \dots, h_1)$ une $\mathcal{A}$-décomposition de $\sigma = \sigma_1\pi\sigma_2$ minimale. Montrons par l'absurde que $\mathcal{E}$ est une $\mathcal{L}_1$-décomposition. L'automate $\mathcal{L}_1$ reconnait tous les mots de longueur 1, donc il existe $n \in \{2, \dots, m\}$ tel que $\mathcal{D} = (h_{n-1}, \dots, h_1)$ soit reconnu, mais pas $(h_n, \dots, h_1)$. Appliquons la proposition 11.3.

Si $\mathrm{fin}_{\mathcal{L}_1}(\mathcal{D}) = E^0_\lambda$, alors $\mathcal{D}$ est une $\mathcal{L}_0$-décomposition et $h_n \in \pi(B \setminus B^\lambda)$. Posons $z_*(\mathcal{D}) = R(y,z)$ et $h_n = \big(y + P(x,z), x + Q(z), z\big)$ alors $z_n(\mathcal{E}) = h_n\big(R(y,z)\big) = R\big(x + Q(z), z\big)$. Puisque $\mathrm{lt}\, R(y,z) \in k[y]$ (proposition 9.7) et $\deg(Q) \geq 1$, on a :

$$\deg\Big(R\big(x + Q(z), z\big)\Big) = \deg_z\Big(R\big(x + Q(z), z\big)\Big) = \deg_y\big(R(y,z)\big)\,\deg(Q),$$

or $\deg\big(R(x,z)\big) = \deg_y\big(R(y,z)\big)$ et $\deg_z\big(R(x,z)\big) < \deg_y\big(R(y,z)\big)$.

Ceci contredit la B-minimalité de $z_n(\mathcal{E})$ dans $B^\pi z_n(\mathcal{E})$.

Si $\mathrm{fin}_{\mathcal{L}_1}(\mathcal{D}) = E_{\pi\lambda}$ alors $z_*(\mathcal{D}) = R(x,z)$ avec $R = z_*(\mathcal{D}_0)$ où $\mathcal{D}_0$ est une $\mathcal{L}_0$-décomposition et $h_n \in \lambda(B \setminus B^{\lambda\pi})$. Posons $h_n = \big(x + P(z,y), z + Q(y)\big)$ alors $z_n(\mathcal{E}) = h_n\big(R(x,z)\big) = R\big(x + P(z,y), z\big)$. Puisque $\mathrm{lt}\, R(y,z) \in k[y]$ (proposition 9.7) et $\deg(P) \geq 1$, on a :

$$\deg\Big(R\big(x + P(z,y), z\big)\Big) = \deg_{y,z}\Big(R\big(x + P(z,y), z\big)\Big) = \deg_y\big(R(y,z)\big)\,\deg(P).$$

Or $\deg\big(R(x,z)\big) = \deg_y\big(R(y,z)\big)$ et $\deg_{y,z}\big(R(x,z)\big) < \deg_y\big(R(y,z)\big)$.

Ceci contredit la B-minimalité de $z_n(\mathcal{E})$ dans $B^\lambda z_n(\mathcal{E})$.

Donc $\mathcal{E}$ est une $\mathcal{L}_1$-décomposition minimale. En appliquant le théorème 11.5 aux sous-décompositions initiales de $\mathcal{E}$, on en déduit que $z_i(\mathcal{D})$ est faible pour tout $i \in \{1, \dots, m\}$, *i.e.*, $\mathrm{CD}(\sigma) \neq \varnothing$.

Corollaire 12.5 ($\mathrm{car}(k) = 0$) *Soit $s_1, s_2 \in F$ et $\sigma_1, \sigma_2 \in D$, alors $s_2\sigma_2\pi\sigma_1 s_1 \notin Z \setminus F$.*

Remarque 12.6 Le corollaire 12.3 (resp. le corollaire 12.5) généralise 1 et 2 (resp. (3) de la proposition 3.6 de [A].

Proposition 12.7 ($\mathrm{car}(k) = 0$) *Soient $\sigma_1, \sigma_2 \in D$ et $b \in B$, alors* $\mathrm{CD}(\sigma_1\pi\sigma_2\pi b\lambda) \neq \varnothing$.

Preuve Soit $\mathcal{E}$ une $\mathcal{A}$-décomposition de σ minimale. Si $\mathrm{lg}_\pi(\mathcal{E}) < 2$, on est ramené au cas des propositions 12.2 ou 12.4. Si $\mathrm{lg}_\pi(\mathcal{E}) = 2$, on montre, de façon analogue à la preuve de la proposition 12.2, que $\mathcal{E}$ est une $\mathcal{L}_1$-décomposition et on conclut de la même façon en appliquant le théorème 11.9.

Corollaire 12.8 ($\mathrm{car}(k) = 0$) *Soient $s_1, s_2 \in F$, $b \in B$ et $\sigma_1, \sigma_2 \in D$, alors $s_2\sigma_2\pi\sigma_1\pi b\lambda s_1 \notin Z \setminus F$.*

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

A Automates

Dans cette section, on rappelle quelques définitions classiques de la théorie des automates. Pour un exposé de la théorie des automates voir [Ko]. Remarquons que nous utilisons des notations un peu inhabituelles mais qui permettent d'éviter les confusions avec la composition des automorphismes et que nous considérons des automates sur un alphabet éventuellement infini.

Dans tout ce qui suit, $\mathcal{H}$ désigne un ensemble appelé *alphabet*.

***Définition A.1* (Mot)** On appelle *mot* sur l'alphabet $\mathcal{H}$ tout suite $h = (h_n, \dots, h_1)$ finie (ou vide) d'éléments de $\mathcal{H}$. L'entier n est la *longueur* de h.

***Définition A.2* (Concaténé)** Soient $g = (g_n, \dots, g_1)$ et $h = (h_m, \dots, h_1)$ deux mots sur l'alphabet $\mathcal{H}$. On appelle *concaténé* de g et h le mot $g*h := (g_n, \dots, g_1, h_m, \dots, l_1)$.

***Définition A.3* (Ordres des mots)** Soient g et h deux mots sur l'alphabet $\mathcal{H}$,

(1) on dit que g est un *préfixe* de h s'il existe un mot f sur l'alphabet $\mathcal{H}$ tel que $h = g * f$,
(2) on dit que g est un *suffixe* de h s'il existe un mot f sur l'alphabet $\mathcal{H}$ tel que $h = f * g$,
(3) on dit que g est un *sous-mot* de h s'il existe deux mots e et f sur l'alphabet $\mathcal{H}$ tel que $h = e * g * f$.

***Définition A.4* (Ordres induits sur un groupe représenté)** Soit G un groupe représenté par un ensemble $\mathcal{H}$ de générateurs et des relations. Cela implique qu'il existe un morphisme ϕ de monoïdes entre l'ensemble des mots sur l'alphabet $\mathcal{H}$ (muni de la concaténation) et le groupe G. Soit $g \in G$, on note $\min(g)$ l'ensemble des mots h sur l'alphabet $\mathcal{H}$ qui représentent g (*i.e.*, tel que $\phi(h) = g$) et de longueur minimale pour cette propriété. Soit $\leq$ un ordre sur l'ensemble des mots (*cf.* par exemple A.3). On définit *l'ordre induit par la représentation de* G sur le groupe G en posant "$g_1 \leq g_2$", si et seulement s'il existe $h_1 \in \min(g_1)$ et $h_2 \in \min(g_2)$ tels que $h_1 \leq h_2$.

***Définition A.5* (Automate)** On appelle *automate* sur l'alphabet $\mathcal{H}$ un quadruplet $\mathcal{A} = (\mathcal{E}, \mathcal{I}, \mathcal{F}, \mathcal{T})$ où :

(1) $\mathcal{E}$ est un ensemble (l'ensemble des *états*),
(2) $\mathcal{I} \subset \mathcal{E}$ est un sous-ensemble d'états (l'ensemble des *états initiaux*),
(3) $\mathcal{F} \subset \mathcal{E}$ est un sous-ensemble d'états (l'ensemble des *états terminaux*),
(4) $\mathcal{T}$ est une application de $\mathcal{E}^2$ dans l'ensemble des sous-ensembles de $\mathcal{H}$ (pour tout couple $(E_1, E_2) \in \mathcal{E}^2$ d'états, $\mathcal{T}(E_1, E_2) \subset \mathcal{H}$ est l'ensemble des *transitions* de E_1 vers E_2).

***Définition A.6* (Automate déterministe)** Soit $\mathcal{A} = (\mathcal{E}, \mathcal{I}, \mathcal{F}, \mathcal{T})$ un automate sur l'alphabet $\mathcal{H}$, on dit que $\mathcal{A}$ est *déterministe* si $\mathcal{I}$ est un singleton et si pour tout triplet $(E_1, E_2, E_3) \in \mathcal{E}^3$ tel que $E_2 \neq E_3$, on a $\mathcal{T}(E_1, E_2) \cap \mathcal{T}(E_1, E_3) = \varnothing$.

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press

***Définition A.7* (Mot reconnu)** Soient $\mathcal{A} = (\mathcal{E}, \mathcal{I}, \mathcal{F}, \mathcal{T})$ un automate et $h = (h_n, \dots, h_1)$ un mot sur l'alphabet $\mathcal{H}$. On dit que h est *reconnu* par $\mathcal{A}$ s'il existe un mot $(E_n, \dots, E_0)$ sur l'alphabet $\mathcal{E}$ (*i.e.*, une suite d'états) tel que $E_0 \in \mathcal{I}$, $E_n \in \mathcal{F}$ et pour tout $i \in \{1, \dots, n\}$, $h_i \in \mathcal{T}(E_{i-1}, E_i)$.

***Définition A.8* (État final)** Soient $\mathcal{A} = (\mathcal{E}, \mathcal{I}, \mathcal{F}, \mathcal{T})$ un automate déterministe sur l'alphabet $\mathcal{H}$ et $h = (h_n, \dots, h_1)$ un mot reconnu par $\mathcal{A}$. Il existe alors une unique suite d'états $(E_n, \dots, E_0)$ telle que $\{E_0\} = \mathcal{I}$, $E_n \in \mathcal{F}$ et, pour tout $i \in \{1, \dots, n\}$, $h_i \in \mathcal{T}(E_{i-1}, E_i)$. On appelle *état final* de h et on note $\mathrm{fin}_{\mathcal{A}}(h)$ (ou simplement $\mathrm{fin}(h)$ s'il n'y a pas d'ambiguïté sur l'automate) l'état terminal E_n.

Références

[A] J. Alev, *A note on Nagata's automorphism.* Dans: Automorphisms of the affine spaces (ed. A. van den Essen), Kluwer Academic Publishers, 1995, 215–221.

[DGY] V. Drensky, J. Gutierrez and J.-T. Yu, *Gröbner bases and the Nagata automorphism.* J. Pure Appl. Algebra (2) **135**(1999), 135–153.

[E] A. van den Essen, *Polynomial automorphisms and the Jacobian Conjecture.* Progr. Math. **190**, Birkhäuser Verlag, Basel-Boston-Berlin, 2000.

[EV] E. Edo and S. Vénéreau, *Length 2 variables and transfer.* Ann. Polon. Math. **76**(2001), 67–76.

[Fr] G. Freudenburg, *Triangulability criteria for additive group actions on affine space*. J. Pure Appl. Algebra (3) **105**(1995), 267–275.

[Fu] J-P. Furter, *On the variety of automorphisms of the affine plane.* J. Algebra (2) **195**(1997), 604–623.

[FM] S. Friedland and J. Milnor, *Dynamical properties of plane polynomial automorphisms.* Ergodic Theory Dynamical Systems (1) **9**(1989), 67–99.

[J] H. Jung, *Über ganze birationale Transformationen der Ebene.* J. Reine Angew. Math. **184**(1942), 161–174.

[Ko] D. Kozen, *Automata and computability.* Undergraduate Texts in Computer Science, Springer-Verlag, New York, 1997.

[Ku] W. van der Kulk, *On polynomial rings in two variables.* Nieuw Arch. Wiskunde (3) **1**(1953), 33–41.

[Lak] I. Lakatos, *Preuves et réfutations, essai sur la logique de la découverte mathématique.* Hermann, Paris, 1984.

[Lam] S. Lamy, *Automorphismes polynômiaux du plan complexe : étude algébrique et dynamique.* Thèse de doctorat, Univ. Paul Sabatier, Toulouse, 2000.

[LB] L. Le Bruyn, *Automorphisms and Lie stacks.* Comm. Algebra (7) **25**(1997), 2211–2226.

[MT] R. Mneimné et F. Testard, *Introduction à la théorie des groupes de Lie classiques.* Collection Méthodes, Hermann, Paris, 1986.

[N] M. Nagata, *On the automorphisms group of* $\mathbb{C}[X, Y]$. Lectures in Math. Kyoto Univ. **5**, 1972.

[R] P. Russell, *Simple birational extensions of two dimensional affine rational domains*. Compositio Math. (2) **33**(1976), 197–208.

Département de mathématiques pures
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex
FRANCE
courriel : edo@math.u-bordeaux.fr

https://doi.org/10.4153/CJM-2003-022-1 Published online by Cambridge University Press